BANKI
KUU YA
KENYA

CENTRAL
BANK OF
KENYA

Haile Selassie Avenue
P. O. Box 60000 - 00200 Nairobi Kenya
Telephone: 2861000/2863000
Fax 340192/250783
Email: supplies@centralbank.go.ke

TENDER DOCUMENT
SUPPLY, INSTALLATION, TESTING, TRAINING AND COMMISSIONING OF INTEGRATED SECURITY SYSTEM FOR CENTRAL BANK OF KENYA

.

TENDER REF. NO. CBK/028/2026-2027

TENDER CLOSING DATE: 5TH OCTOBER 2026 AT 10.30 A.M.

C2: CBK - Official

Table of contents

Section I - Instructions to Tenderers **7**

A. GENERAL **7**

1. Scope of Tender 7
2. Definitions 7
3. Fraud and Corruption 7
4. Eligible Tenderers 8
5. Eligible Goods and Services 9

B. Contents of Tendering Document **10**

6. Sections of Tendering Document
7. Site Visit 10
8. Pre-Tender Meeting 10
9. Clarification of Tendering Document 11
10. Amendment of Tendering Document 11

C. PREPARATION OF TENDERS **11**

11. Cost of Tendering 11
12. Language of Tender 11
13. Documents Comprising the Tender 11
14. Form of Tender and Price Schedules 12
15. Alternative Tenders 12
16. Documents Establishing the Eligibility of the Information System 13
17. Documents Establishing the Eligibility and Qualifications of the Tenderer 13
18. Documents Establishing Conformity of the Information System 14
19. Tender Prices 14
20. Currencies of Tender and Payment 15
21. Period of Validity of Tenders 16
22. Tender Security 16
23. Format and Signing of Tender 16

D. Submission and Opening of Tenders **17**

24. Submission, Sealing and Marking of Tenders 17
25. Deadline for Submission of Tenders 18
26. Late Tenders 18
27. Withdrawal, Substitution, and Modification of Tenders 18
28. Tender Opening 18

E. Evaluation and Comparison of Tenders **19**

29. Confidentiality 19
30. Clarification of Tenders 19
31. Deviations, Reservations, and Omissions 19
32. Determination of Responsiveness 20
33. Nonmaterial Non-conformities 20
34. Correction of Arithmetical Errors 20
35. Conversion to Single Currency 21
36. Margin of Preference and Reservations 21
37. Evaluation of Tenders 21
38. Preliminary Examination 21
39. Technical Evaluation 21
40. Financial/Economic Evaluation 22
41. Comparison of Tenders 22
42. Abnormally Low Tenders and Abnormally High Tenders 23
43. Unbalanced or Front-Loaded Tenders 23
44. Eligibility and Qualification of the Tenderer 23
45. Procuring Entity's Right to Accept Any Tender, and to Reject Any or All Tenders 24

A. Award of Contract **24**

6. Award Criteria 24
7. Procuring Entity's Right to Vary Quantities at Time of Award 24
8. Notice of Intention to enter into a contract/ Notification of Award 25
9. Standstill Period 25
10. Debriefing by the Procuring Entity 25
11. Letter of Award 25
12. Signing of Contract 25
13. Performance Security 25
14. Publication of Procurement Contract 26
15. Adjudicator 26
16. Procurement Related Complaint & Administrative Review 26

SECTION II - TENDER DATA SHEET (TDS) **27**

SECTION III - EVALUATION AND QUALIFICATION CRITERIA **31**

1. Evaluation Criteria 31
2. Post Qualification and Contract Award 35
3. Qualification Form 35
4. Personnel 35

SECTION IV - TENDERING FORMS **36**

1. FORM OF TENDER **36**
- a. TENDERER'S ELIGIBILITY- CONFIDENTIAL BUSINESS QUESTIONNAIRE 39
- b. CERTIFICATE OF INDEPENDENT TENDER DETERMINATION 42
- c. SELF-DECLARATION FORM 43
- d. APPENDIX 1- FRAUD AND CORRUPTION 46

2. Price Schedule Forms **50**
- a. Grand Summary Cost Table 51
- b. Supply and Installation Cost Summary Table 51
- c. Recurrent Cost Summary Table 52
- d. supply and Installation Cost Sub-Table 53
- e. Recurrent Cost Sub-Table 54
- f. Country of Origin Code Table 55

QUALIFICATION FORMS **53**

1. FOREIGN TENDERERS 40% RULE 53
2. Form ELI-1 Tenderer Information Form 54
3. Form ELI-1 Tenderer's JV Members Information Form 55
4. Form CON – 1 Historical Contract Non-Performance and Pending Litigation. 56
5. Form EXP -1 Experience - General Experience 57
6. Form EXP – 2 Specific Experience 57
7. Form EXP – 2 (cont.) Specific Experience(cont.) 58
8. Form CCC-1 Summary Sheet: Current Contract Commitments / Work in Progress 58
9. Form FIN –1 Financial Situation 59
10. Form FIN –2 Average Annual Turnover 59
11. Form F-3 Financial Resources 60
12. Personnel Capabilities 60
13. Intellectual Property Forms 63
14. Conformance of Information System Materials 65

PART 2 – PROCURING ENTITY'S REQUIREMENTS **70**

Section V - REQUIREMENTS OF THE RENEWAL OF NETWORK ACCESS CONTROL SOLUTION **71**

i) Technical Requirements for the Procurement of Maintenance Services **71**

Technical support for the solution 71
ii) Project Plan & Implementation Schedule **71**
Implementation Schedule Table 73
Site Tables 73
Tables of Holidays & Other non-working Days 73
System Inventory Tables **74**
System Inventory Table (Supply & Installation Cost Items) 75
System Inventory Table (Recurrent Cost Items) 75

PART 3 – Conditions of Contract and Contract Forms **88**

Section VI - General Conditions of Contract **General Conditions of Contract** **89**
1. Contract and Interpretation 89
2. Contract Documents 92
3. Interpretation 92
4. Notices 93
5. Governing Law 94
6. Fraud and Corruption 94
7. Scope of the System 94
8. Time for Commencement and Operational Acceptance 95
9. Supplier's Responsibilities 95
10. Procuring Entity's Responsibilities 96
11. Contract Price 97
12. Terms of Payment 97
13. Securities 97
14. Taxes and Duties 98
15. Copyright 98
16. Software License Agreements 99
17. Confidential Information 100
18. Representatives 100
19. Project Plan 101
20. Subcontracting 102
21. Design and Engineering 103
22. Procurement, Delivery, and Transport 104
23. Product Upgrades 105
24. Implementation, Installation, and Other Services 106
25. Inspections and Tests 106
26. Installation of the System 106
27. Commissioning and Operational Acceptance 107
28. Operational Acceptance Time Guarantee 108
29. Defect Liability 109
30. Functional Guarantees 110
31. Intellectual Property Rights Warranty 111
32. Intellectual Property Rights Indemnity 111
33. Limitation of Liability 112
34. Transfer of Ownership 112
35. Care of the System 113
36. Loss of or Damage to Property; Accident or Injury to Workers; Indemnification 113
37. Insurances 114
38. Force Majeure 115
39. Changes to the System 116
40. Extension of Time for Achieving Operational Acceptance 113
41. Termination 119
42. Assignment 122
43. Settlement of Disputes 122

Section VII - Special Conditions of Contract **124**

A. Contract and Interpretation 124
B. Subject Matter of Contract 124
C. Payment 125
D. Intellectual Property 126

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System 129
F. Guarantees and Liabilities 131
G. Risk Distribution 132
H. Change in Contract Elements 133
I. Settlement of Disputes 133

Section XIII - Contract Forms 134

1. Contract Forms 135
   a) Notification of Intention toward 135
   b) Letter of Award 137
2. Contract Agreement 138
3. APPENDIXES 140
   Appendix 1. Supplier's Representative 140
   Appendix 2. Adjudicator *[if there is no Adjudicator, state "not applicable"]* 141
   Appendix 3. List of Approved Subcontractors 142
   Appendix 4. Categories of Software Appendix 5. Custom Materials 143
   Appendix 6. Revised Price Schedules (if any) 145
   Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments 146
4. Performance and Advance Payment Security Forms 147
5. Installation and Acceptance Certificates *(insert format)* 149
6. Change Order Procedures and Forms 151
7. Beneficial Ownership Disclosure Form 151

INVITATION TO TENDER (ITT) BY CENTRAL BANK OF KENYA

1. The **Central Bank of Kenya** invites sealed tenders **for Supply, Installation, testing, training and Commissioning of Integrated Security System for Central Bank of Kenya (Tender Reference No. CBK/028/2026-2027)**

2. A complete set of tender documents containing detailed information can be downloaded free of charge from the Central Bank of Kenya website: www.centralbank.go.ke or from the Government tenders portal: www.tenders.go.ke. All interested and eligible bidders should forward their emails and address to the **Email address: supplies@centralbank.go.ke**. to facilitate any further clarification or addendum.

3. Prices quoted should be net inclusive of all taxes and levies, must be in Kenya Shillings and shall remain valid for **140 days** from the closing date of the tender.

4. All Tenders must be accompanied by a **Tender Security** of **Kes. 100,000.00** in the format provided in the tender document valid for **170 days** from the date of tender opening.

5. A pre-bid meeting will be held on **24th September 2026** at 10.30 a.m. virtually or physically at 11th floor Extelcom house, Procurement conference room. Interested bidders intending to join the meeting to share their details and for online are requested to share their email addresses using Supplies@centralbank.go.ke and a link to the meeting will be shared.

6. Completed tender documents are to be enclosed in plain sealed envelopes marked with tender reference number and be deposited in the **Green Tender Box No. 3** at the main entrance, ground floor of **Central Bank of Kenya along Haile Selassie Avenue,** to be received on or before **5th October 2026 at 10.30 A.M**. Electronic Tenders ***will not*** **be permitted**.

7. Tenders will be opened immediately after the deadline date and time specified above or any deadline date and time specified later in the **Senior Staff Canteen Room on 6th floor of CBK Building, Haile Selassie Avenue, Nairobi**. Tenders will be publicly opened in the presence of the Tenderers' designated representatives or anyone who chooses to attend. Bidders' representatives and other persons who choose to attend the tender opening session will be required to have personal identification documents (National ID/Passport).

8. Late tender will be rejected.

9. The addresses referred to above are:

A. Address for obtaining further information and for purchasing tender documents

Central Bank of Kenya
The Director, General Services Department
Central Bank of Kenya, Head Office in Nairobi on Haile Selassie Avenue,
P. O. Box 60000 – 00200, Nairobi
Tel. No. 020 2860000, E-mail address: **supplies@centralbank.go.ke**.

B. Address for Submission of Tenders.
Central Bank of Kenya, Head Office in Nairobi, Haile Selassie Avenue
Green Tender Box No. 3 at the main entrance, ground floor
P. O. Box 60000 – 00200, Nairobi

C. Address for Opening of Tenders.
Central Bank of Kenya, Head Office in Nairobi, Senior Staff canteen room on 6th floor

Deputy Director/Head of Procurement Division
General Services Department

PART 1 - TENDERING PROCEDURES

SECTION I - INSTRUCTIONS TO TENDERERS (ITT)

Section I - Instructions to Tenderers

A. GENERAL

1. Scope of Tender

1.1 The Procuring Entity, as indicated **in the TDS**, issues this tendering document for the supply and installation of the Integrated Security System as specified in Section V, Procuring Entity's Requirements. The name, identification and number of lots (contracts) of this ITT are specified **in the TDS.**

2. Definitions

2.1 Unless otherwise stated, throughout this tendering document definitions and interpretations shall be as prescribed in Section VI, General Conditions of Contract.

2.3 Throughout this tendering document:

a) The term "in writing" means communicated in written form (e.g., by mail, e-mail, fax, including if specified in the **TDS**, distributed or received through the electronic-procurement system used by the Procuring Entity) with proof of receipt.
b) If the context so requires, "singular" means "plural" and vice versa; and
c) "Day" means calendar day, unless otherwise specified as "Business Day". A Business Day is any day that is an official working day of the Procuring Entity. It excludes the Procuring Entity's official public holidays.
d) "Security System" shall carry the same meaning as "Technological Security/Information Technology".

3. Fraud and Corruption

3.1 The Procuring Entity requires compliance with the provisions of the Public Procurement and Asset Disposal Act, 2015, Section 62 "Declaration not to engage in corruption". The tender submitted by a person shall include a declaration that the person shall not engage in any corrupt or fraudulent practice and a declaration that the person or his or her sub-contractors are not debarred from participating in public procurement proceedings.

3.2 The Procuring Entity requires compliance with the provisions of the Competition Act 2010, regarding collusive practices in contracting. Any tenderer found to have engaged in collusive conduct shall be disqualified and criminal and/ or civil sanctions may be imposed. To this effect, Tenderers shall be required to complete and sign the "Certificate of Independent Tender Determination" annexed to the Form of Tender.

3.3 Unfair Competitive Advantage -Fairness and transparency in the tender process require that the Firms or their Affiliates competing for a specific assignment do not derive a competitive advantage from having provided consulting services related to this tender. The Procuring Entity shall indicate in the TDS firms (if any) that provided consulting services for the contract being tendered for. The Procuring Entity shall check whether the owners or controllers of the Tenderer are same as those that provided consulting services. The Procuring Entity shall, upon request, make available to any tenderer information that would give such firm unfair competitive advantage over competing firms.

3.4 Tenderers shall permit and shall cause their agents (whether declared or not), subcontractors, sub-consultants, service providers, suppliers, and their personnel, to permit the Procuring Entity to inspect all accounts, records and other documents relating to any initial selection process, pre-qualification process, tender submission, proposal submission, and contract performance (in the case of award), and to have them audited by auditors appointed by the Procuring Entity.

4 Eligible Tenderers

4.1 A Tenderer may be a firm that is a private entity, a state-owned enterprise or institution subject to ITT 4.6, or any combination of such entities in the form of a joint venture (JV) under an existing agreement or with the intent to enter in to such an agreement supported by a Form of Intent. Public employees and their close relatives *(spouses, children, brothers, sisters and uncles and aunts)* are not eligible to participate in the tender. In the case of a joint venture, all members shall be jointly and severally liable for the execution of the contract in accordance with the

Contract terms. The JV shall nominate a Representative who shall have the authority to conduct all business for and on behalf of any and all the members of the JV during the Tendering process and, in the event the JV is awarded the contract, during contract execution. Members of a joint venture may not also make an individual tender, be a subcontractor in a separate tender or be part of another joint venture for the purposes of the same Tender. The maximum number of JV members shall be specified in the **TDS.**

4.2 Public Officers of the Procuring Entity, their Spouses, Child, Parent, Brothers or Sister. Child, Parent, Brother or Sister of a Spouse, their business associates or agents and firms / organizations in which they have a substantial or controlling interest shall not be eligible to tender or be awarded a contract. Public Officers are also not allowed to participate in any procurement proceedings.

4.3 A Tenderer shall not have a conflict of interest. Any Tenderer found to have a conflict of interest shall be disqualified. A Tenderer may be considered to have a conflict of interest for the purpose of this Tendering process, if the Tenderer:

a. Directly or indirectly controls, is controlled by or is under common control with another Tenderer; or
b. Receives or has received any direct or indirect subsidy from another Tenderer; or
c. Has the same legal representative as another Tenderer; or
d. Has a relationship with another Tenderer, directly or through common third parties, that puts it in a position to influence the Tender of another Tenderer, or influence the decisions of the Procuring Entity regarding this Tendering process; or
e. Any of its affiliates participates as a consultant in the preparation of the design or technical specifications of the Information System that are the subject of the Tender; or
f. Or any of its affiliates has been hired (or is proposed to be hired) by the Procuring Entity or Procuring Entity as Project Manager for the Contract implementation; or
g. Would be providing goods, works, or non-consulting services resulting from or directly related to consulting services for the preparation or implementation of the project specified in the TDSITT2.1 that it provided or were provided by any affiliate that directly or indirectly controls, is controlled by, or is under common control with that firm; or
h. Has a close business or family relationship with a professional staff of the Procuring Entity who: -
    i. Are directly or in directly involved in the preparation of the tendering document or specifications of the Contract, and/ or the Tender evaluation process of such Contract. or
    ii. Would be involved in the implementation or supervision of such Contract unless the conflict stemming from such relationship has been resolved in a manner acceptable to the Procuring Entity throughout the Tendering process and execution of the Contract.

4.4 A firm that is a Tenderer (either individually or as a JV member) shall not participate as a Tenderer or as JV member in more than one Tender except for permitted alternative Tenders. Such participation shall result in the disqualification of all Tenders in which the firm is involved. However, this does not limit the participation of a Tenderer as subcontractor in another Tender or of a firm as a subcontractor in more than one Tender.

4.5 A Tenderer may have the nationality of any country, subject to the restrictions pursuant to ITT4.9. A Tenderer shall be deemed to have the nationality of a country if the Tenderer is constituted, incorporated or registered in and operates in conformity with the provisions of the laws of that country, as evidenced by its articles of incorporation (or equivalent documents of constitution or association) and its registration documents, as the case maybe. This criterion also shall apply to the determination of the nationality of proposed sub-contractors or sub- consultants for any part of the Contract including related Services.

4.6 A Tenderer that has been debarred from participating in public procurement shall be ineligible to tender or be awarded a contract. The list of debarred firms and individuals is available from the website of PPRA www.ppra.go.ke.

4.7 Tenderers that are state-owned enterprises or institutions in Kenya may be eligible to compete and be awarded a Contract(s) only if they can establish that they (i) are legally and financially autonomous (ii) operate under commercial law, and (iii) are not under supervision of the Procuring Entity.

4.8 Firms and individuals may be ineligible if (a) as a matter of law or official regulations, Kenya prohibits commercial relations with that country, or (b) by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, Kenya prohibits any import of goods or contracting of works or services from that country, or any payments to any country, person, or entity in that country.

4.9 The Procuring Entity may require tenderers to be registered with certain authorities in Kenya. Such registration shall be defined in the **TDS**, but care must be taken to ensure such registration requirement does not discourage competition, nor exclude competent tenderers. Registration shall not be a condition for tender, but where a selected tenderer is not so registered, the tenderer shall be given the opportunity to register before signing the contract.

4.10 Foreign tenderers are required to source at least forty (40%) percent of their contract inputs (in supplies, subcontracts, and labor) from national suppliers and contractors. To this end, a foreign tenderer shall provide in its tender documentary evidence that this requirement is met. Foreign tenderers not meeting this criterion will be automatically disqualified. Information required to enable the Procuring Entity to determine if this condition is met shall be provided in for this purpose is be provided in "SECTION III- EVALUATION AND QUALIFICATION CRITERIA, Item 9".

4.11 Pursuant to the eligibility requirements of ITT 4.11, a tenderer is considered a foreign tenderer, if it is registered in Kenya, has less than 51 percent ownership by nationals of Kenya and if it does not subcontract foreign contractors more than 10 percent of the contract price, excluding provisional sums. JVs are considered as foreign tenderers if the individual member firms are registered in Kenya have less than 51 percent ownership by nationals of Kenya. The JV shall not subcontract to foreign firms more than 10 percent of the contract price, excluding provisional sums.

4.12 The Competition Act of Kenya requires that firms wishing to tender as Joint Venture undertakings which may prevent, distort, or lessen competition in provision of services are prohibited unless they are exempt in accordance with the provisions of Section 25 of the Competition Act, 2010. JVs will be required to seek exemptions from the Competition Authority. Exemption shall not be a condition for tender, but it shall be a condition of contract award and signature. A JV tenderer shall be given the opportunity to seek such an exemption as a condition of award and signature of contract. Application for exemption from the Competition Authority of Kenya may be accessed from the website www.cak.go.ke

4.13 Tenderers shall be considered ineligible for procurement if they offer goods, works and production processes with characteristics that have been declared by the relevant national environmental protection agency or by other competent authority as harmful to human beings and to the environment.

4.14 A Kenyan tenderer shall be eligible to tender if it provides evidence of having fulfilled his/her tax obligations by producing a valid tax compliance certificate or tax exemption certificate issued by the Kenya Revenue Authority.

5 Eligible Goods and Services

5.1 The Information Systems to be supplied under the Contract may have their origin in any eligible country.

5.2 For the purposes of this tendering document, the term "Information System" means all:

i. the required information technologies, including all information processing and communications-related hardware, software, supplies, and consumable items that the Supplier is required to supply and install under the Contract, plus all associated documentation, and all other materials and goods to be supplied, installed, integrated, and made operational; and

ii. the related software development, transportation, insurance, installation, customization, integration, commissioning, training, technical support, maintenance, repair, and other services necessary for proper operation of the Information System to be provided by the selected Tenderer and as specified in the Contract.

5.3 For purposes of ITT 5.1 above, "origin" means the place where the goods and services making the Information System are produced in or supplied from. An Information System is deemed to be produced in a certain country when, in the territory of that country, through software development, manufacturing, or substantial and major

assembly or integration of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

5.4 Any goods, works and production processes with characteristics that have been declared by the relevant national environmental protection agency or by other competent authority as harmful to human beings and to the environment shall not be eligible for procurement under this Act.

B. CONTENTS OF TENDERING DOCUMENT

6 Sections of Tendering Document

PART 1 - Tendering Procedures

Section I - Instructions to Tenderers (ITT)

Section II - Tender Data Sheet (TDS)

Section III - Evaluation and Qualification Criteria

Section IV - Tendering Forms

PART 2 - Procuring Entity's Requirements

Section V - Requirements of the Information Systems

Section VI – Procurement of Oracle Implementation Services - Technical Requirements

Section VII – Capacity to Implement and Support the Solution

Section VIII - Project Plan - Implementation Schedule

Section IX - Background and Informational Materials

PART 3 - Contract

Section X - General Conditions of Contract

Section XII - Special Conditions of Contract

Section XIII - Contract Forms

6.1 The Invitation to Tender Notice issued by the Procuring Entity is not part of this tendering document.

6.2 Unless obtained directly from the Procuring Entity, the Procuring Entity is not responsible for the completeness of the document, responses to requests for clarification, the Minutes of the pre-Tender meeting (if any), or Addenda to the tendering document in accordance with ITT 10. In case of any contradiction, documents obtained directly from the Procuring Entity shall prevail.

6.3 The Tenderer is expected to examine all instructions, forms, terms, and specifications in the tendering document and to furnish with its Tender all information or documentation as is required by the tendering document.

7 Site Visit

7.1 The Tenderer, at the Tenderer's own responsibility and risk, is encouraged to visit and examine the Site of the Required Services and its surroundings and obtain all information that may be necessary for preparing the Tender and entering into a contract for the Services. The costs of visiting the Site shall be at the Tenderer's own expense.

8 Pre-Tender Meeting and a pre- arranged pretender visit of the site of the works.

8.1 The Procuring Entity shall specify in the **TDS** if a pre-tender conference will be held, when and where. The Procuring Entity shall also specify in the **TDS** if a pre-arranged pretender visit of the site of the works will be held and when. The Tenderer's designated representative is invited to attend a pre-arranged pretender visit of the site of the works. The purpose of the meeting will be to clarify issues and to answer questions on any matter that may be raised at that stage.

8.2 The Tenderer is requested to submit any questions in writing, to reach the Procuring Entity not later than the period specified in the **TDS** before the meeting.

8.3 Minutes of the pre-Tender meeting and the pre-arranged pre-tender visit of the site of the works, if applicable, including the text of the questions asked by Tenderers and the responses given, together with any responses prepared after the meeting, will be transmitted promptly to all Tenderers who have acquired the Tender Documents in accordance with ITT 6.3. Minutes shall not identify the source of the questions asked.

8.4 The Procuring Entity shall also promptly publish anonymized (*no names*) Minutes of the pre-Tender meeting and the pre-arranged pre-tender visit of the site of the works at the web page identified **in the TDS**. Any modification to the Tender Documents that may become necessary as a result of the pre-Tender meeting shall be made by the Procuring Entity exclusively through the issue of an Addendum pursuant to ITT 10 and not through the minutes of the pre-Tender meeting. Non-attendance at the pre-Tender meeting will not be a cause for disqualification of a Tenderer.

9 Clarification of Tender Documents

9.1 A Tenderer requiring any clarification of the Tender Document shall contact the Procuring Entity in writing at the Procuring Entity's address specified in the TDS or raise its enquiries during the pre-Tender meeting and the pre- arranged pretender visit of the site of the works if provided for in accordance with ITT 8.4. The Procuring Entity will respond in writing to any request for clarification, provided that such request is received no later than the period specified in the TDS prior to the deadline for submission of tenders. The Procuring Entity shall forward copies of its response to all tenderers who have acquired the Tender Documents in accordance with ITT 6.3, including a description of the inquiry but without identifying its source. If so specified in the **TDS**, the Procuring Entity shall also promptly publish its response at the web page identified in the **TDS**. Should the clarification result in changes to the essential elements of the Tender Documents, the Procuring Entity shall amend the Tender Documents appropriately following the procedure under ITT 10.

10 Amendment of Tendering Document

10.1 At any time prior to the deadline for submission of Tenders, the Procuring Entity may amend the Tendering document by issuing addenda.

10.2 Any addendum issued shall be part of the tendering document and shall be communicated in writing to all who have obtained the tendering document from the Procuring Entity in accordance with ITT 6.3. The Procuring Entity shall also promptly publish the addendum on the Procuring Entity's webpage in accordance with ITT 8.1.

10.3 To give prospective Tenderers reasonable time in which to take an addendum into account in preparing their Tenders, the Procuring Entity shall extend, as necessary, the deadline for submission of Tenders, in accordance with ITT 24.2 below.

C. PREPARATION OF TENDERS

11 Cost of Tendering

11.1 The Tenderer shall bear all costs associated with the preparation and submission of its Tender, and the Procuring Entity shall not be responsible or liable for those costs, regardless of the conduct or outcome of the Tendering process.

12 Language of Tender

12.1 The Tender, as well as all correspondence and documents relating to the tender exchanged by the Tenderer and the Procuring Entity, shall be written in the English language**.** Supporting documents and printed literature that are part of the Tender may be in another language provided they are accompanied by an accurate translation of the relevant passages in the English language, in which case, for purposes of interpretation of the Tender, such translation shall govern.

13 Documents Comprising the Tender

13.1 The Tender submitted by the Tenderer shall comprise the following:

a. **Form of Tender** prepared in accordance with ITT 14.
b. **Price Schedules** completed in accordance with ITT 14 and ITT 16.
c. **Tender Security or Tender-Securing Declaration** in accordance with ITT 22.
d. **Alternative Tender:** if permissible, in accordance with ITT 15.

e. **Authorization:** written confirmation authorizing the signatory of the Tender to commit the Tenderer, in accordance with ITT 23.3.

f. **Eligibility of Information System:** documentary evidence established in accordance with ITT 16.1 that the Information System offered by the Tenderer in its Tender or in any alternative Tender, if permitted, are eligible.

g. **Tenderer's Eligibility:** documentary evidence in accordance with ITT 17 establishing the Tenderer's eligibility and qualifications to perform the contract if its Tender is accepted.

h. **Conformity:** documentary evidence established in accordance with ITT 18 that the Information System offered by the Tenderer conforms to the tendering document.

i. **Subcontractors:** list of subcontractors, in accordance with ITT 18.4.

j. **Intellectual Property**: a list of: Intellectual Property as defined in GCC Clause 15.

i) All Software included in the Tender, assigning each item to one of the software categories defined in GCC Clause1.1(C):

a. System, General Purpose, and Application Software; or

b. Standard and Custom Software.

iii. All Custom Materials, as defined in GCCClause1.1(c), included in the Tender.

All Materials not identified as Custom Materials shall be deemed Standard Materials, as defined in GCC Clause 1.1 (c); Re-assignments among the Software and Materials categories, if necessary, will be made during the implementation of the Contract according to GCC Clause 39 (Changes to the Information System); and

k. Any other document required **in the TDS.**

13.2 In addition to the requirements under ITT 13.1, Tenders submitted by a JV shall include a copy of the Joint Venture Agreement entered into by all members indicating at least the parts of the Information System to be executed by the respective members. Alternatively, a Form of intent to execute a Joint Venture Agreement in the information System to be executed by the respective members.

13.1 The Tenderer shall furnish in the Form of Tender information on commissions and gratuities, if any, paid or to be paid to agents or any other party relating to this Tender. The Tenderer shall serialize page so fall tender documents submitted.

14 Form of Tender and Price Schedules

14.1 The Tenderer shall complete the Form of Tender, including the appropriate Price Schedules, using the relevant forms furnished in Section IV, Tendering Forms. The forms must be completed without any alterations to the text, and no substitutes shall be accepted except as provided under ITT 21.3. All blank spaces shall be filled in with the information requested. The Tenderer shall chronologically serialize all pages of the tender documents submitted.

15 Alternative Tenders

15.1 The TDS indicates whether alternative Tenders are allowed. If they are allowed, the **TDS** will also indicate whether they are permitted in accordance with ITT 13.3 or invited in accordance with ITT 13.2 and/or ITT 13.4.

15.2 When alternatives to the Time Schedule are explicitly invited, a statement to that effect will be included **in the TDS**, and the method of evaluating different time schedules will be described in Section III, Evaluation and Qualification Criteria.

15.1 Except as provided under ITT 15.4 below, Tenderers wishing to offer technical alternatives to the Procuring Entity's requirements as described in the tendering document must also provide: (i) a price at which they are prepared to offer an Information System meeting the Procuring Entity's requirements; and (ii) all information necessary for a complete evaluation of the alternatives by the Procuring Entity, including drawings, design calculations, technical specifications, breakdown of prices, and proposed installation methodology and other relevant details. Only the technical alternatives, if any, of the Tenderer with the Best Evaluated Tender conforming to the basic technical requirements shall be considered by the Procuring Entity.

15.4 When Tenderers are invited **in the TDS** to submit alternative technical solutions for specified parts of the system, such parts shall be described in Section V,Procuring Entity's Requirements. Technical alternatives that comply with the performance and technical criteria specified for the Information System shall be considered

by the Procuring Entity on their own merits, pursuant to ITT 35.

16 Documents Establishing the Eligibility of the Information System

16.1 To establish the eligibility of the Information System in accordance with ITT 5, Tenderers shall complete the country-of-origin declarations in the Price Schedule Forms, included in Section IV, Tendering Forms.

17 Documents Establishing the Eligibility and Qualifications of the Tenderer

17..1 To establish its eligibility and qualifications to perform the Contracting accordance with Section III, Evaluation and Qualification Criteria, the Tenderer shall provide the information requested in the corresponding information sheets included in Section IV, Tendering Forms.

17.1 In the event that pre-qualification of potential Tenderers has been undertaken as stated **in the TDS**, only Tenders from pre-qualified Tenderers shall be considered for award of Contract. These qualified Tenderers should submit with their Tenders any information updating their original pre-qualification applications or, alternatively, confirm in their Tenders that the originally submitted pre-qualification information remains essentially correct as of the date of Tender submission.

17.2 Tenderers shall be asked to provide, as part of the data for qualification, such information, including details of ownership, as shall be required to determine whether, according to the classification established by the Procuring Entity, a particular contractor or group of contractors qualifies for a margin of preference. Further the information will enable the Procuring Entity to identify any actual or potential conflict of interest in relation to the procurement and/or contract management processes, or a possibility of collusion between tenderers, and thereby help to prevent any corrupt influence in relation to the procurement process or contract management.

17.3 The purpose of the information described in ITT 15.1 above overrides any claims to confidentiality which a tenderer may have. There can be no circumstances in which it would be justified for a tenderer to keep information relating to its ownership and control confidential where it is tendering to undertake public sector work and receive public sector funds. Thus, confidentiality will not be accepted by the Procuring Entity as a justification for a Tenderer's failure to disclose, or failure to provide required information on its ownership and control.

17.4 The Tenderer shall provide further documentary proof, information, or authorizations that the Procuring Entity may request in relation to ownership and control, any changes to the information which was provided by the tenderer under ITT 6.3. The obligations to require this information shall continue for the duration of the procurement process and contract performance and after completion of the contract, if any change to the information previously provided may reveal a conflict of interest in relation to the award or management of the contract.

17.5 All information provided by the tenderer pursuant to these requirements must be complete, current, and accurate as at the date of provision to the Procuring Entity. In submitting the information required pursuant to these requirements, the Tenderer shall warrant that the information submitted is complete, current, and accurate as at the date of submission to the Procuring Entity.

17.6 If a tenderer fails to submit the information required by these requirements, its tenderer will be rejected. Similarly, if the Procuring Entity is unable, after taking reasonable steps, to verify to a reasonable degree the information submitted by a tenderer pursuant to these requirements, then the tender will be rejected.

17.7 If information submitted by a tenderer pursuant to these requirements, or obtained by the Procuring Entity (whether through its own enquiries, through notification by the public or otherwise), shows any conflict of interest which could materially and improperly benefit the tenderer in relation to the procurement or contract management process, then:

a. If the procurement process is still ongoing, the tenderer will be disqualified from the procurement process,
b. If the contract has been awarded to that tenderer, the contract award will be set aside,
c. the tenderer will be referred to the relevant law enforcement authorities for investigation of whether the tenderer or any other persons have committed any criminal offence.

17.8 If a tenderer submits information pursuant to these requirements that is in complete, inaccurate or out-of-date, or attempts to obstruct the verification process, then the consequences ITT 6.7 will ensue unless the tenderer can show to the reasonable satisfaction of the Procuring Entity that any such act was not material or was due to genuine error which was not attributable to the intentional act, negligence or recklessness of the tenderer.

18 Documents Establishing Conformity of the Information System

18.1 Pursuant to ITT 11.1(h), the Tenderer shall furnish, as part of its Tender documents establishing the conformity to the tendering documents of the Information System that the Tenderer proposes to design, supply and install under the Contract.

18.2 The documentary evidence of conformity of the Information System to the tendering documents including:

a) Preliminary Project Plan describing, among other things, the methods by which the Tenderer will carry out its overall management and coordination responsibilities if awarded the Contract, and the human and other resources the Tenderer proposes to use. The Preliminary Project Plan must also address any other topics **specified in the TDS**. In addition, the Preliminary Project Plan should state the Tenderer's assessment of what it expects the Procuring Entity and any other party involved in the implementation of the Information System to provide during implementation and how the Tenderer proposes to coordinate the activities of all involved parties.

b) Written confirmation that the Tenderer accepts responsibility for the successful integration and inter-operability of all components of the Information System as required by the tendering documents.

c) An item-by-item commentary on the Procuring Entity's Technical Requirements, demonstrating the substantial responsiveness of the Information System offered to those requirements. In demonstrating responsiveness, the Tenderer is encouraged to use the Technical Responsiveness Checklist (or Checklist Format) in the Sample Tendering Forms (Section IV). The commentary shall include explicit cross-references to the relevant pages in the supporting materials included in the tender. Whenever a discrepancy arises between the item-by-item commentary and any catalogs, technical specifications, or other preprinted materials submitted with the tender, the item-by-item commentary shall prevail;

d) Support material (e.g., product literature, white papers, narrative descriptions of technologies and/or technical approaches), as required and appropriate; and

e) Any separate and enforceable contract(s) for Recurrent Cost items which the TDS ITT 17.2 required Tenderers to tender.

18.3 Referencestobrandnamesormodelnumbersornationalorproprietarystandardsdesignatedbytheprocuring Entity in the tendering documents are intended to be descriptive and not restrictive. Except where explicitly prohibited in the **TDS** for specific items or standards, the Tenderer may substitute alternative brand /model names or standards in its tender, provided that it demonstrates to the Procuring Entity's satisfaction that the use of the substitute(s) will result in the Information System being able to perform substantially equivalent to or better than that specified in the Technical Requirements.

18.4 For major items of the Information System as listed by the Procuring Entity in Section III, Evaluation and Qualification Criteria, which the Tenderer intends to purchase or subcontract, the Tenderer shall give details of the name and nationality of the proposed subcontractors, including manufacturers, for each of those items. In addition, the Tenderer shall include in its Tender information establishing compliance with the requirements specified by the Procuring Entity for these items. Quoted rates and prices will be deemed to apply to whichever subcontractor is appointed, and no adjustment of the rates and prices will be permitted.

18.5 The Tenderer shall be responsible for ensuring that any subcontractor proposed complies with the requirements of ITT 4, and that any goods or services to be provided by the subcontractor comply with the requirements of ITT 5 and ITT 16.1.

19 Tender Prices

19.1 All Goods and Services identified in the Supply and Installation Cost Sub-Tables in System Inventory Tables in Section VII, and all other Goods and Services proposed by the Tenderer to fulfill the requirements of the Information System, must be priced separately and summarized in the corresponding cost tables in the Sample Tendering Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below.

19.2 **Unless otherwise specified in the TDS**, the Tenderer must also tender Recurrent Cost Items specified in the Technical Requirements, Recurrent Cost Sub-Table of the System Inventory Tables in Section VII (if any). These must be priced separately and summarized in the corresponding cost table sin the Sample Tendering Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below:

a) **If specified in the TDS,** the Tenderer must also tender separate enforceable contracts for the Recurrent Cost Items not included in the main Contract.

b) prices for Recurrent Costs are all-inclusive of the costs of necessary Goods such as spare parts, software license renewals, labor, etc., needed for the continued and proper operation of the Information System and, if appropriate, of the Tenderer's own allowance for price increases.

c) prices for Recurrent Costs beyond the scope of warranty services to be incurred during the Warranty Period, defined in GCC Clause 29.4 and prices for Recurrent Costs to be incurred during the Post-Warranty Period, defined in SCC Clause 1.1. (e) (xiii), shall be quoted as Service prices on the Recurrent Cost Sub-Table in detail, and on the Recurrent Cost Summary Table in currency totals.

19.3 Unit prices must be quoted at a level of detail appropriate for calculation of any partial deliveries or partial payments under the contract, in accordance with the Implementation Schedule in Section VII), and with GCC and SCC Clause 12 – Terms of Payment. Tenderers may be required to provide a breakdown of any composite or lump-sum items included in the Cost Tables

19.4 The price of items that the Tenderer has left blank in the cost tables provided in the Sample Tender Forms (Section IV) shall be assumed to be included in the price of other items. Items omitted altogether from the cost tables shall be assumed to be omitted from the tender and, provided that the tender is substantially responsive, an adjustment to the tender price will be made during tender evaluation in accordance with ITT 31.3.

19.5 The prices for Goods components of the Information System are to be expressed and shall be defined and governed in accordance with the rules prescribed in the edition of incoterms **specified in the TDS,** as follows:

a) Goods supplied from outside Kenya:
Unless otherwise specified in the TDS, the prices shall be quoted on a CIP (named place of destination) basis, exclusive of all taxes, stamps, duties, levies, and fees imposed in Kenya. The named place of destination and special instructions for the contract of carriage are as specified in the SCC for GCC 1.1(e) (iii)**.** In quoting the price, the Tenderer shall be free to use transportation through carriers registered in any eligible countries. Similarly, the Tenderer may obtain insurance services from any eligible source country.

b) Locally supplied Goods: Unit prices of Goods offered from within Kenya, shall be quoted on an EXW (ex- factory, ex works, ex ware house or off- the-shelf, as applicable) basis, including all customs duties, levies, fees, sales and other taxes incurred until delivery of the Goods, but excluding all VAT or sales and other taxes and duties/fees incurred for the Goods at the time of invoicing or sales transaction, if the Contract is awarded; and

c) Inland transportation.

19.6 Unless otherwise stated in the **TDS,** inland transportation, insurance and related local costs incidental to the delivery of the Goods to the designated Project Sites must be quoted separately as a Service item in accordance with ITT 17.5, whether the Goods are to be supplied locally or from outside Kenya, except when these costs are already included in the price of the Goods, as is, e.g., the case, when ITT 17.5 (a) specifies CIP, and the named places of destination are the Project Sites.

19.7 The price of Services shall be separated into their local and foreign currency components and where appropriate, broken down into unit prices. Prices must include all taxes, duties, levies and fees whatsoever, except only VAT or other indirect taxes, or stamp duties, that may be assessed and/ or apply in Kenyan /to the price of the Services invoiced to the Procuring Entity, if the Contract is awarded.

19.8 Unless otherwise specified in the **TDS**, the prices must include all costs incidental to the performance of the Services, as incurred by the Supplier, such as travel, subsistence, office support, communications, translation, printing of materials, etc. Costs incidental to the delivery of the Services but incurred by the Procuring Entity or its staff, or by third parties, must be included in the price only to the extent such obligations are made explicit in these tendering documents (as, e.g., a requirement for the Tenderer to include the travel and subsistence costs of trainees).

19.9 Unless otherwise specified in the **TDS,** prices quoted by the Tenderer shall be fixed during the Tenderer's performance of the Contract and not subject to increases on any account. Tenders submitted that are subject to price adjustment will be rejected.

20 Currencies of Tender and Payment

20.1 The currency(ies) of the Tender and currencies of payment shall be the same. The Tenderer shall quote in Kenya shillings the portion of the Tender price that corresponds to expenditures incurred in Kenya currency, unless otherwise specified **in the TDS**.

20.2 The Tenderer may express the Tender price in any currency. If the Tenderer wishes to be paid in a combination of amounts in different currencies, it may quote its price accordingly but shall use no more than **two foreign currencies** in addition to Kenyan currency.

21 Period of Validity of Tenders

21.1 Tenders shall remain valid for the period specified **in the TDS** after the Tender submission deadline date prescribed by the Procuring Entity in accordance with ITT 23.1. A Tender valid for a shorter period shall be rejected by the Procuring Entity as non-responsive.

21.2 exceptional circumstances, prior to the expiration of the Tender validity period, the Procuring Entity may request Tenderers to extend the period of validity of their Tenders. The request and the responses shall be made in writing. If a Tender Security is requested in accordance with ITT 20.1, it shall also be extended for thirty days (30) beyond the deadline of the extended validity period. A Tenderer may refuse the request without forfeiting its Tender Security. A Tenderer granting the request shall not be required or permitted to modify its Tender, except as provided in ITT 19.3.

22 Tender Security

22.1 The Tenderer shall furnish as part of its Tender, either a Tender-Securing Declaration or a Tender Security as specified **in the TDS**, in original form and, in the case of a Tender Security, in the amount and currency specified **in the TDS**.

22.2 A Tender-Securing Declaration shall use the form included in Section IV, Tendering Forms.

22.3 If a Tender Security is specified pursuant to ITT 20.1, the tender security shall be a demand guarantee in any of the following forms at the Tenderer's option:

a. cash.
b. a bank guarantee.
c. a guarantee by an insurance company registered and licensed by the Insurance Regulatory Authority listed by the Authority; or
d. a guarantee issued by a financial institution approved and licensed by the Central Bank of Kenya,
e. any other form specified in the **TDS.**

If an unconditional guarantee is issued by a non-bank financial institution located outside Kenya, the issuing non-bank financial institution shall have a correspondent financial institution located in Kenya to make it enforceable unless the Procuring Entity has agreed in writing, prior to Tender submission, that a correspondent financial institution is not required.

22.4 In the case of a bank guarantee, the Tender Security shall be submitted either using the Tender Security Form included in Section IV, Tendering Forms or in another substantially similar format approved by the Procuring Entity prior to Tender submission. I neither case, the form must include the complete name of the Tenderer. The Tender Security shall be valid for thirty days (30) beyond the original validity period of the Tender, or beyond any period of extension if requested under ITT 19.2.

22.5 If a Tender Security or a Tender-Securing Declaration is specified pursuant to ITT 20.1, any Tender not accompanied by a substantially responsive Tender Security or Tender-Securing Declaration shall be rejected by the Procuring Entity as non-responsive.

22.6 The Tender Security shall be returned/release as promptly as possible

a) The procurement proceedings are terminated.
b) The procuring entity determines that none of the submitted tenders is responsive.
c) A bidder declines to extend the tender validity.
d) Once the successful Tenderer has signed the Contract and furnished the required Performance Security.

22.7 The Tender Security may be forfeited, or the Tender-Securing Declaration executed:

a) if a Tenderer withdraws its Tender during the period of Tender validity specified by the Tenderer on the Form of Tender; or
b) if the successful Tenderer fails to**:**

i) sign the Contract in accordance with ITT 47; or
ii) furnish performance security in accordance with ITT 48.

22.8 Where the Tender-Securing Declaration is executed the Procuring Entity will recommend to the PPRA to debar the Tenderer from participating in public procurement as provided in the law.

22.9 The Tender Security or the Tender-Securing Declaration of a JV shall be in the name of the JV that submits the tender. If the JV has not been legally constituted into a legally enforceable JV at the time of Tendering, the Tender Security or the Tender-Securing Declaration shall be in the names of all future members as named in the Form of intent referred to in ITT 4.1 and ITT 11.2.

22.10 A tenderer shall not issue a tender security to guarantee itself.

23 Format and Signing of Tender

23.1 The Tenderer shall prepare one original of the documents comprising the Tender as described in ITT 11 and clearly mark it "ORIGINAL." Alternative Tenders, if permitted in accordance with ITT 13, shall be clearly marked "ALTERNATIVE". In addition, the Tenderer shall submit copies of the Tender, in the number specified **in the TDS** and clearly mark them "COPY." In the event of any discrepancy between the original and the copies, the original shall prevail.

23.2 Tenderers shall mark as "CONFIDENTIAL" information in their Tenders which is confidential to their business. This may include proprietary information, trade secrets, or commercial or financially sensitive information.

23.3 The original and all copies of the Tender shall be typed or written in indelible ink and shall be signed by a person duly authorized to sign on behalf of the Tenderer. This authorization shall consist of a written confirmation as specified **in the TDS** and shall be attached to the Tender. The name and position held by each person signing the authorization must be typed or printed below the signature. All pages of the Tender where entries or amendments have been made shall be signed or initialed by the person signing the Tender.

23.4 In case the Tenderer is a JV, the Tender shall be signed by an authorized representative of the JV on behalf of the JV, and so as to be legally binding on all the members as evidenced by a power of attorney signed by their legally authorized representatives.

23.5 Any interlineations, erasures, or overwriting shall be valid only if they are signed or initialed by the person signing the Tender.

D. SUBMISSION AND OPENING OF TENDERS

24 Submission, Sealing and Marking of Tenders

24.1 The Tenderer shall deliver the Tender in a single, sealed envelope (one (1) envelope process). Within the single envelope the Tenderer shall place the following separate, sealed envelopes:
a) In an envelope marked "ORIGINAL", all documents comprising the Tender, as described in ITT 11; and
b) In an envelope marked "COPIES", all required copies of the Tender; and,
c) If alternative Tenders are permitted in accordance with ITT 13, and if relevant:
i) In an envelope marked "ORIGINAL – ALTERNATIVE TENDER", the alternative Tender; and
ii) in the envelope marked "COPIES – ALTERNATIVE TENDER" all required copies of the alternative Tender.

24.2 The inner envelopes shall:
a) Bear the name and address of the Tenderer.
b) Be addressed to the Procuring Entity/ Employer in accordance with ITT 23.1.
c) Bear the specific identification of this Tendering process specified in accordance with ITT 1.1; and
d) Bear a warning not to open before the time and date for Tender opening.

The outer envelopes shall:

e) Be addressed to the Procuring Entity/ Employer in accordance with ITT 23.1.
f) Bear the specific identification of this Tendering process specified in accordance with ITT 1.1; and bear a warning not to open before the time and date for Tender opening.

24.3 If all envelopes are not sealed and marked as required, the Procuring Entity will assume no responsibility for the misplacement or premature opening of the Tender. Tenders that are misplaced or opened prematurely will not be accepted.

25 Deadline for Submission of Tenders

25.1 Tenders must be received by the Procuring Entity at the address and no later than the date and time indicated **in the TDS**. When so specified **in the TDS**, Tenderers shall have the option of submitting their Tenders electronically. Tenderers submitting Tenders electronically shall follow the electronic Tender submission procedures specified **in the TDS**.

25.2 The Procuring Entity may, at its discretion, extend this deadline for submission of Tenders by amending the tendering documents in accordance with ITT 8, in which case all rights and obligations of the Procuring Entity and Tenderers will thereafter be subject to the deadline as extended.

26 Late Tenders

26.1 The Procuring Entity shall not consider any Tender that arrives after the deadline for submission of Tenders, in accordance with ITT 23. Any Tender received by the Procuring Entity after the deadline for submission of Tenders shall be declared late, rejected, and returned unopened to the Tenderer.

27 Withdrawal, Substitution, and Modification of Tenders

27.1 A Tenderer may withdraw, substitute, or modify its Tender after it has been submitted by sending a written notice, duly signed by an authorized representative, and shall include a copy of the authorization in accordance with ITT 21.3, (except that withdrawal notices do not require copies). The corresponding substitution or modification of the Tender must accompany the respective written notice. All notices must be:

a) prepared and submitted in accordance with ITT 21 and ITT 22 (except that withdrawals notices do not require copies), and in addition, the respective envelopes shall be clearly marked "WITHDRAWAL," "SUBSTITUTION," "MODIFICATION;" and
b) received by the Procuring Entity prior to the deadline prescribed for submission of Tenders, in accordance with ITT23.

27.2 Tenders requested to be withdrawn in accordance with ITT 25.1 shall be returned unopened to the Tenderers.

27.3 No Tender may be withdrawn, substituted, or modified in the interval between the deadline for submission of Tender sand the expiration of the period of Tender validity specified by the Tenderer on the Form of Tender or any extension thereof.

28 Tender Opening

28.1 Except as in the cases specified in ITT 24 and ITT 25.2, the Procuring Entity shall conduct the Tender opening in public, in the presence of Tenderers' designated representatives who chooses to attend, and at the address, date and time specified **in the TDS**. Any specific electronic Tender opening procedures required if electronic tendering is permitted in accordance with ITT 23.1, shall be as specified **in the TDS**.

28.2 First, envelopes marked "WITHDRAWAL" shall be opened and read out and the envelopes with the corresponding Tender shall not be opened but returned to the Tenderer. No Tender withdrawal shall be permitted unless the corresponding withdrawal notice contains a valid authorization to request the withdrawal and is read out at Tender opening.

28.3 Next, envelopes marked "SUBSTITUTION" shall be opened and read out and exchanged with the corresponding Tender being substituted, and the substituted Tender shall not be opened, but returned to the Tenderer. No Tender substitution shall be permitted unless the corresponding substitution notice contains a valid authorization to request the substitution and is read out at Tender opening.

28.4 Envelopes marked "Modification" shall be opened and read out with the corresponding Tender. No Tender modification shall be permitted unless the corresponding modification notice contains a valid authorization to request the modification and is read out at Tender opening. Only Tenders that are opened and read out at Tender opening shall be considered further.

28.5 Next, all remaining envelopes shall be opened one at a time, reading out: the name of the Tenderer and the Tender Price(s), including any discounts and alternative Tenders, and indicating whether there is a modification; the presence or absence of a Tender Security or Tender-Securing Declaration; and any other details as the Procuring Entity may consider appropriate.

28.6 Only Tenders, alternative Tenders and discounts that are opened and read out at Tender opening shall be considered further in the evaluation. The Form of Tender and the Price Schedules are to be initialed by representatives of the Procuring Entity attending Tender opening in the manner specified **in the TDS**.

28.7 The Procuring Entity shall neither discuss the merits of any Tender nor reject any Tender (except for late Tenders, in accordance with ITT 24.1).

28.8 The Procuring Entity shall prepare a record of the Tender opening that shall include, as a minimum:
a) The name of the Tenderer and whether there is a withdrawal, substitution, or modification.
b) The Tender Price, per lot if applicable, includes any discounts.
c) Any alternative Tenders; and
d) The presence or absence of a Tender Security or a Tender-Securing Declaration.

28.9 The Tenderers' representatives who are present shall be requested to sign the minutes. The omission of a Tenderer's signature on the minutes shall not invalidate the contents and effect of the minutes. A copy of the tender opening register shall be distributed to all Tenderers upon request.

E. Evaluation and Comparison of Tenders

29 Confidentiality

29.1 Information relating to the evaluation of Tenders and recommendation of contract award, shall not be disclosed to Tenderers or any other persons not officially concerned with the Tendering process until the Notification of Intention to Award the Contract is transmitted to all Tenderers in accordance with ITT 42.

29.2 Any effort by a Tenderer to influence the Procuring Entity in the evaluation of the Tenders or Contract award decisions may result in the rejection of its Tender.

29.3 Not with standing ITT 27.2, from the time of Tender opening to the time of Contract award, if any Tenderer wishes to contact the Procuring Entity on any matter related to the Tendering process, it should do so in writing.

30 Clarification of Tenders

30.1 To assist in the examination, evaluation, and comparison of the Tenders, and qualification of the Tenderers, the Procuring Entity may, at its discretion, ask any Tenderer for a clarification of its Tender. Any clarification submitted by a Tenderer that is not in response to a request by the Procuring Entity shall not be considered. The Procuring Entity's request for clarification and the response shall be in writing. No change in the prices or substance of the Tender shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the Procuring Entity in the evaluation of the Tenders, in accordance with ITT32.

30.2 If a Tenderer does not provide clarifications of its Tender by the date and time set in the Procuring Entity's request for clarification, its Tender may be rejected.

31 Deviations, Reservations, and Omissions

31.1 During the evaluation of Tenders, the following definitions apply:
a) "Deviation" is a departure from the requirements specified in the tendering document.
b) "Reservation" is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the tendering document; and
c) "Omission" is the failure to submit part, or all the information or documentation required in the tendering document.

32 Determination of Responsiveness

32.1 The Procuring Entity's determination of a Tender's responsiveness is to be based on the contents of the Tender itself, as defined in ITT 11.

32.2 A substantially responsive Tender is one that meets the requirements of the tendering document without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that.

a) If accepted, would:
   i) Affect in any substantial way the scope, quality, or performance of the Support and Maintenance Services specified in the Contract; or
   ii) Limit in any substantial way, in consistent with the tendering document, the Procuring Entity's rights or the Tenderer's obligations under the proposed Contract; or
b) if rectified, would unfairly affect the competitive position of other Tenderers presenting substantially responsive Tenders.

32.3 The Procuring Entity shall examine the technical aspects of the Tender in particular, to confirm that all requirements of Section V, Procuring Entity's Requirements have been met without any material deviation, reservation, or omission.

32.4 To be considered for Contract award, Tenderers must have submitted Tenders:

a) for which detailed Tender evaluation using the same standards for compliance determination as listed in ITT 29 and ITT 30.3 confirms that the Tenders are commercially and technically responsive, and include the hardware, Software, related equipment, products, Materials, and other Goods and Services components of the Information System in substantially the full required quantities for the entire Information System or, if allowed in the TDS ITT 35.8, the individual Subsystem, lot or slice Tender on; and are deemed by the Procuring Entity as commercially and technically responsive; and
b) that offer Information Technologies that are proven to perform up to the standards promised in the tender by having successfully passed the performance, benchmark, and/or functionality tests the Procuring Entity may require, pursuant to ITT 39.3.

33 Non-material non-conformities

33.1 Provided that a Tender is substantially responsive, the Procuring Entity may waive any nonconformity in the Tender that does not constitute a material deviation, reservation, or omission.

33.2 Provided that a Tender is substantially responsive, the Procuring Entity may request that the Tenderer submit the necessary information or documentation, within a reasonable period of time, to rectify nonmaterial non-conformities in the Tender related to documentation requirements. Requesting information or documentation on such non-conformities shall not be related to any aspect of the price of the Tender. Failure of the Tenderer to comply with the request may result in the rejection of its Tender.

33.3 Provided that a Tender is substantially responsive, the Procuring Entity shall rectify quantifiable nonmaterial non-conformities related to the Tender Price. To this effect, the Tender Price shall be adjusted, for comparison purposes only, to reflect the price of a missing or non-conforming item or component in the manner specified **in the TDS**.

34 Correction of Arithmetical Errors

34.1 The tender sum as submitted and read out during the tender opening shall be absolute and final and shall not be the subject of correction, adjustment, or amendment in any way by any person or entity.

34.2 Provided that the Tender is substantially responsive, the Procuring Entity shall handle errors on the following basis:

a) Any error detected if considered a major deviation that affects the substance of the tender, shall lead to disqualification of the tender as non-responsive.
b) Any errors in the submitted tender a rising from a miscalculation of unit price, quantity, subtotal, and total bid price shall be considered as a major deviation that affects the substance of the tender and shall lead to disqualification of the tender as non-responsive. and
c) If there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail.

35 Conversion to Single Currency

35.1 For evaluation and comparison purposes, the currency(ies) of the Tender shall be converted into a single currency as specified **in the TDS**.

36 Margin of Preference and Reservations

36.1 A margin of preference on local contractors may be allowed only when the contract is open to international competitive tendering where foreign contractors are expected to participate in the tendering process and where the contract exceeds the value/ threshold specified in the Regulations.

36.2 A margin of preference shall not be allowed unless it is specified in the **TDS**.

36.3 Contracts procured on basis of international competitive tendering shall not be subject to reservations exclusive to specific groups as provided in ITT 34.4.

36.4 Where it is intended to reserve a contract to a specific group of businesses (these groups are Small and Medium Enterprises, Women Enterprises, Youth Enterprises and Enterprises of persons living with disability, as the case maybe), and who are appropriately registered as such by the authority to be specified in the **TDS**, a procuring entity shall ensure that the invitation to tender specifically indicates in the **TDS** that only businesses or firms belonging to the specified group are eligible to tender. No tender shall be reserved to more than one group. If not so stated in the Invitation to Tender and in the Tender documents, the invitation to tender will be open to all interested tenderers.

37 Evaluation of Tenders

37.1 The Procuring Entity shall use the criteria and methodologies listed in this ITT and Section III, Evaluation and Qualification criteria. No other evaluation criteria or methodologies shall be permitted. By applying the criteria and methodologies the Procuring Entity shall determine the Best Evaluated Tender.

37.2 To evaluate a Tender, the Procuring Entity shall consider the following:

a) Price adjustment due to discounts offered in accordance with ITT 14.4.
b) converting the amount resulting from applying (a) and (b) above, if relevant, to a single currency in accordance with ITT 33.
c) price adjustment due to quantifiable nonmaterial non-conformities in accordance with ITT 31.3; and
d) any additional evaluation factors specified **in the TDS** and Section III, Evaluation and Qualification Criteria.

38 Preliminary Examination

38.1 The Procuring Entity will examine the tenders, to determine whether they have been properly signed, whether required sureties have been furnished, whether any computational errors have been made, whether required sure ties have been furnished and are substantially complete (e.g., not missing key parts of the tender or silent on excessively large portions of the Technical Requirements). In the case where a pre-qualification process was undertaken for the Contract (s) for which these tendering documents have been issued, the Procuring Entity will ensure that each tender is from a pre-qualified Tenderer and, in the case of a Joint Venture, that partners and structure of the Joint Venture are unchanged from those in the pre-qualification.

39 Technical Evaluation

39.1 The Procuring Entity will examine the information supplied by the Tenderers Pursuant to ITT 11 and ITT 16, and in response to other requirements in the Tendering document, considering the following factors:

a) Overall completeness and compliance with the Technical Requirements; and deviations from the Technical Requirements.
b) suitability of the Information System offered in relation to the conditions prevailing at the site; and the suitability of the implementation and other services proposed, as described in the Preliminary Project Plan included in the tender.
c) achievement of specified performance criteria by the Information System.
d) compliance with the time schedule called for by the Implementation Schedule and any alternative time schedules offered by Tenderers, as evidenced by a milestone schedule provided in the Preliminary Project Plan included in the tender.
e) type, quantity, quality, and long-term availability of maintenance services and of any critical consumable items necessary for the operation of the Information System.

f) any other relevant technical factors that the Procuring Entity deems necessary or prudent to take into consideration.
g) any proposed deviations in the tender to the contractual and technical provisions stipulated in the tendering documents.

39.2 The Procuring Entity's evaluation of tenders will consider technical factors, in addition to cost factors. The Technical Evaluation will be conducted following the Criteria specified in Section III, Evaluation and Qualification Criteria, which permits a comprehensive assessment of the technical merits of each Tender. All tenders that fail to pass this evaluation will be considered non-responsive and will not be evaluated further.

39.3 Where alternative technical solutions have been allowed in accordance with ITT 13, and offered by the Tenderer, the Procuring Entity will make a similar evaluation of the alternatives. Where alternatives have not been allowed but have been offered, they shall be ignored.

39.4 Where the tender involves multiple lots or contracts, the tenderer will be allowed to tender for one or more lots (contracts). Each lot or contract will be evaluated in accordance with ITT 35.2. The methodology to determine the lowest evaluated tenderer or tenderers based one lot (contract) or based on a combination of lots (contracts), will be specified in Section III, Evaluation and Qualification Criteria. In the case of multiple lots or contracts, tenderer will be required to prepare the Eligibility and Qualification Criteria Form for each Lot.

40 Financial/ Economic Evaluation

40.1 To evaluate a Tender, the Procuring Entity shall consider the following:
a) price adjustment due to unconditional discounts offered in accordance with ITT 26.8; excluding provisional sums and contingencies, if any, but including Day work items, were priced competitively.
b) Price adjustment due to quantifiable nonmaterial non-conformities in accordance with ITT 31.3.
c) converting the amount resulting from applying (a) to (c) above, if relevant, to a single currency in accordance with ITT 33; and
d) the evaluation factors indicated in Section III, Evaluation and Qualification Criteria.
If price adjustment is allowed in accordance with ITT 17.9, the estimated effect of the price adjustment provisions of the Conditions of Contract, applied over the period of execution of the Contract, shall not be considered in Tender evaluation.

40.1 The Procuring Entity will evaluate and compare the Tenders that have been determined to be substantially responsive, pursuant to ITT 35.4. The evaluation will be performed assuming either that:
a) The Contract will be awarded to the Lowest Evaluated Tender for the entire Information System; or
b) if specified **in the TDS**, Contracts will be awarded to the Tenderers for each individual Subsystem, lot, or slice if so defined in the Technical Requirements whose Tenders result in the Lowest Evaluated Tender/ Tenders for the entire System.

In the latter case, discounts that are conditional on the award of more than one Subsystem, lot, or slice may be offered in Tenders. Such discounts will be considered in the evaluation of tenders as specified **in the TDS**.

41 Comparison of Tenders

41.1 The Procuring Entity shall compare all substantially responsive Tenders in accordance with ITT 35.6 to determine the lowest evaluated cost.

42 Abnormally Low Tenders and Abnormally High Tenders

42.1 An Abnormally Low Tender is one where the Tender price in combination with other constituent elements of the Tender appears unreasonably low to the extent that the Tender price raises material concerns as to the capability of the Tenderer to perform the Contract for the offered Tender Price or that genuine competition between Tenderers is compromised.

42.2 In the event of identification of a potentially Abnormally Low Tender, the Procuring Entity shall seek written clarifications from the Tenderer, including detailed price analyses of its Tender price in relation to the subject matter of the contract, scope, proposed methodology, schedule, allocation of risks and responsibilities and any other requirements of the tendering document.

42.3 After evaluation of the price analyses, in the event that the Procuring Entity determines that the Tenderer has failed to demonstrate its capability to perform the Contract for the offered Tender Price, the Procuring Entity shall reject the Tender.

Abnormally High Tenders

42.4 An abnormally high tender price is one where the tender price, in combination with other constituent elements of the Tender, appears unreasonably too high to the extent that the Procuring Entity is concerned that it (the Procuring Entity) may not be getting value for money, or it may be paying too high a price for the contract compared with market prices or that genuine competition between Tenderers is compromised.

42.5 In case of an abnormally high price, the Procuring Entity shall make a survey of the market prices, check if the estimated cost of the contract is correct and review the Tender Documents to check if the specifications, scope of work and conditions of contract are contributory to the abnormally high tenders. The Procuring Entity may also seek written clarification from the tenderer on the reason for the high tender price. The Procuring Entity shall proceed as follows:

a. If the tender price is abnormally high based on wrong estimated cost of the contract, the Procuring Entity may accept or not accept the tender depending on the Procuring Entity's budget considerations.

b. If specifications, scope of work and/ or conditions of contract are contributory to the abnormally high tender prices, the Procuring Entity shall reject all tenders and may retender for the contract based on revised estimates, specifications, scope of work and conditions of contract, as the case may be.

42.6 If the Procuring Entity determines that the Tender Price is abnormally too high because genuine competition between tenderers is compromised (*often due to collusion, corruption or other manipulations*), the Procuring Entity shall reject all Tenders and shall institute or cause competent Government Agencies to institute an investigation on the cause of the compromise, before retendering.

43 Unbalanced or Front-Loaded Tenders

43.1 If the Tender that is evaluated as the lowest evaluated cost is, in the Procuring Entity's opinion, seriously unbalanced or front loaded the Procuring Entity may require the Tenderer to provide written clarifications. Clarifications may include detailed price analyses to demonstrate the consistency of the Tender prices with the scope of information systems, installations, proposed methodology, schedule and any other requirements of the tendering document.

43.2 After the evaluation of the information and detailed price analyses presented by the Tenderer, the Procuring Entity may: -

a) Accept the Tender; or
b) If appropriate, require that the total amount of the Performance Security be increased, at the expense of the Tenderer, to a level not exceeding twenty percent (20%) of the Contract Price; or
c) Reject the Tender.

44 Eligibility and Qualification of the Tenderer

44.1 The Procuring Entity shall determine to its satisfaction whether the Tenderer that is selected as having submitted the lowest evaluated and substantially responsive Tender is eligible and meets the qualifying criteria specified in Section III, Evaluation and Qualification Criteria.

44.2 The determination shall be based upon an examination of the documentary evidence of the Tenderer's qualifications submitted by the Tenderer, pursuant to ITT 15.

44.3 Unless otherwise specified in the **TDS,** the Procuring Entity will NOT carry out tests at the time of post-qualification, to determine that the performance or functionality of the Information System offered meets those stated in the Technical Requirements. However, if so specified in the **TDS** the Procuring Entity may carry out such tests as detailed in the **TDS**.

44.4 An affirmative determination shall be a prerequisite for award of the Contract to the Tenderer. A negative determination shall result in disqualification of the Tender, in which event the Procuring Entity shall proceed to the next lowest evaluated cost or best evaluated Tender, as the case may be, to make a similar determination of that Tenderer's qualifications to perform satisfactorily.

44.5 The capabilities of the manufacturers and subcontractors proposed by the Tenderer that is determined to have offered the Best Evaluated Tender for identified major items of supply or services will also be evaluated for acceptability in accordance with Section III, Evaluation and Qualification Criteria. Their participation should be confirmed with a Form of intent between the parties, as needed. Should a manufacturer or subcontractor be determined to be unacceptable, the Tender will not be rejected, but the Tenderer will be required to substitute

an acceptable manufacturer or subcontractor without any change to the Tender price. Prior to signing the Contract, the corresponding Appendix to the Contract Agreement shall be completed, listing the approved manufacturers or subcontractors for each item concerned.

44.6 Foreign tenderers are required to source at least forty (40%) percent of their contract inputs (in supplies, subcontracts and labor) from national suppliers and contractors. To this end, a foreign tenderer shall provide in its tender documentary evidence that this requirement is met. Foreign tenderers not meeting this criterion will be automatically disqualified. Information required to enable the Procuring Entity determine if this condition is met shall be provided in for this purpose is be provided in *"SECTION III- EVALUATION AND QUALIFICATION CRITERIA.*

45 Procuring Entity's Right to Accept Any Tender, and to Reject Any or All Tenders

45.1 The Procuring Entity reserves the right to accept or reject any Tender, and to annul the Tendering process and reject all Tenders at any time prior to contract award, without there by incurring any liability to Tenderers. In case of annulment, all Tenders submitted and specifically, Tender securities, shall be promptly returned to the Tenderers.

F. AWARD OF CONTRACT

46 Award Criteria

46.1 Subject to ITT 40, the Procuring Entity shall award the Contract to the successful tenderer whose tender has been determined to be the Lowest/ best Evaluated Tender. The determination of the lowest/ Best Evaluated Tender will be made in accordance to one of the two options as defined in the **TDS**. The methodology options are:

The Procuring Entity shall award the Contract to the successful tenderer whose tender has been determined to be the Lowest Evaluated Tender

a) When **rated criteria are used**: The Tenderer that meets the qualification criteria and whose Tender:
   i) Is substantially responsive; and
   ii) Is the Best Evaluated Tender (i.e., the Tender with the highest combined technical/ quality/ price score); or

b) When **rated criteria are not used**: The Tenderer that meets the qualification criteria and whose Tender has been determined to be:
   i) Most responsive to the tendering document; and
   ii) The lowest evaluated cost.

47 Procuring Entity's Right to Vary Quantities at Time of Award

47.1 The Procuring Entity reserves the right at the time of Contract award to increase or decrease, by the percentage (s) for items as indicated **in the TDS.**

48 Notice of Intention to enter into a Contract/ Notification of award

48.1 Upon award of the contract and prior to the expiry of the Tender Validity Period the Procuring Entity shall issue a Notification of Intention to Enter into a Contract/ Notification of award to all tenderers which shall contain, at a minimum, the following information:

a) The name and address of the Tenderer submitting the successful tender.
b) The Contract price of the successful tender.
c) a statement of the reason(s) the tender of the unsuccessful tenderer to whom the letter is addressed was unsuccessful unless the price information in (c) above already reveals the reason.
d) the expiry date of the Standstill Period; and
e) instructions on how to request a debriefing and/ or submit a complaint during the standstill period.

49 Standstill Period

49.1 The Contract shall not be signed earlier than the expiry of a Standstill Period of 14 days to allow any dissatisfied tenderer to launch a complaint. Where only one Tender is submitted, the Standstill Period shall not apply.

49.2 Where a Standstill Period applies, it shall commence when the Procuring Entity has transmitted to each Tenderer the Notification of Intention to Enter into a Contract with the successful Tenderer.

50 Debriefing by the Procuring Entity

50.1 On receipt of the Procuring Entity's Notification of Intention to Enter into a Contract referred to in ITT 43, an unsuccessful tenderer may make a written request to the Procuring Entity for a debriefing on specific issues or concerns regarding their tender. The Procuring Entity shall provide the debriefing within five days of receipt of the request.

50.2 Debriefings of unsuccessful Tenderers may be done in writing or verbally. The Tenderer shall bear its own costs of attending such a debriefing meeting.

51 Letter of Award

51.1 Prior to the expiry of the Tender Validity Period and upon expiry of the Standstill Period specified in ITT44.1, upon addressing a complaint that has been filed within the Standstill Period, the Procuring Entity shall transmit the Letter of Award to the successful Tenderer. The letter of award shall request the successful tenderer to furnish the Performance Security within 21days of the date of the letter.

52 Signing of Contract

52.1 Upon the expiry of the fourteen days of the Notification of Intention to enter in to contract and upon the parties meeting their respective statutory requirements, the Procuring Entity shall send the successful Tenderer the Contract Agreement.

52.2 Within fourteen (14) days of receipt of the Contract Agreement, the successful Tenderer shall sign, date, and return it to the Procuring Entity.

52.3 The written contract shall be entered into within the period specified in the notification of award and before expiry of the tender validity period.

52.4 Notwithstanding ITT 47.2 above, in case signing of the Contract Agreement is prevented by any export restrictions attributable to the Procuring Entity, to Kenya, or to the use of the Information System to be supplied, where such export restrictions arise from trade regulations from a country supplying those Information System, the Tenderer shall not be bound by its Tender, provided that the Tenderer can demonstrate that signing of the Contract Agreement has not been prevented by any lack of diligence on the part of the Tenderer in completing any formalities, including applying for permits, authorizations and licenses necessary for the export of the Information System under the terms of the Contract.

53 Performance Security

53.1 Within twenty-one (21) days of the receipt of the Form of Acceptance from the Procuring Entity, the successful Tenderer shall furnish the performance security in accordance with the General Conditions, subject to ITT38.2 (b), using for that purpose the Performance Security Form included in Section X, Contract Forms, or another form acceptable to the Procuring Entity. If the Performance Security furnished by the successful Tenderer is in the form of a bond, it shall be issued by a bonding or insurance company that has been determined by the successful Tenderer to be acceptable to the Procuring Entity. A foreign institution providing a Performance Security shall have a correspondent financial institution located in Kenya.

53.2 Failure of the successful Tenderer to submit the above-mentioned Performance Security or sign the Contract shall constitute sufficient grounds for the annulment of the award and forfeiture of the Tender Security. In that event the Procuring Entity may award the Contract to the Tenderer offering the next Best Evaluated Tender.

54. Publication of Procurement Contract

Within fourteen days after signing the contract, the Procuring Entity shall publish the awarded contract at its notice boards and websites: and on the Website of the Authority. At the minimum, the notice shall contain the following information:

a) Name and address of the Procuring Entity.
b) Name and reference number of the contract being awarded, a summary of its scope and the selection method used.
c) The name of the successful Tenderer, the final total contract price, the contract duration.
d) Dates of signature, commencement, and completion of contract.
e) Names of all Tenderers that submitted Tenders, and their Tender prices as read out at Tender opening.

55. Adjudicator

55.1. Unless **the TDS** states otherwise, the Procuring Entity proposes that the person named **in the TDS** be appointed as Adjudicator under the Contract to assume the role of informal Contract dispute mediator, as described in GCC Clause 43.1. In this case, a résumé of the named person is attached to the TDS. The proposed hourly fee for the Adjudicator is specified in the TDS. The expenses that would be considered reimbursable to the Adjudicator are also specified **in the TDS**. If a Tenderer does not accept the Adjudicator proposed by the Procuring Entity, it should state its non-acceptance in its Tender Form and make a counter proposal of an Adjudicator and an hourly fee, attaching résumé of the alternative. If the successful Tenderer and the Adjudicator nominated **in the TDS** happen to be from the same country, and this is not Kenya too, the Procuring Entity reserves the right to cancel the Adjudicator nominated **in the TDS** and propose a new one. If by the day the Contract is signed, the Procuring Entity and the successful Tenderer have not agreed on the appointment of the Adjudicator, the Adjudicator shall be appointed, at the request of either party, by the Appointing Authority specified in the SCC clause relating to GCC Clause 43.1.4, or if no Appointing Authority is specified there, the Contract will be implemented without an Adjudicator.

56. Procurement Related Complaints and Administrative Review

51.1The procedures for making a Procurement-related Complaint are as specified in the **TDS.**

51.2A request for administrative review shall be made in the form provided under contract forms.

SECTION II - TENDER DATA SHEET (TDS)

The following specific data for the Information System to be procured shall complement, supplement, or amend the provisions in the Instructions to Tenderers (ITT). Whenever there is a conflict, the provisions here in shall prevail over those in ITT.

Reference to ITC Clause	PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS
	A. General
ITT 1.1	The reference number of the Invitation to Tender (ITT) is: **Tender No. CBK/028/2026-2027** The Procuring Entity is**: Central Bank of Kenya** The name of the ITT is **Supply, Delivery, Installation, training and Commissioning of Integrated Security System for Central Bank of Kenya**
ITT 2.3 (a)	The name of the Project is: **Supply, Installation, testing, training and Commissioning of Integrated Security System for Central Bank of Kenya (Tender Reference No. CBK/028/2026-2027)** Electronic-procurement system shall be used to manage any aspects of the Procurement process: **Not Applicable**
ITT 3.3	The firms (if any) that provided consulting services for the contract being tendered for are **Not Applicable**
ITT 4.1	The maximum number of members in the Joint Venture (JV) where applicable shall be: - **Two**
ITT 4.9	The Procuring Entity requires tenderers to provide manufacturer's authorization form from the Original Equipment Manufacturer from OEM.
	B. Tendering Document
ITT 8.1	For **Tender submission purposes** only, the Procuring Entity's address is: **Central Bank of Kenya,** Head Office in Nairobi, Ground Floor, Haile Selassie Avenue, **Green Tender Box No. 3** at the main entrance, P. O. Box 60000 – 00200, Nairobi Attention: Head of Procurement Function/ Deputy Director, Procurement Division Physical Address, Nairobi, Haile Selassie Avenue, CBK Building, Ground Floor **The deadline for Tender submission is 5th October 2026 at 10:30am** Tenderers ***shall not*** have the option of submitting their Tenders electronically. The electronic Tendering submission procedures shall be ***N/A*** Requests for clarification should be received by the Procuring Entity no later than: **Four (4) days before tender closing/opening day/date.**
ITT 8.2	The tender has been published on www.centralbank.go.ke and www.tenders.go.ke
ITT 8.4	A pre-bid meeting will be held on **24th September 2026** at 10.30 a.m. virtually or physically at 11th floor Extelcom house, Procurement conference room. Interested bidders intending to join the meeting to share their details and for online are requested to share their email addresses using Supplies@centralbank.go.ke and a link to the meeting will be shared.
ITT 9.1	The Procuring Entity shall publish its response at the website www.centralbank.go.ke and www.tenders.go.ke
	C. Preparation of Tenders
ITT 13.1 (k)	The Tenderer shall submit with its Tender the following additional documents: **As indicated in the evaluation criteria**
ITT 15.1	Alternative Tenders are not permitted.
ITT 15.2	Alternatives to the Time Schedule **shall not** be permitted. If alternatives to the Time Schedule are permitted, the evaluation method will be as specified in Section III, Evaluation and Qualification Criteria. **Not Applicable for this tender**
ITT 15.4	Alternative technical solutions shall be permitted for the following parts of the Information System: N/A as further detailed in the Specification. If alternative technical solutions

Reference to ITC Clause	PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS
	are permitted, the evaluation method will be as specified in Section III, Evaluation and Qualification Criteria. **Not Applicable for this tender**
ITT 18.2 (a)	In addition to the topics described in ITT Clause 16.2 (a), the Preliminary Project Plan must address the following topics: [*modify as appropriate]:* (i) ***Project Organization and Management Sub-Plan, including management authorities, responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format).*** (ii) ***Implementation Sub-Plan.*** (iii) ***Training Sub-Plan.*** (iv) ***Testing and Quality Assurance Sub-Plan.*** (v) ***Warranty Defect Repair and Technical Support Service Sub-Plan***
ITT 19.2	The Tenderer *must* tender Recurrent Cost Items
ITT 19.5	The Incoterms edition is: ***2020***
ITT 19.5 (a)	Named place of destination is: **__ Central Bank of Kenya Head Office, Nairobi**
ITT 19.6	Named place of final destination (or Project site) is: As will be indicated in the contract
ITT 19.7	**TAX, DUTIES/ LEVIES** The price quoted must include all associated costs and taxes. 2. Capacity Building Levy. The tenderers are hereby notified of PPRA circular No. 01/2024 dated 30th August 2024 and Legal notice No. 206 of 6th November 2023 which introduces a Capacity Building Levy to be paid/borne by a supplier on all procurement contracts signed between the supplier and the procuring entity at a rate of 0.03% of the value of contract exclusive of applicable taxes. The procuring entity shall deduct and remit the levy to PPRA
ITT 19.9	The prices quoted by the Tenderer ***shall not be*** subject to adjustment during the performance of the Contract.
ITT 20.1	The Tenderer ***is*** required to quote in **Kenya Shillings (Kes.)**
ITT 21.1	The Tender validity period shall be **140 days.**
ITT 22.1	Provide original tender security of **KES 100,000.00**issued by a financial institution approved and licensed by the Central Bank of Kenya valid for not less than **170 days** from the date of tender opening.
ITT 22.3 (v)	Other types of acceptable securities are _____**N/A**_____
ITT 23.1	In addition to the Original Tender, the number of copies required **is one**.
ITT 23.3	The written confirmation of authorization to sign on behalf of the Tenderer shall consist of **Power of Attorney**
D. Submission and Opening of Tenders	
ITT 25.1	For **Tender submission purposes** only, the Procuring Entity's address is: **Central Bank of Kenya,** Head Office in Nairobi, Ground Floor, Haile Selassie Avenue, **Green Tender Box No. 3** at the main entrance, P. O. Box 60000 – 00200, Nairobi Attention: Head of Procurement Function/Deputy Director, Procurement Division Physical Address, Nairobi, Haile Selassie Avenue, CBK Building, Ground Floor **The deadline for Tender submission is 5th October 2026 at 10:30am** Tenderers ***shall not*** have the option of submitting their Tenders electronically.
ITT 25.1	Tenderers **do *not*** have the option of submitting their Tenders electronically. The Electronic Tendering submission procedures shall be: **Not Applicable to this tender**_____
ITT 28.1	The Tender opening shall take place at Central Bank of Kenya, Head Office in Nairobi, Haile Selassie Avenue, Senior Staff canteen room, 6th Floor CBK Building

Reference to ITC Clause	PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS
ITT 28.6	The Form of Tender and Price Schedules shall be initialed by at least three (3) representatives of the Procuring Entity conducting Tender opening. Each Tender shall be initialed by all representatives and shall be numbered, any modification to the unit or total price shall be initialed by the Representative of the Procuring Entity. The tender opening committee will prepare a tender opening register listing all the bids received and tender opening minutes
E. Evaluation, and Comparison of Tenders	
ITT 33.3	The adjustment shall be based on the ***average*** price of the item or component as quoted in other substantially responsive Tenders. If the price of the item or component cannot be derived from the price of other substantially responsive Tenders, the Procuring Entity shall use its best estimate.
ITT 35.1	The currency that shall be used for Tender evaluation and comparison purposes to convert (at the selling exchange rate) all Tender prices expressed in various currencies into a single currency is Kenya Shillings The source of exchange rate shall be ***the Central Bank in*** **Kenya** The date for the exchange rate shall be the date of tender opening.
ITT 36.4	The invitation to tender is extended to the following group that qualify for Reservations. **This is not applicable to this Tender**
ITT 39.5	The tender involves two lots or contracts, and tenderers are therefore allowed to bid for one or both lots (contracts). The preliminary evaluation criteria are the same for both lots while Compliance with the Technical Requirements and Evaluation on technical Qualifications evaluation criteria are separate for both. Bidders can win both or either of the two lots. **Not Applicable**
ITT 40.1	The Procuring Entity will evaluate and compare the Tenders that have been determined to be substantially responsive, pursuant to ITT 35.4. The evaluation will be performed assuming either that The Contract will be awarded to the Lowest Evaluated Tender.
ITT 44.3	As additional qualification measures, the Information System (or components/parts of it) offered by the Tenderer with the Best Evaluated Tender may be subjected to the following tests and performance benchmarks prior to Contract award such as demonstration tests, performance benchmarks, documentation reviews, reference site visits, etc., by the Tender Evaluation Committee.
ITT 50.1	On receipt of the Bank's Notification_letter, an unsuccessful tenderer may make a written request to the Bank for a debriefing on specific issues or concerns regarding their tender. The Bank shall provide the debriefing within five days of receipt of the request.
ITT 53.1	Within twenty-one (21) days of the receipt of the Form of Acceptance from the Procuring Entity, the successful Tenderer shall furnish the Bank with a **performance security of 5% of** the value of the tender sum provided by a Commercial Bank operating in Kenya and Regulated by the Central Bank of Kenya.
ITT 54.1	Within fourteen days after signing the contract, the Procuring Entity shall publish the awarded contract on www.tenders.go.ke . At the minimum, the notice shall contain the following information: a) Name and address of the Procuring Entity. b) Name and reference number of the contract being awarded, a summary of its scope and the selection method used. c) The name of the successful Tenderer, the final total contract price, the contract duration. d) Dates of signature, commencement, and completion of contract. Names of all Tenderers that submitted Tenders, and their Tender prices as read out at Tender opening

Reference to ITC Clause	PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS
ITT 56.1	The procedures for making a Procurement-related Complaint are detailed in the "Notice of Intention to Award the Contract" herein and are also available from the PPRA website info@ppra.go.ke **or** complaints@ppra.go.ke**.** If a Tenderer wishes to make a Procurement-related Complaint, the Tenderer should submit its complaint following these procedures, in writing (by the quickest means available, that is either by email or fax), to: For the attention: Director, General Services Department, Title/position: Director Procuring Entity: Central Bank of Kenya Email address*:* supplies@centralbank.go.ke In summary, a Procurement-related Complaint may challenge any of the following: 1. the terms of the Tendering Documents; and 2. the Procuring Entity's decision to award the contract.

SECTION III- EVALUATION AND QUALIFICATION CRITERIA

EVALUATION CRITERIA

The evaluation will be carried out through five stages as follows:

Stage 1: Preliminary examination (Compliance with Mandatory Requirements - MR)

Stage 2: Compliance with Technical Specifications

Stage 3: Technical Capacity to Deliver the Proposed Solution

Stage 4: Financial Evaluation

Stage 5: Due Diligence – Verification of information provided.

Recommendation of Award

Stage	Matrix	Criteria
Stage 1	Mandatory Business Requirements	Fully compliant
Stage 2	Technical Requirements	Fully Compliant
Stage 3	Evaluation of Technical capacity to Deliver the Proposed Solution	The Bidder must attain a minimum of 75% to proceed to the next Stage.
Stage 4	Financial Evaluation.	Inclusion of all items and costs of proposed solution.
Stage 5	Due Diligence:	Verification of the bidder's qualification and information submitted.
	Recommendations of Award	Recommendation of award to the lowest bidder who will have met all the requirements

Stage 1: Preliminary examination (Compliance with Mandatory Requirements -MR)

The Procuring Entity will start by examining all tenders to ensure they meet in all respects the eligibility criteria and other mandatory requirements in the ITT, and that the tender is complete in all aspects in meeting the requirements provided for in the preliminary evaluation criteria outlined below. Tenders that do not pass the Preliminary Examination will be considered non-responsive and will not be considered further.

Preliminary Examination and Mandatory Requirements Parameters – Stage 1 of the Evaluation A: Main Contractor

No	Requirements	Compliance (YES/NO)
MR 1	Provide documentary evidence of the company's Certificate of Incorporation/Business Registration Certificate (Legal structure). **Minimum 7 years of Operations.** ***Incase of a Joint Venture both partners to submit. (For foreign firms equivalent certificate to be provided)***	
MR 2	Duly executed Joint Venture Agreement.	

No	Requirements	Compliance (YES/NO)
	Only applicable to Joint Ventures	
MR 3	Provide copy of current CR 12 for Incorporated Firms. ***Incase of a Joint Venture, only one to provide. (For foreign firms equivalent certificate to be provided)***	
MR 4	Field of Activity. Extra Low Voltage Systems and Technological Security. Provide Letter signed by the CEO of the Organization and witnessed by an Authorized Notary. ***Incase of a Joint Venture both partners must meet at least one sector to submit. But both sectors to be met as a minimum.***	
MR 5	Provide copy of the company's **current** Certificate of Tax Compliance issued by Kenya Revenue Authority (KRA) valid at least up to the date of tender opening. ***Incase of a Joint Venture both partners to submit. (For foreign firms equivalent certificate to be provided)***	
MR 6	Submit a duly filled Form of Tender with a validity period of at least **140 days** in the format provided in the tender document. ***Incase of a Joint Venture, only Lead JV Partner to provide.***	
MR 7	Submit a completed company's profile using the business questionnaire attached. ***Incase of a Joint Venture both partners to submit.***	
MR 8	Submit duly filled self-declaration forms as follows: (***Incase of a Joint Venture, both Partners to provide.)*** i). On debarment from participating in Public Procurement (Form SD1) ii). That the person/tenderer will not engage in any corruption/fraudulent practices (Form SD2) iii). Declaration and Commitment to the Code of Ethics	
MR 9	Submit original Tender Security of **Kshs 100,000** in the form provided in this tender document valid for **170 Days** from the date of tender opening) inform of Bank guarantee issued by a Commercial Bank or Microfinance Institution licensed and regulated by CBK or Insurance guarantee issued by an Insurance Company authorized by PPRA. (***Incase of a Joint Venture, only Lead JV Partner to provide.)***	
MR 10	Provide documentary evidence in form of Audited Accounts for the Company for at least three (3) consecutive years 2023, 2024 and 2025 an average annual turnover of Kenya Three Billion (Kshs.3,000,000,000.00) and above in the three years. The audited accounts MUST be signed by the auditor preparing the audited accounts **(A copy of practicing license of the Auditor should be attached for the accounts to be considered for each of the audited years)** and the candidate's Company Director(s). ***Incase of a Joint Venture one of the parties should meet. For Foreign firms equivalent financial documents to be provided***	
MR 11	The nature of business indicated in the audited books of account shall be Technological Security Only. Provide Letter signed by the CEO of the Organization and witnessed by CFO.	

No	Requirements	Compliance (YES/NO)
MR 12	Provide documentary evidence of the Company's valid registration by National Construction Authority as an Electrical Works Contractor Category NCA 1 ***Incase of a Joint Venture either party to provide***	
MR 13	Provide documentary evidence of the Company's valid annual practicing license from the National Construction Authority as an Electrical Works Contractor Category NCA 1 ***Local JV Partners to Provide, for Foreign Firms to submit commitment letter that they will submit upon receiving award letter but before signing of the Contract. Conditions for registration are contained in https://www.nca.go.ke/foreign-contractors***	
MR 14	Provide documentary evidence of the Company's valid Registration with ICT Authority Under ICTA 1-End User Computing Devices. ***Incase of a Joint Venture either party to provide***	
MR 15	Provide documentary evidence of the Company's valid Registration with ICT Authority Under ICTA 1-Information Security. ***Incase of a Joint Venture either party to provide***	
MR 16	Provide documentary evidence of the Company's valid Registration with Energy and Petroleum Regulatory Authority (EPRA) -E1 ***Incase of a Joint Venture either party to provide***	
MR 17	Provide documentary evidence of the Company's valid Registration and Compliance Certificate by Communication Authority of Kenya as a Telecommunication Contractor ***Incase of a Joint Venture either party to provide***	
MR 18	Provide documentary evidence of the Company's valid Registration with ICT Authority Under ICTA 1-Networks. ***Incase of a Joint Venture either party to provide***	
MR 19	Proof of ISO certification for standards 9001 and 27001. ***Incase of a Joint Venture, only Lead JV Partner to provide.***	
MR 20	Provide Manufacturer letter of Authority for the following major components in this Tender. Specifically addressed to Central Bank of Kenya and quoting the tender name and number affirming compliance to technical specifications: - a) Closed Circuit Television System (CCTV) b) Video Management Systems (VMS) c) Artificial Intelligence Analytics Solution d) Access Control System e) Anti Ram Barrier System f) Cyber Security Solution g) Servers h) Physical Security Information Management Platform ***Letters from Authorized Distributors MUST be accompanied by OEM***	

No	Requirements	Compliance (YES/NO)
	Authorization.	
MR 21	Copies of valid compliance certificates for the Cyber Security platform (UL 2900-2-3, General Data Protection Regulations, ISO/IEC 27001 Statement of Applicability, ISO/IEC 270001:2022, ISO/IEC 27017:2015, SOC2 Type 2)	
MR 22	Proof of Pre-Bid Attendance	
Determination of Responsiveness (R/NR)		

Note: All documents submitted by the bidders may be authenticated

Bidders shall be required to meet all the Mandatory Requirements to progress to stage 2 of the evaluation on Technical Specification.

Stage 2: Evaluation on Technical Qualifications

Tenderers meeting all the mandatory requirements shall have their bids checked against compliance with technical specifications indicated in Section "V" of this tender document. Bidders will be required to meet ALL technical specifications and be **FULLY COMPLIANT** to qualify to be progressed to the next stage [Technical Capacity to Deliver the Proposed Solution].

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
3	**Physical security information management system**						
3.1	PSIM software application - for Main Control Center						
3.2	PSIM software application - for site						
3.3	PSIM Client workstation						
3.4	24-inch monitor						
3.5	27-inch monitor						
3.6	GIS engine						
4	**Servers, storage & clients**						
4.1	VMS Recording Server						
4.2	VMS Management Server						
4.3	PSIM Server						
4.4	ACS Server						
4.5	LPR Server						
4.6	UVSS Server						
4.7	Radar Server						
4.8	LiDAR Radar Server						
4.9	Management Out-of-Band server						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
4.10	NTP server						
5	**CCTV cameras**						
5.1	5 MP AI IR Dome camera						
5.2	5 MP AI IR Bullet camera						
5.3	8 MP AI IR Dome camera						
5.4	8 MP AI IR Bullet camera						
5.5	PTZ camera 4 MP						
5.6	Thermal camera 19/25/35mm						
5.7	Camera pole, 10 meter						
5.8	Wall-mounted camera pole						
6	**Video management system**						
6.1	VMS client workstation						
7	**Perimeter surveillance radar**						
7.1	Radar system management software						
7.2	Radar unit, 250 meter						
7.3	Client workstation						
8	**LiDAR perimeter surveillance radar**						
8.1	Radar system management software						
8.2	Long-range 3D LiDAR & AI-based perimeter detection unit						
8.3	Client workstation						
9	**Multimedia**						
9.1	HDMI Matrix Switch 4×4 with Scaler						
9.2	HDMI Matrix Switch 8X8 with Scaler						
9.3	HDMI Matrix Switch 16X16 with Scaler						
9.4	Control box						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
9.5	10.1" touch control panel						
9.6	55" Professional video wall display with wall/ cileing mount						
9.7	USB HDMI KVM Extender						
10	**AI system**						
10.1	Facial recognition software						
11	**Acsess Control System**						
11.1	ACS software application						
11.2	Client workstation						
11.3	4 doors ACS controller						
11.4	2 doors ACS controller						
11.5	Combined RFID &Finger Print reader						
11.6	Combined Face recognition & RFID & Finger print reader						
11.7	600 lbs Electromagnetic lock, single door configuration						
11.8	600 lbs Electromagnetic lock, double door configuration						
11.9	300 lbs Electromagnetic lock, for installation in communication rack						
11.10	Electric strike lock						
11.11	Contactless Push to Exit button						
11.12	Emergency door release unit						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
11.13	High-security magnetic door position switches						
11.14	Hydraulic door closer						
11.15	ACS enrolment and card production workstation						
11.16	Enrolment RFID reader						
11.17	Contactless smart cards						
11.18	Door alarm						
11.19	RFID reader						
12	**Intrusion Detection System**						
12.1	IDS controller, Grade 3						
12.2	Internal 8-zone expander, Grade 3						
12.3	32-zone expander, Grade 3						
12.4	Keypad, Grade 3						
12.5	Wall-mounted detector, Grade 3						
12.6	Ceiling-mounted detector anti mask, 4 m installation height, Grade 3						
12.7	Ceiling-mounted detector, Anti mask 8 m installation height, Grade 3						
12.8	Seismic detector, Grade 3						
12.9	Dual technologies detector, outdoor						
12.10	Panic button, Grade 3						
12.11	Curtain detector, 10 meters detection range, Grade 3						
12.12	Laser detector, Grade 3						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
12.13	High-security magnetic switch						
12.14	Heavy duty magnet						
12.15	Internal sounder/strobe, Grade 3						
12.16	External sounder/strobe, Grade 3						
13	**Public address system**						
13.1	Horn speaker						
13.2	Indoor ceiling speaker						
13.3	PA master station console						
13.4	Public address management software						
14	**Intercom system**						
14.1	Video intercom door unit						
14.2	Intercom master station console						
14.3	Intercom IP Software						
15	**LPR system**						
15.1	Parking management software						
15.2	Client workstation						
15.3	LPR camera						
15.4	Arm barrier						
15.5	One-way trafic spike barrier						
16	**Under Vehicle Surveillance System (UVSS)**						
16.1	Under vehicle surveillance system						
16.2	Client workstation						
18	**Speed gates**						
18.1	Speed gate, 55 - 65 CM pass width						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
18.2	Speed gate, 90 - 180 CM pass width						
18.3	Disabled persons access gate						
18.5	Full height turnstile						
19	**Data communication network**						
19.1	Backbone switch, Layer 3						
19.2	24 ports managed access switch						
19.3	Industrial 16 ports managed PoE switch						
19.4	Industrial 8 ports managed PoE switch						
19.5	Optical patch panel, 24 ports						
19.6	Patch panel RJ45, 24 ports						
19.7	Single mode fiber optic cable, 12-strand						
19.8	44U Equipment rack						
19.9	22U Equipment rack						
19.10	15U Communication cabinet						
19.11	6U Communication cabinet						
19.12	Outdoor communication cabinet						
19.13	Outdoor electricity backup system						
19.14	UPS for indoor communication cabinets						
19.15	UPS 10 KVA						
19.16	Industrial-grade 6-channel digital I/O ethernet-based controller						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
19.17	Rodent repellent system						
19.18	Environmental monitoring system						
21	**Control room**						
21.1	Operators control desk module for 1 operator						
21.2	Monitors arms						
22	**Scanning devices**						
22.1	Archway metal detector						
22.2	X-ray Bags and Parcels Inspection Machine						
23	**Barriers, gates and turnstiles**						
23.1	Hydro-electric bollards (K-4)						
23.2	Anti – ram arm barrier, K4						
23.3	Cantilever sliding gate						
23.4	Operating control panel						
24	**Electronic Key Management System**						
24.1	Electronic key management system, 60 Keys						
25	**Doors, and Security Grilles**						
25.1	5-Minute forced entry rated door						
25.2	5-Minute forced entry rated security grille						
27	**Cyber security**						
27.1	Cyber security monitoring system						
27.2	SIEM security monitoring platform						
27.3	Network intrusion detection and threat monitoring & IOT DPI						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
27.4	Network Access Control for IOT & device authentication						
27.5	Protection against unauthorized USB device usage						
27.6	Continuous vulnerability and CVE monitoring system						
27.7	System health & IOT Health monitoring sensors						
27.8	Operator workstations						
27.9	Network traffic probe appliances for analysis						
17.1	Network traffic probe appliances for analysis						
27.11	Out of Band switches for High secure management						
27.12	Management Servers						
27.13	EPS Platform						
27.14	Application execution control for endpoints						
27.15	PKI infrastructure for encryption and certificates						
27.16	Centrazlized Next Generation Firewall						
27.17	Segmatation NGFW						
27.18	Monitoring system for IT infrastructure health						
27.19	Operational training for system administrators						
27.2	Service laptops for maintenance operations						

SN	ITEM	Manufacturer	Model	Datasheet (Make reference to the specific pages)	Comply with specs	Not comply with specs	Bidder remarks
27.21	Portable laptops for field technical support						
27.22	Content Disarm and Reconstruction						

Stage 3: Technical Capacity to Deliver the Proposed Solution

Bidders should demonstrate their capacity in terms of technical capability, project planning, professional experience and technical personnel to deliver the proposed solution.

Tenderers meeting the qualification on Compliance to Technical Specification will be subjected to technical evaluation on qualification based on the technical parameters given below:

	Evaluation Attribute	Weighting Score	Max Score
T1	**General Experience – Physical Security Installations** Provide a list of at least Six **(6) project with references (names and telephone of contact persons)** to which the company has undertaken the following Physical Security Installation Works in the last Seven (7) years i.e. 2019 – 2026, project value not less than Kenya Shillings Four Hundred Million 400,000,000, for a public, governmental, state-security, or municipal entity, including: Command and control system and integration between all of the following systems: - VMS Systems - Cameras - Access Control - Alarm - Analytics **Note**: Bidder to provide copies of contracts/completion certificates/letter from client clearly stating the nature of the contract, amount and completion date as proof of having undertaken the works.	Each reference client will earn **5 marks**	**30**
T2	**General Experience – Service Level Agreement** Provide a list of at least one **(1) project with references (names and telephone of contact persons)** to which the company has undertaken a service level agreement for a Physical Security Installation in the last Seven (7) years i.e. 2019 – 2026, value not less than Kenya Shillings One Hundred and Thirty Million 130,000,000 **Note**: Bidder to provide copies of **Note**: Bidder to provide copies of contracts/completion certificates/letter from client clearly stating the nature of the contract, amount completion date as proof of having undertaken the works.	Reference will earn **10 marks**	**10**

	Evaluation Attribute	Weighting Score	Max Score
T3.1	**Specific Experience – Public / Government / State Security / Municipality Entity etc.** Provide at least two projects that includes, within its scope, a client's control room managing an array of more than 1000 cameras and at least 10 end sites, with 24/7 viewing and recording at a central control center, each reference shall receive 10 points. **Note**: Bidder to provide copies of **Note**: Bidder to provide copies of contracts/completion certificates/letter from client clearly stating the nature of the contract, amount completion date as proof of having undertaken the works.	Each reference will earn **10 marks**	**20**
T3.2	**Specific Experience – Major Financial Institutions/Reserve/Central Banks / Security Project** Provide at least One (1) **Projects with references (names and telephone of contact persons)** undertaken in the last **7 years that includes the following components.** 1. Main control center including a command and control system 2. VMS system 3. 500 cameras 4. 50 analytics systems 5. 100 alarm sensors **6.** 50 controlled doors **Note**: Bidder to provide copies of **Note**: Bidder to provide copies of contracts/completion certificates/letter from client clearly stating the nature of the contract, amount completion date as proof of having undertaken the works.	Each reference client will earn **10 marks**	**10**
T4	**Quality Certification** Valid copy of ISO 22301 Business Continuity certification.	5 marks for valid certificate	**5**
T5	**Cyber Security Certification** • System and Organization Controls 2 (SOC2 Type 2)	5 Marks	**5**

	Evaluation Attribute	Weighting Score	Max Score
T6	Provide a list of at least Four (4) Qualified Technical Staff in each category below: • Cyber Security Expert • PSIM Configuration Expert • Network Engineer • Project Manager For any of the personnel provided to qualify, the following requirements MUST be met: **A.** All technical staff provided MUST have as a minimum five years' post college experience in Technological Security/Information Technology Industry/Project Management. Each personnel MUST indicate the firms he/she has worked in since graduation. **B. Detailed Curriculum Vitae (CV's) of each staff MUST be attached.** The Curriculum Vitae MUST state qualification, experience, and duration with the firm and active contacts of the staff. The contacts given in the Curriculum Vitae MUST be active email addresses. **C. Copies of academic certificates MUST be provided.** **D.** The role of each technical staff should be indicated **E.** All the Staff Proposed Must have been in the Current Employment with the Bidder for a Minimum of **TWO** Years, a signed letter from the Human Resource Department to be included.		
T6.1	**Cyber Security Expert** **Academic Qualification** **a)** Holder of a Degree in either Computer Science/Engineering, Software Engineering or Information System Engineering – 1 Marks **b)** No degree – 0 Marks **Professional Qualification** **c)** Holder of Certified Information Systems Security Professional (CISSP) or Internationally recognized equivalent – 2 Marks **d)** No certification – 0 Marks **Experience Qualification** **e)** Relevant Experience – 2 Marks **f)** No Relevant Experience – 0 Marks	Maximum **5 marks**	**5**
T6.2	**PSIM Configuration Expert** **Academic Qualification** **a)** Holder of a Degree in either Computer Science/Engineering, Software Engineering or Information System Engineering – 1 Marks **b)** No degree – 0 Marks **Professional Qualification** **c)** Holder of PSIM OEM Configuration Expert Certificate from the OEM– 2 Marks **d)** No certification – 0 Marks	Maximum **5 marks**	**5**

	Evaluation Attribute	Weighting Score	Max Score
	Experience Qualification **e)** Relevant Experience – 2 Marks **f)** No Relevant Experience – 0 Marks		
T6.3	**Network Engineer** **Academic Qualification** **a)** Holder of a Degree in either Computer Science/Engineering, Software Engineering or Information System Engineering – 1 Marks **b)** No degree – 0 Marks **Professional Qualification** **c)** Holder of Certified Internetwork Expert (CIE) or Internationally recognized equivalent – 2 Marks **d)** No certification – 0 Marks **Experience Qualification** **e)** Relevant Experience – 2 Marks **f)** No Relevant Experience – 0 Marks	Maximum **5 marks**	**5**
T6.4	**Project Manager** **Academic Qualification** a) Holder of a Degree in either Computer Science/Engineering, Software Engineering or Information System Engineering – 1 Marks b) No degree – 0 Marks **Professional Qualification** c) Certified Project Management Certification i.e PMP/Prince 2 or equivalent – 2 Marks **d)** No Certification – 0 Marks **Experience Qualification** **e)** Relevant Experience – 2 Marks **f)** No Relevant Experience – 0 Marks	Maximum **5 marks**	**5**
	Total		**100**

Tenderers will be required to score 75 % and above on the above Technical Qualification Evaluation to qualify for financial evaluation.

Stage 4: Financial Evaluation

Tenderers passing Technical Qualification Evaluation will have their bids subjected to financial evaluation. Financial Evaluation will involve checking for completeness of the bill of quantities and ranking to determine the lowest evaluated bidder. The lowest evaluated bidder will be subjected to due diligence on reference projects.

The bidder that emerges **with the lowest evaluated bid price** will be recommended for the due diligence stage. The bidder will be notified to prepare for due diligence and presentation.

Stage 5: Due diligence.

The lowest evaluated bidder shall be subjected to due diligence. This involves verification of the bidder's qualification information submitted in compliance with the mandatory requirements, technical requirements and confirmation of bidders ability and capability to provide the services.

Recommendation of Award

The lowest evaluated bidder who complies with all the requirements as contained in the tender document will be recommended for award of the tender.

SECTION IV - TENDERING FORMS

1. FORM OF TENDER

INSTRUCTIONS TO TENDERERS

i) The Tenderer must prepare this Form of Tender on stationery with its letter head clearly showing the Tenderer's complete name and business address.

ii) All italicized text is to help Tenderer in preparing this form.

iii) Tenderer must complete and sign TENDERER'S ELIGIBILITY- CONFIDENTIAL BUSINESS QUESTIONNAIRE, *CERTIFICATE OF INDEPENDENT TENDER DETERMINATION and the SELF DECLARATION OF THE TENDERER,* all *attached to this Form of Tender*

iv) The Form of Tender shall include the following Forms duly completed and signed by the Tenderer.

- *Tenderer's Eligibility-Confidential Business Questionnaire*
- *Certificate of Independent Tender Determination*
- *Self-Declaration of the Tenderer*

Date of this Tender submission..... [*insert date (as day, month and year) of Tender submission*] **ITT No.:** ..... [*insert number of ITT process*]

Alternative No.: ..... [*insert identification No if this is a Tender for an alternative*]

To: ..... **[*insert complete name of Procuring Entity]***

a) **No reservations:** We have examined and have no reservations to the tendering document, including Addenda issued in accordance with Instructions to Tenderers (ITT 8);

b) **Eligibility**: We meet the eligibility requirements and have no conflict of interest in accordance with ITT 4;

c) **Tender-Securing Declaration:** We have not been debarred by the Authority based on execution of a Tender-Securing Declaration or Tender Securing Declaration in Kenya in accordance with ITT 4.8;

d) **Conformity:** We offer to provide design, supply and installation services in conformity with the tendering document of the following: [*insert a brief description of the IS Design, Supply and Installation Services*];

e) **Tender Price:** The total price of our Tender, excluding any discounts offered in item (f) below is: *[Insert one of the options below as appropriate]*

[Option1, in case of one lot:] Total price is: [*insert the total price of the Tender in words and figures, indicating the various amounts and the respective currencies*];

Or

[Option 2, in case of multiple lots:] (a) Total price of each lot [*insert the total price of each lot in words and figures, indicating the various amounts and the respective currencies*]; and (b) Total price of all lots (sum of all lots) [*insert the total price of all lots in words and figures, indicating the various amounts and the respective currencies*];

(f) **Discounts:** The discounts offered and the methodology for their application are:

i) The discounts offered are: [*Specify in detail each discount offered.*]

ii) The exact method of calculations to determine the net price after application of discounts is shown below: [*Specify in detail the method that shall be used to apply the discounts*].

g) **Tender Validity Period:** Our Tender shall be valid for the period of 140 days from the date fixed for the Tender submission deadline (specified in TDS ITT 23.1 (as amended if applicable), and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

C2: CBK Official

h) **Performance Security:** If our Tender is accepted, we commit to obtain a Performance Security in accordance with the tendering document.

i) **One Tender per Tenderer:** We are not submitting any other Tender (s) as an individual Tenderer, and we are not participating in any other Tender (s) as a Joint Venture member, and meet the requirements of ITT 4.3, other than alternative Tenders submitted in accordance with ITT 13.

j) **Suspension and Debarment**: We, along with any of our subcontractors, suppliers, consultants, manufacturers, or service providers for any part of the contract, are not subject to, and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the PPRA. Further, we are not in eligible under Laws of Kenya or official regulations or pursuant to a decision of the United Nations Security Council.

k) **State-owned enterprise or institution**: [*select the appropriate option and delete the other*] [*We are not a state-owned enterprise or institution*]/ [*We are a state-owned enterprise or institution but meet the requirements of ITT 4.7*].

l) **Commissions, gratuities, and fees**: We have paid, or will pay the following commissions, gratuities, or fees with respect to the Tendering process or execution of the Contract: *[insert complete name of each Recipient, its full address, the reason for which each commission or gratuity was paid and the amount and currency of each such commission or gratuity]*

Name of Recipient	Address	Reason	Amount

(If none has been paid or is to be paid, indicate "none.")

m) **Binding Contract**: We understand that this Tender, together with your written acceptance thereof included in your Form of Acceptance, shall constitute a binding contract between us, until a formal contract is prepared and executed.

n) **Not Bound to Accept:** We understand that you are not bound to accept the lowest evaluated cost Tender, the Best Evaluated Tender, or any other Tender that you may receive; and

o) **Fraud and Corruption:** We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf engages in any type of Fraud and Corruption.

Name of the Tenderer: *[*insert complete name of person signing the Tender*]

p) **Collusive practices:** We hereby certify and confirm that the tender is genuine, non-collusive and made with the intention of accepting the contract if awarded. To this effect we have signed the "Certificate of Independent Tender Determination" attached below.

q) **Code of Ethical Conduct:** We undertake to adhere by the Code of Ethical Conduct for Persons Participating in Public Procurement and Asset Disposal Activities in Kenya, copy available from ***www.pppra.go.ke*** during the procurement process and the execution of any resulting contract.

r) We, the Tenderer, have fully completed and signed the following Forms as part of our Tender:

i) Tenderer's Eligibility: Confidential Business Questionnaire – to establish we are not in any conflict to interest.

ii) Certificate of Independent Tender Determination – to declare that we completed the tender without colluding with other tenderers.

iii) Self-Declaration of the Tenderer–to declare that we will, if awarded a contract, not engage in any form of fraud and corruption.

iv) Declaration and commitment to the code of ethics for Persons Participating in Public Procurement and Asset Disposal Activities in Kenya. Further, we confirm that we have read and understood the full content and scope of fraud and corruption as in formed in **"Appendix1-Fraud and Corruption**" attached to the Form of Tender.

Name of the person duly authorized to sign the Tender on behalf of the Tenderer: **[*insert complete name of person duly authorized to sign the Tender*]

Title of the person signing the Tender: [*insert complete title of the person signing the Tender*] Signature **of the person named above**: [*insert signature of person whose name and capacity are shown above*] **Date signed** [*insert date of signing*] **day of** [*insert month*], [*insert year*].

I. TENDERER'S ELIGIBILITY-CONFIDENTIAL BUSINESS QUESTIONNAIRE

Instruction to Tenderer

Tender is instructed to complete the particulars required in this Form, *one form for each entity if Tender is a JV.*
Tenderer is further reminded that it is an offence to give false information on this Form.

a) Tenderer's details

	ITEM	DESCRIPTION
1	Name of the Procuring Entity	
2	Reference Number of the Tender	
3	Date and Time of Tender Opening	
4	Name of the Tenderer	
5	Full Address and Contact Details of the Tenderer.	1. Country 2. City 3. Location 4. Building 5. Floor 6. Postal Address 7. Name and email of contact person. 8. Email of contact person
6	Current Trade License Registration Number and Expiring date	
7	Name, country and full address (*postal and physical addresses, email, and telephone number*) of Registering Body/Agency	
8	Description of Nature of Business	
9	Maximum value of business which the Tenderer handles.	
10	State if Tenders Company is listed in stock exchange, give name and full address (*postal and physical addresses, email, and telephone number*) of state which stock exchange	

C2: CBK: Official

General and Specific Details

b) **Sole Proprietor,** provide the following details.

Name in full_____Age_____

Nationality_____Country of Origin_____

Citizenship _____

c) **Partnership,** provide the following details.

	Names of Partners	Nationality	Citizenship	% Shares owned
1				
2				
3				

d) **Registered Company,** provide the following details.

(i) Private or public Company _____

(ii) State the nominal and issued capital of the Company.

Nominal Kenya Shillings (Equivalent).....

Issued Kenya Shillings (Equivalent).....

(iii) Give details of Directors as follows.

	Names of Director	Nationality	Citizenship	% Shares owned
1				
2				
3				

e) DISCLOSURE OF INTEREST - Interest of the Firm in the Procuring Entity.

i) are there any person/persons in…… (*Name of Procuring Entity)* who has/have an interest or relationship in this firm? Yes/ No……

If yes, provide details as follows.

	Names of Person	Designation in the Procuring Entity	Interest or Relationship with Tenderer
1			
2			
3			

C2: CBK-Official

ii) Conflict of interest disclosure

	Type of Conflict	Disclosure YES OR NO	If YES provide details of the relationship with Tenderer
1	Tenderer is directly or indirectly controls, is controlled by or is under common control with another tenderer.		
2	Tenderer receives or has received any direct or indirect subsidy from another tenderer.		
3	Tenderer has the same legal representative as another tenderer		
4	Tender has a relationship with another tenderer, directly or through common third parties, that puts it in a position to influence the tender of another tenderer or influence the decisions of the Procuring Entity regarding this tendering process.		
5	Any of the Tenderer's affiliates participated as a consultant in the preparation of the design or technical specifications of the works that are the subject of the tender.		
6	Tenderer would be providing goods, works, non-consulting services or consulting services during implementation of the contract specified in this Tender Document.		
7	Tenderer has a close business or family relationship with a professional staff of the Procuring Entity who are directly or indirectly involved in the preparation of the Tender document or specifications of the Contract, and/or the Tender evaluation process of such contract.		
8	Tenderer has a close business or family relationship with a professional staff of the Procuring Entity who would be involved in the implementation or supervision of such Contract.		
9	Has the conflict stemming from such relationship stated in item 7 and 8 above been resolved in a manner acceptable to the Procuring Entity throughout the tendering process and execution of the Contract.		

f) Certification

On behalf of the Tenderer, I certify that the information given above is complete, current, and accurate as at the date of submission.

Full Name_____

Title orDesignation_____

_____ _____

(Signature) *(Date)*

C2: CBK Official

II. CERTIFICATE OF INDEPENDENT TENDER DETERMINATION

I, the undersigned, in submitting the accompanying Letter of Tender to the_____*[Name of Procuring Entity]* for:_____*[Name and number of tenders]* in response to the request for tenders made by: _____*[Name of Tenderer]* do hereby make the following statements that I certify to be true and complete in every respect:

I certify, on behalf of_____*[Name of Tenderer]* that:

i). I have read and I understand the contents of this Certificate.

ii). I understand that the Tender will be disqualified if this Certificate is found not to be true and complete in every respect.

iii). I am the authorized representative of the Tenderer with authority to sign this Certificate, and to submit the Tender on behalf of the Tenderer.

iv). For the purposes of this Certificate and the Tender, I understand that the word "competitor" shall include any individual or organization, other than the Tenderer, whether or not affiliated with the Tenderer, who:

a) Has been requested to submit a Tender in response to this request for tenders.

b) could potentially submit a tender in response to this request for tenders, based on their qualifications, abilities or experience.

v). The Tenderer discloses that [check one of the following, as applicable]:

a) The Tenderer has arrived at the Tender independently from, and without consultation, communication, agreement or arrangement with, any competitor.

b) the Tenderer has entered into consultations, communications, agreements or arrangements with one or more competitors regarding this request for tenders, and the Tenderer discloses, in the attached document(s), complete details thereof, including the names of the competitors and the nature of, and reasons for, such consultations, communications, agreements or arrangements.

vi). In particular, without limiting the generality of paragraphs (5) (a) or (5) (b) above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:

a) prices.

b) methods, factors or formulas used to calculate prices.

c) the intention or decision to submit, or not to submit, a tender; or

d) the submission of a tender which does not meet the specifications of the request for Tenders; except as specifically disclosed pursuant to paragraph (5) (b) above.

vii). In addition, there has been no consultation, communication, agreement or arrangement with any competitor regarding the quality, quantity, specifications or delivery particulars of the works or services to which this request for tenders relates, except as specifically authorized by the procuring authority or as specifically disclosed pursuant to paragraph (5) (b) above.

viii). The terms of the Tender have not been, and will not be, knowingly disclosed by the Tenderer, directly or indirectly, to any competitor, prior to the date and time of the official tender opening, or of the awarding of the Contract, whichever comes first, unless otherwise required by law or as specifically disclosed pursuant to paragraph(5)(b) above.

Name_____

Title_____

Date_____

_____

[Name, title and signature of authorized agent of Tenderer and Date]

III. SELF-DECLARATION FORMS

FORM SD1

SELF DECLARATION THAT THE PERSON/ TENDERER IS NOT DEBARRED IN THE MATTER OF THE PUBLIC PROCUREMENT AND ASSET DISPOSAL ACT 2015.

I, ……., of Post Office Box …….……. being a resident of …….. in the Republic of ……. do hereby make a statement as follows: -

1. THAT I am the Company Secretary/ Chief Executive/Managing Director/Principal Officer/Director of ……...…….. *(Insert name of the Company)* who is a Bidder in respect of **Tender No.……** for…… *(Insert tender title/description)* for……. *(Insert name of the Procuring entity)* and duly authorized and competent to make this statement.

2. THAT the aforesaid Bidder, its directors and subcontractors have not been debarred from participating in procurement proceeding under Part IV of the Act.

3. THAT what is deponed to here in above is true to the best of my knowledge, information, and belief.

……. ……. ……
(Title) (Signature) (Date)

Bidder Official Stamp

FORM SD2

SELF DECLARATION THAT THE PERSON/TENDERER WILL NOT ENGAGE IN ANY CORRUPT OR FRAUDULENT PRACTICE

I, ...of P. O. Box..... being a resident of ……. in the Republic of.....do hereby make a statement as follows: -

1. THAT I am the Chief Executive /Managing Director/ Principal Officer/ Director of……..... .....…… *(insert name of the Company)* who is a Bidder in respect of **Tender No. ……..** for ……. *(insert tender title/description)* for …… *(insert name of the Procuring entity)* and duly authorized and competent to make this statement.

2. THAT the aforesaid Bidder, its servants and/or agents /subcontractors will not engage in any corrupt or fraudulent practice and has not been requested to pay any inducement to any member of the Board, Management, Staff and /or employees and /or agents of……. *(insert name of the Procuring entity)* which is the procuring entity.

3. THAT the aforesaid Bidder, its servants and /or agents /subcontractors have not offered any inducement to any member of the Board, Management, Staff and/ or employees and/ or agents of……. *(name of the procuring entity).*

4. THAT the aforesaid Bidder will not engage /has not engaged in any corrosive practice with other bidders participating in the subject tender

5. THAT what is deponed to here in above is true to the best of my knowledge information and belief.

…….. ……. ……
(Title) (Signature) (Date)

Bidder Official Stamp

C2: CBK: Official

DECLARATION AND COMMITMENT TO THE CODE OF ETHICS

I ..... (person) on behalf of ***(Name of the Business/Company/Firm***) ……. declare that I have read and fully understood the contents of the Public Procurement & Asset Disposal Act, 2015, Regulations and the Code of Ethics for persons participating in Public Procurement and Asset Disposal activities in Kenya and my responsibilities under the Code.

I do hereby commit to abide by the provisions of the Code of Ethics for persons participating in Public Procurement and Asset Disposal.

Name of Authorized signatory….....…….

Sign…….....…….....

Position…….....…….....……

Office address…….....……. Telephone…….

E-mail…….....……

Name of the Firm/Company…….....….....

Date…….....…...

(Company Seal/ Rubber Stamp where applicable)

Witness

Name…….....

Sign…….....

Date…….....

C2: CBK Official

IV APPENDIX 1 - FRAUD AND CORRUPTION

(Appendix 1 shall not be modified)

1. Purpose

1.1 The Government of Kenya's Anti-Corruption and Economic Crime laws and their sanction's policies and procedures, Public Procurement and Asset Disposal Act, 2015 (the Act) and the Public Procurement and Asset Regulations, 2020 (the Regulations) and any other relevant Kenya's Acts or Regulations related to Fraud and Corruption, and similar offences, shall apply with respect to Public Procurement Processes and Contracts that are governed by the laws of Kenya.

2. Requirements

2.1 The Government of Kenya requires that all parties including Procuring Entities, Tenderers, (applicants/proposers), Consultants, Contractors and Suppliers; any Sub-contractors, Sub-consultants, Service providers or Suppliers; any Agents (whether declared or not); and any of their Personnel, involved and engaged in procurement under Kenya's Laws and Regulation, observe the highest standard of ethics during the procurement process, selection and contract execution of all contracts, and refrain from Fraud and Corruption and fully comply with Kenya's laws and Regulations as per paragraphs 1.1 above.

2.2 Section 66 of the Act describes rules to be followed and actions to be taken in dealing with Corrupt, Coercive, Obstructive, Collusive or Fraudulent practices, and Conflicts of Interest in procurement including consequences for offences committed. A few of the provisions noted below high light Kenya's policy of no tolerance for such practices and behavior:

i) A person to whom this Act applies shall not be involved in any corrupt, coercive, obstructive, collusive, or fraudulent practice; or conflicts of interest in any procurement or asset disposal proceeding.

ii) And a person referred to under subsection (1) who contravenes the provisions of that sub-section commits an offence.

iii) Without limiting the generality of the subsection (1) and (2), the person shall be: -

a) disqualified from entering into a contract for a procurement or asset disposal proceeding; or

b) if a contract has already been entered into with the person, the contract shall be voidable.

iv) The voiding of a contract by the procuring entity under subsection (7) does not limit any legal remedy the procuring entity may have.

v) An employee or agent of the procuring entity or a member of the Board or committee of the procuring entity who has a conflict of interest with respect to a procurement: -
   a) Shall not take part in the procurement proceedings.
   b) shall not, after a procurement contract has been entered into, take part in any decision relating to the procurement or contract; and

c) shall not be a subcontractor for the tenderer to whom was awarded contract, or a member of the group of tenderers to whom the contract was awarded, but the subcontractor appointed shall meet all the requirements of this Act.

vi) An employee, agent or member described in subsection (1) who refrains from doing anything prohibited under that subsection, but for that subsection, would have been within his or her duties shall disclose the conflict of interest to the procuring entity.

vii) If a person contravenes sub section (1) with respect to a conflict of interest described in sub section (5) (a) and the contract is awarded to the person or his relative or to another person in whom one of them had a direct or indirect pecuniary interest, the contract shall be terminated, and all costs incurred by the public entity shall be made good by the awarding officer. Etc.

2.2 In compliance with Kenya's laws, regulations and policies mentioned above, the Procuring Entity:

a) Defines broadly, for the purposes of the above provisions, the terms:
   i) "Corrupt practice" is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party.

ii) "Fraudulent practice" is any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation.

iii) "Collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party.

iv) "Coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.

v) "Obstructive practice" is:

1) Deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede investigation by Public Procurement Regulatory Authority (PPRA) or any other appropriate authority appointed by Government of Kenya into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or

2) acts intended to materially impede the exercise of the PPRA's, or the appointed authority's inspection and audit rights provided for under paragraph 2.3e. below.

b) Defines more specifically, in accordance with the Act, provisions set forth for fraudulent and collusive practices as follows:

"Fraudulent practice" includes a misrepresentation of fact in order to influence a procurement or disposal processor the exercise of a contract to the detriment of the procuring entity or the tenderer or the contractor and includes collusive practices amongst tenderers prior to or after tender submission designed to establish tender prices at artificial non-competitive levels and to deprive the procuring entity of the benefits of free and open competition.

c) Rejects a proposal for award[1] of a contract if PPRA determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-contractors, service providers, suppliers and/ or their employees, has, directly or indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question.

d) Pursuant to the Act and the Regulations, the Procuring Entity may recommend to PPRA for sanctioning and debarment of a firm or individual, as applicable under the Act and the Regulations.

e) Requires that a clause be included in the tender documents and Request for Proposal documents requiring (i) Tenderers (applicants/proposers), Consultants, Contractors, and Suppliers, and their Sub-contractors, Sub-consultants, Service providers, Suppliers, Agents personnel, permit the PPRA or any other appropriate authority appointed by Government of Kenya to inspect[2]all accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have them audited by auditors appointed by the PPRA or any other appropriate authority appointed by Government of Kenya; and

f) Pursuant to Section 62 of the Act, requires Applicants/Tenderers to submit along with their Applications/Tenders/Proposals a "Self-Declaration Form" as included in the procurement document declaring that they and all parties involved in the procurement process and contract execution have not engaged/ will not engage in any corrupt or fraudulent practices.

---

[1] *For the avoidance of doubt, a party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in A consultancy, and tendering, either directly or as a nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider, in respect of such contract, and (ii) entering into an addendum or amendment introducing a material modification to any existing contract.*

[2] *Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Investigating Authority or persons appointed by the Procuring Entity to address specific matters related to investigations/ audits, such as evaluating the veracity of an allegation of possible Fraud and Corruption, through the appropriate mechanisms. Such activity includes but is not limited to: accessing and examining a firm's or individual's financial records and information, and making copies there of as relevant; accessing and examining any other documents ,data and information (whether in hard copy or electronic format) deemed relevant for the investigation/ audit, and making copies there of as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.*

C2: CBK Official

PRICE SCHEDULE FORMS

Notes to Tenderers on working with the Price Schedules

1.1 General

The Price Schedules are divided into separate Schedules as follows:

a Grand Summary Cost Table

b Supply and Installation Cost Summary Table

c Recurrent Cost Summary Table

d Supply and Installation Cost Sub-Table (s)

e Recurrent Cost Sub-Tables (s)

f Country of Origin Code Table

[insert:]

1.2 The Schedules do not generally give a full description of the information technologies to be supplied, installed, and operationally accepted, or the Services to be performed under each item. However, it is assumed that Tenderers shall have read the Technical Requirements and other sections of these tendering documents to ascertain the full scope of the requirements associated with each item prior to filling in the rates and prices. The quoted rates and prices shall be deemed to cover the full scope of these Technical Requirements, as well as overhead and profit.

1.3 If Tenderers are unclear or uncertain as to the scope of any item, they shall seek clarification in accordance with the Instructions to Tenderers in the tendering documents prior to submitting their tender.

2. Pricing

2.1 Prices shall be filled in indelible ink, and any alterations necessary due to errors, etc., shall be initialed by the Tenderer. As specified in the Tender Data Sheet, prices shall be fixed and firm for the duration of the Contract.

2.2 Tender prices shall be quoted in the manner indicated and, in the currencies, specified in ITT 18.1 and ITT 18.2. Prices must correspond to items of the scope and quality defined in the Technical Requirements or elsewhere in these tendering documents.

2.3 The Tenderer must exercise great care in preparing its calculations, since there is no opportunity to correct errors once the deadline for submission of tenders has passed. A single error in specifying a unit price can therefore change a Tenderer's overall total tender price substantially, make the tender noncompetitive, or subject the Tenderer to possible loss. The Procuring Entity will correct any arithmetic error in accordance with the provisions of ITT 32.

2.4 Payments will be made to the Supplier in the currency or currencies indicated under each respective item. As specified in ITT18.2, no more than two foreign currencies may be used.

C2: CBK Official

A. PRICE SCHEDULE SUMMARY

	Licenses	**Quantity**	***Total Price(Kes)***
1.	Supply, Delivery, Installation, training and Commissioning of Integrated Security System for Central Bank of Kenya	LOT	
	Sub-Total		
	0.03% PPRA Capacity Building Levy		
	16% VAT		
	TOTAL COST VAT INCLUSIVE (to be transferred to Form of tender)		

Name of Tenderer: _____

Signature_____ Date _____

Recurrent Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITT 17 and ITT18.

Line-Item No.	**Subsystem / Item**	**Recurrent Cost Sub-Table No.**	***[insert: Kenya shilling] Price***	***[insert: Foreign Currency A] Price***	***[insert: Foreign Currency B] Price***
	Subtotals (to Grand Summary Table)				

Note: Refer to the relevant Recurrent Cost Sub-Tables for the specific components that constitute the Sub system or line item in this summary table.

Name of Tenderer:_____

Date_____

Authorized Signature of Tenderer: _____

3. Supply and Installation Cost Sub-Table *[insert identifying number]*

Line-item number: [*specify* ***relevant line-item number from the Supply and Installation Cost Summary Table*** *(e.g., 1.1)]*

Prices, rates, and subtotals MUST be quoted in accordance with ITT 17 and ITT18.

				Unit Prices / Rates					**Total Prices**			
				Supplied Locally	**Supplied from outside Kenya**				**Supplied Locally**	**Supplied from outside Kenya**		
Compo-nent No.	**Component Description**	**Country of Origin Code**	**Quan-tity**	***[** insert: **local currency]***	***[** insert: **local currency]***	***[** insert: **foreign currency A]***	***[** insert **foreign currency B]***		***[** insert: **local currency]***	***[** insert: **local currency]***	***[** insert: **foreign currency A]***	***[** insert: **foreign currency B]***
X.1	____	- -	- -	- -	- -	- -	- -					
Subtotals (to *[insert line **item]*** of Supply and Installation Cost Summary Table)												

Note: - - indicates not applicable

Name of Tenderer: _____

_____Date_____

Authorized Signature of Tenderer:

C2: CBK - Official

4. Country of Origin Code Table

Country of Origin	Country Code	Country of Origin	Country Code	Country of Origin	Country Code

QUALIFICATION FORMS

1. FOREIGN TENDERERS 40% RULE

Pursuant to ITT 4.11, a foreign tenderer must complete this form to demonstrate that the tender fulfils this condition.

ITEM	Description of Work Item	Describe location of Source	COST in K. shillings	Comments, if any
A	Local Labor			
1				
2				
3				
4				
5				
B	Sub contracts from Local sources			
1				
2				
3				
4				
5				
C	Local materials			
1				
2				
3				
4				
5				
D	Use of Local Plant and Equipment			
1				
2				
3				
4				
5				
E	Add any other items			
1				
2				
3				
4				
5				
6				
	TOTAL COST LOCAL CONTENT		xxxxx	
	PERCENTAGE OF CONTRACT PRICE		xxxxxx	

2. Form ELI-1 Tenderer Information Form

[The Tenderer shall fill in this Form in accordance with the instructions indicated below. No alterations to its format shall be permitted and no substitutions shall be accepted.]

Date: .....*[insert date (as day, month and year) of Tender submission*]

ITT No.: .....*[insert number of Tendering process]*

Alternative No.: .....*[insert identification No if this is a Tender for an alternative]*

1. Tenderer's Name [*insert Tenderer's legal name]*
2. In case of JV, legal name of each member: *[insert legal name of each member in JV]*
3. Tenderer's actual or intended country of registration: *[insert actual or intended country of registration]*
4. Tenderer's year of registration: *[insert Tenderer's year of registration]*
5. Tenderer's Address in country of registration: *[insert Tenderer's legal address in country of registration]*
6. Tenderer's Authorized Representative Information Name: *[insert Authorized Representative's name]* Address: *[insert Authorized Representative's Address]* Telephone/Fax numbers: *[insert Authorized Representative's telephone/fax numbers]* Email Address: *[insert Authorized Representative's email address]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or documents of registration of the legal entity named above, in accordance with ITT 4.4. ☐ In case of JV, Form of intent to form JV or JV agreement, in accordance with ITT 4.1. ☐ In case of state-owned enterprise or institution, in accordance with ITT 4.6 documents establishing: • Legal and financial autonomy • Operation under commercial law • Establishing that the Tenderer is not under the supervision of the Procuring Entity ☐ Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

3. Form ELI-1 Tenderer's JV Members Information Form

[The Tenderer shall fill in this Form in accordance with the instructions indicated below. The following table shall be filled in for the Tenderer and for each member of a Joint Venture].

Date: .....*[insert date (as day, month, and year) of Tender submission*]

ITT No.: .....*[insert number of Tendering process]*

Alternative No.: .....*[insert identification No if this is a Tender for an*

alternative] Page_____of_____pages

1. Tenderer's Name: *[insert Tenderer's legal name]*
2. Tenderer's JV Member's name: *[insert JV's Member legal name]*
3. Tenderer's JV Member's country of registration: *[insert JV's Member country of registration]*
4. Tenderer's JV Member's year of registration: *[insert JV's Member year of registration]*
5. Tenderer's JV Member's legal address in country of registration: *[insert JV's Member legal address in country of registration]*
6. Tenderer's JV Member's authorized representative information Name: *[insert name of JV's Member authorized representative]* Address: *[insert address of JV's Member authorized representative]* Telephone/Fax numbers: *[insert telephone/fax numbers of JV's Member authorized representative]* Email Address: *[insert email address of JV's Member authorized representative]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or registration documents of the legal entity named above, in accordance with ITT 4.4. ☐ In case of a state-owned enterprise or institution, documents establishing legal and financial autonomy, operation in accordance with commercial law, and they are not under the supervision of the Procuring Entity in accordance with ITT 4.6. ☐ Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

4. Form CON–1 Historical Contract Non-Performance and Pending Litigation.

In case a pre-qualification process was conducted this form should be used only if the information submitted at the time of pre-qualification requires updating

Tenderer's Legal Name:_____ Date:_____

JV member Legal Name: _____

ITT No.: _____

Age of_____ pages

Non-Performing Contracts in accordance with Section III, Evaluation and Qualification Criteria			
Contract non-performance did not occur during the stipulated period, in accordance with Sub- Factor 2.2.1 of Section III, Evaluation Criteria			
Pending Litigation, in accordance with Section III, Evaluation and Qualification Criteria			
No pending litigation in accordance with Sub-Factor 2.2.3 of Section III, Evaluation Criteria Pending litigation in accordance with Sub-Factor 2.2.3 of Section III, Evaluation Criteria, as indicated below			
Year	Outcome as Percent of Total Assets	Contract Identification	Total Contract Amount (current value, US$ equivalent)
_____	_____	Contract Identification: Name of Procuring Entity: Address of Procuring Entity: Matter in dispute:	_____
_____	_____	Contract Identification: Name of Procuring Entity: Address of Procuring Entity: Matter in dispute:	_____

5. Form EXP - 1 Experience – General Experience

Tenderer's Legal Name:_____ Date:_____

JV Member Legal Name:_____ ITT No.: _____

Page_____ of_____ pages

Starting Month / Year	Ending Month / Year	Years*	Contract Identification	Role of Tenderer
_____	_____		Contract name: Brief Description of the Information System performed by the Tenderer: Name of Procuring Entity: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Tenderer: Name of Procuring Entity: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Tenderer: Name of Procuring Entity: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Tenderer: Name of Procuring Entity: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Tenderer: Name of Procuring Entity: Address:	_____
_____	_____		Contract name: Brief Description of the Information System performed by the Tenderer: Name of Procuring Entity: Address:	_____

*List calendar year for years with contracts with at least nine (9) months activity per year starting with the earliest year.

6. Form EXP – 2 Specific Experience

Tenderer's Legal Name: _____ Date: _____
JV Member Legal Name: _____ ITT No.: _____

Page _____ of _____ pages

Similar Contract Number: ___ of ___ required.	Information
Contract Identification	_____
Award date Completion date	_____ _____

Similar Contract Number: ___ of ___ required.	**Information**		
Role in Contract	☐ Prime Supplier	☐ Management Contractor	☐ Subcontractor
Total contract amount	_____		US$_____
If member in a JV or subcontractor, specify participation of total contract amount	_____%	_____	US$_____
Procuring Entity's Name:	_____		
Address: Telephone/fax number: E-mail:	_____ _____ _____ _____		

7. Form EXP – 2 (cont.) Specific Experience (cont.)

Tenderer's Legal Name: _____ Page _____ of _____ pages
JV Member Legal Name: _____

Similar Contract No. __ [insert specific number] of [total number of contracts] ___ required	**Information**
Description of the similarity in accordance with Sub-Factor 2.4.2 of Section III:	
Amount	_____
Physical size	_____
Complexity	_____
Methods/Technology	_____
Key Activities	_____

8. Form CCC-1 Summary Sheet: Current Contract Commitments/ Work in Progress

Name of Tenderer or partner of a Joint Venture.

Tenderers and each partner to a Joint Venture tender should provide information on their current commitments on all contracts that have been awarded, or for which a Form of intent or acceptance has been received, or for contracts approaching completion, but for which an unqualified, full completion certificate has yet to be issued

Name of contract	**Procuring Entity, contact address/tel./fax**	**Value of outstanding Information System (curre US$ equivalent)**	**Estimated completio date**	**Average monthly invoicin over last six months (US$/month)**
1.				
2.				
3.				

4.				
5.				
etc.				

9. Form FIN – 1 Financial Situation

Historical Financial Performance

Tenderer's Legal Name: _____Date: _____

JV Member Legal Name: _____ITT No._____

Page _____ of _____ pages

To be completed by the Tenderer and, if JV, by each member

Financial information in US$ equivalent	Historic information for previous _____ (__) years (US$ equivalent in 000s)						
	Year 1	Year 2	Year 3	Year …	Year n	Avg.	Avg. Ratio
Information from Balance Sheet							
Total Assets (TA)							
Total Liabilities (TL)							
Net Worth (NW)							
Current Assets (CA)							
Current Liabilities (CL)							
Information from Income Statement							
Total Revenue (TR)							
Profits Before Taxes (PBT)							

Attached are copies of financial statements (balance sheets, including all related notes, and income statements) for the years required above complying with the following conditions:

a) Must reflect the financial situation of the Tenderer or member to a JV, and not sister or parent companies.

b) Historic financial statements must be audited by a certified accountant.

c) Historic financial statements must be complete, including all notes to the financial statements.

d) Historic financial statements must correspond to accounting periods already completed and audited (no statements for partial periods shall be requested or accepted).

---

10. Form FIN –2 Average Annual Turnover

Tenderer's Legal Name: _____ Date: _____

JV Member Legal Name: _____ ITT No.: _____

Page _____ of _____ pages

Annual turnover data (applicable activities only)		
Year	Amount and Currency	US$ equivalent

	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
*Average Annual Turnover	_____	_____

*Average annual turnover calculated as total certified payments received for work in progress or completed, divided by the number of years specified in Section III, Evaluation and Qualification Criteria, Sub-Factor 2.3.2.

11. Form F-3 Financial Resources

Specify proposed sources of financing, such as liquid assets, unencumbered real assets, lines of credit, and other financial means, net of current commitments, available to meet the total cash flow demands of the subject contract or contracts as indicated in Section III, Evaluation and Qualification Criteria.

Source of financing	**Amount (US$ equivalent)**
1.	
2.	
3.	
4.	

12. Personnel Capabilities

i) Key Personnel

Name of Tenderer or partner of a Joint Venture

Tenderers should provide the names and details of the suitably qualified Personnel to perform the Contract. The data on their experience should be supplied using the Form PER-2 below for each candidate.

1.	**Title of position:** ...	
	Name of candidate:	
	Duration of appointment:	[*insert the whole period (start and end dates) for which this position will be engaged*]
	Time commitment: for this position:	[*insert the number of days/week/months/ that has been scheduled for this position*]
	Expected time schedule for this position:	[*insert the expected time schedule for this position (e.g., attach high level Gantt chart*]
2.	**Title of position: …**	
	Name of candidate:	
	Duration of appointment:	[*insert the whole period (start and end dates) for which this position will be engaged*]

	Time commitment: for this position:	[*insert the number of days/week/months/ that has been scheduled for this position*]
	Expected time schedule for this position:	[*insert the expected time schedule for this position (e.g., attach high level Gantt chart*]
3.	**Title of position:** *...*	
	Name of candidate:	
	Duration of appointment:	[*insert the whole period (start and end dates) for which this position will be engaged*]
	Time commitment: for this position:	[*insert the number of days/week/months/ that has been scheduled for this position*]
	Expected time schedule for this position:	[*insert the expected time schedule for this position (e.g., attach high level Gantt chart*]
4.	**Title of position:**	
	Name of candidate	
	Duration of appointment:	[*insert the whole period (start and end dates) for which this position will be engaged*]
	Time commitment: for this position:	[*insert the number of days/week/months/ that has been scheduled for this position*]
	Expected time schedule for this position:	[*insert the expected time schedule for this position (e.g., attach high level Gantt chart*]
6...	**Title of position:**	
	Name of candidate	
	Duration of appointment:	[*insert the whole period (start and end dates) for which this position will be engaged*]
	Time commitment: for this position:	[*insert the number of days/week/months/ that has been scheduled for this position*]
	Expected time schedule for this position:	[*insert the expected time schedule for this position (e.g., attach high level Gantt chart*]

ii) Candidate Summary

Position		**Candidate** ☐ Prime ☐ Alternate
Candidate information	Name of candidate	Date of birth
	Professional qualifications	
Present employment	Name of Employer	
	Address of Employer	
	Telephone	Contact (manager / personnel officer)
	Fax	Email
	Job title of candidate	Years with present Employer

Summarize professional experience over the last twenty years, in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.

From	To	Company/Project/ Position/Relevant technical and management experience

iii) **Technical**

Tenderer shall provide adequate information to demonstrate clearly that it has the technical capability to meet the requirements for the Information System. With this form, the Tenderer should summarize important certifications, proprietary methodologies, and/or specialized technologies that the Tenderer proposes to utilize in the execution of the Contract or Contracts.

(iv) Manufacturer's Authorization

Note: This authorization should be written on the Form head of the Manufacturer and be signed by a person with the proper authority to sign documents that are binding on the Manufacturer.

Invitation for Tenders Title and No.:_____[*Procuring Entity insert:* ***ITT Title and Number****]*

To:_____[*Procuring Entity insert:* ***Procuring Entity's Officer to receive the Manufacture's Authorization****]*

WHEREAS *[insert:* ***Name of Manufacturer****]* who are official producers of_____*[insert:* ***items of supply by Manufacturer****]* and having production facilities at_____*[insert:* ***address of Manufacturer****]* do here by authorize_____*[insert:* ***name of Tenderer or Joint Venture****]* located at_____*[insert:* ***address of Tenderer or Joint Venture****]* (hereinafter, the "Tenderer") to submit a tender and subsequently negotiate and sign a Contract with you for resale of the following Products produced by us:

We hereby confirm that in case the tendering results in a Contract between you and the Tenderer, the above-listed products will come with our full standard warranty.

Name *[insert:* ***Name of Officer****]* in the capacity of *[insert:* ***Title of Officer]*** Signed_____

Duly authorized to sign the authorization for and on behalf of:_____*[insert:* ***Name of Manufacturer****]*

Dated this_____*[insert* ***ordinal****]* day of _____ [*insert* ***month****]*, *[insert* ***year****]*. *[add Corporate Seal*

(where appropriate)]

(v) Subcontractor's Agreement

Note: This agreement should be written on the Form head of the Subcontractor and be signed by a person with the proper authority to sign documents that are binding on the Subcontractor.

Invitation for Tenders Title and No.:_____[*Procuring Entity insert:* ***ITT Title and Number****]*

To:_____[*Procuring Entity insert:* ***Procuring Entity's Officer to receive the Subcontractor's Agreement]***

WHERE AS *[insert:* ***Name of Subcontractor****],* having head offices at_____*[insert* ***address of Subcontractor****],* have been informed by_____*[insert* ***name of Tenderer or Joint Venture****] located* at _____*[insert* ***address of Tenderer or Joint Venture****]* (here in after, the "Tenderer") that it will submit a tender in which_____*[insert* ***Name of Subcontractor****]* will provide_____[*insert* ***items of supply or services provided by the Subcontractor****].* We hereby commit to provide the above-named items, in the

instance that the Tenderer is awarded the Contract.

Name *[insert: **Name of Officer**]*in the capacity of_____*[insert: **Title of Officer]***

Signed_____ Duly authorized to sign the authorization for and on

behalf of:_____*[insert: **Name of Subcontractor]***

Dated this_____*[insert **ordinal]*** day of_____[*insert **month]***, _____ *[insert **year]***.

[add Corporate Seal (where appropriate)]

v) List of Proposed Subcontractors

	Item	**Proposed Subcontractor**	**Place of Registration & Qualifications**

13. Intellectual Property Forms

Notes to Tenderers on working with the Intellectual Property Forms

In accordance with ITT 11.1(j), Tenderers must submit, as part of their tenders, lists of all the Software included in the tender assigned to one of the following categories: (A) System, General-Purpose, or Application Software; or (B) Standard or Custom Software. Tenderers must also submit a list of all Custom Materials. These categorizations are needed to support the Intellectual Property in the GCC and SCC.

i) Software List

	(Select one per item)			(Select one per item)	
Software Item	System Software	General-Purpose Software	Application Software	Standard Softwa	Custom Softwar

	(Select one per item)			(Select one per item)	
Software Item	System Software	General-Purpose Software	Application Software	Standard Softwa	Custom Softwar

ii) List of Custom Materials

Custom Materials

14. Conformance of Information System Materials

I) Format of the Technical Tender

In accordance with ITT 16.2, the documentary evidence of conformity of the Information System to the tendering documents includes (but is not restricted to):

a) The Tenderer's Preliminary Project Plan, including, but not restricted, to the topics specified in the TDS ITT 16.2. The Preliminary Project Plan should also state the Tenderer's assessment of the major responsibilities of the Procuring Entity and any other involved third parties in System supply and installation, as well as the Tenderer's proposed means for coordinating activities by each of the involved parties to avoid delays or interference.

b) A written confirmation by the Tenderer that, if awarded the Contract, it shall accept responsibility for successful integration and interoperability of all the proposed Information Technologies included in the System, as further specified in the Technical Requirements.

c) Item-by-Item Commentary on the Technical Requirements demonstrating the substantial responsiveness of the overall design of the System and the individual Information Technologies, Goods, and Services offered to those Technical Requirements.

In demonstrating the responsiveness of its tender, the Tenderer must use the Technical Responsiveness Checklist (Format). Failure to do so increases significantly the risk that the Tenderer's Technical Tender will be declared technically non-responsive. Among other things, the checklist should contain explicit cross-references to the relevant pages in supporting materials included the Tenderer's Technical Tender.

Note: The Technical Requirements are voiced as requirements of the *Supplier* and/or the *System*. The Tenderer's response must provide clear evidence for the evaluation team to assess the credibility of the response. A response of "yes" or "will do" is unlikely to convey the credibility of the response. The Tenderer should indicate *that*–and to the greatest extent practical–*how* the Tenderer would comply with the requirements if awarded the contract. Whenever the technical requirements relate to feature(s) of existing products (e.g., hardware or software), the features should be described, and the relevant product literature referenced. When the technical requirements relate to professional services (e.g., analysis, configuration, integration, training, etc.) some effort should be expended to describe how they would be rendered – not just a commitment to perform the [cut-and-paste] requirement. Whenever a technical requirement is for the Supplier to provide certifications (e.g., ISO9001), copies of these certifications must be included in the Technical Tender.

Note: The Manufacture's Authorizations (and any Subcontractor Agreements) are to be included in Attachment 2 (Tenderer Qualifications), in accordance with and ITT 15.

Note: As a matter of practice, the contract cannot be awarded to a Tenderer whose Technical Tender deviates (materially) from the Technical Requirements – *on any Technical Requirement*. Such deviations include omissions (e.g., non-responses) and responses that do not meet or exceed the requirement. Extreme care must be exercised in the preparation and presentation of the responses to all the Technical Requirements.

d) Supporting materials to underpin the Item-by-item Commentary on the Technical Requirements (e.g., product literature, white-papers, narrative descriptions of technical approaches to be employed, etc.). In the interest of timely tender evaluation and contract award, Tenderers are encouraged not to overload the supporting materials with documents that do not directly address the Procuring Entity's requirements.

e) Any separate and enforceable contract(s) for Recurrent Cost items which the TDSITT17.2 required Tenderers to tender.

Note: To facilitate tender evaluation and contract award, Tenderers encouraged to provide electronic copies of their Technical Tender–preferably in a format that the evaluation team can extract text from to facilitate the tender clarification process and to facilitate the preparation of the Tender Evaluation Report.

ii) Technical Responsiveness Checklist (Format)

Tech. Require. No. _	**Technical Requirement:** ***[insert: abbreviated description of Requirement]***
Tenderer's technical reasons supporting compliance:	
Tenderer's cross references to supporting information in Technical Tender:	

FORM OF TENDER SECURITY- [Option 1–Demand Bank Guarantee]

Beneficiary:_____

Request forTenders No:

_____

Date:_____

TENDER GUARANTEE No.:_____

Guarantor: _____

1. We have been informed that_____(here inafter called "the Applicant") has submitted or will submit to the Beneficiary its Tender (here inafter called" the Tender") for the execution of_____ under Request for Tenders No._____("the ITT").

2. Furthermore, we understand that, according to the Beneficiary's conditions, Tenders must be supported by a Tender guarantee.

3. At the request of the Applicant, we, as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of_____(_____) upon receipt by us of the Beneficiary's complying demand, supported by the Beneficiary's statement, whether in the demand itself or a separate signed document accompanying or identifying the demand, stating that either the Applicant:

(a) has withdrawn its Tender during the period of Tender validity set forth in the Applicant's Letter of Tender ("the Tender Validity Period"), or any extension thereto provided by the Applicant; or

b) having been notified of the acceptance of its Tender by the Beneficiary during the Tender Validity Period or any extension there to provided by the Applicant, (i) has failed to execute the contract agreement, or (ii) has failed to furnish the Performance.

4. This guarantee will expire: (a) if the Applicant is the successful Tenderer, upon our receipt of copies of the contract agreement signed by the Applicant and the Performance Security and, or (b) if the Applicant is not the successful Tenderer, upon the earlier of (i) our receipt of a copy of the Beneficiary's notification to the Applicant of the results of the Tendering process; or (ii) thirty days after the end of the Tender Validity Period.

5. Consequently, any demand for payment under this guarantee must be received by us at the office indicated above onor before that date.

_____

[signature(s)]

Note: All italicized text is for use in preparing this form and shall be deleted from the final product.

FORMAT OF TENDER SECURITY [Option 2–Insurance Guarantee] NOT APPLICABLE

TENDER GUARANTEE No.: _____

1. Whereas …… [*Name of the tenderer]* (hereinafter called "the tenderer") has submitted its tender dated …… [*Date of submission of tender]* for the …… *[Name and/or description of the tender]* (hereinafter called "the Tender") for the execution of under Request for Tenders No. _____("the ITT").

2. KNOW ALL PEOPLE by these presents that WE …… of …… [**Name of Insurance Company**] having our registered office at …… (hereinafter called "the Guarantor"), are bound unto ……. [*Name of Procuring Entity*] (hereinafter called "the Procuring Entity") in the sum of …… (Currency and guarantee amount) for which payment well and truly to be made to the said Procuring Entity, the Guarantor binds itself, its successors, and assigns, jointly and severally, firmly by these presents.

   Sealed with the Common Seal of the said Guarantor this ___day of _____ 20 __.

3. NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION is such that if the Applicant:

   a) has withdrawn its Tender during the period of Tender validity set forth in the Principal's Letter of Tender ("the Tender Validity Period"), or any extension thereto provided by the Principal; or

   b) having been notified of the acceptance of its Tender by the Procuring Entity during the Tender Validity Period or any extension thereto provided by the Principal; (i) failed to execute the Contract agreement; or (ii) has failed to furnish the Performance Security, in accordance with the Instructions to tenderers ("ITT") of the Procuring Entity's Tendering document.

   then the guarantee undertakes to immediately pay to the Procuring Entity up to the above amount upon receipt of the Procuring Entity's first written demand, without the Procuring Entity having to substantiate its demand, provided that in its demand the Procuring Entity shall state that the demand arises from the occurrence of any of the above events, specifying which event(s) has occurred.

4. This guarantee will expire: (a) if the Applicant is the successful Tenderer, upon our receipt of copies of the contract agreement signed by the Applicant and the Performance Security and, or (b) if the Applicant is not the successful Tenderer, upon the earlier of (i) our receipt of a copy of the Beneficiary's notification to the Applicant of the results of the Tendering process; or (ii)twenty-eight days after the end of the Tender Validity Period.

5. Consequently, any demand for payment under this guarantee must be received by us at the office indicated above on or before that date.

_____	_____
[Date]	*[Signature of the Guarantor]*
_____	_____
[Witness]	*[Seal]*

Note: All italicized text is for use in preparing this form and shall be deleted from the final product.

TENDER - SECURING DECLARATION FORM {r 46 and155(2)}

[The Bidder shall complete this Form in accordance with the instructions indicated] Date: .....

[insert date (as day, month and year) of Tender Submission]

Tender No.: ..... *[insert number of tendering process]*

To: ..... *[insert complete name of Purchaser]* I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Tender-Securing Declaration.

2. I/We accept that I/we will automatically be suspended from being eligible for tendering in any contract with the Purchaser for the period of time of [insert number of months or years] starting on [insert date], if we are in breach of our obligation (s) under the bid conditions, because we–(a) have withdrawn our tender during the period of tender validity specified by us in the Tendering Data Sheet; or (b) having been notified of the acceptance of our Bid by the Purchaser during the period of bid validity, (i) fail or refuse to execute the Contract, if required, or (ii) fail or refuse to furnish the Performance Security, in accordance with the instructions to tenders.

3. I/We understand that this Tender Securing Declaration shall expire if we are not the successful Tenderer(s), upon the earlier of:
   a) Our receipt of a copy of your notification of the name of the successful Tenderer; or
   b) thirty days after the expiration of our Tender.

4. I/We understand that if I am/ we are/ in a Joint Venture, the Tender Securing Declaration must be in the name of the Joint Venture that submits the bid, and the Joint Venture has not been legally constituted at the time of bidding, the Tender Securing Declaration shall be in the names of all future partners as named in the letter of intent.

Signed: …….…….....

Capacity / title (director or partner or sole proprietor, etc.) …….…….....…….

Name: …….....

Duly authorized to sign the bid for and on behalf of: _____ [insert complete name of Tenderer] Dated

on……. day of…….……. [Insert date of signing]

Seal or stamp

PART 2 – CENTRAL BANK OF KENYA'S REQUIREMENTS

SECTION V – BILL OF QUANTITIES FOR THE SUPPLY, INSTALLATION, TRAINING AND COMMISSIONING OF INTEGRATED SECURITY SYSTEM

SN	ITEM	Description	Unit	Qty	Price per Unit KES	Total Price KES
1	Engineering and project management					
1.1	Project management - big site	Project planning, scheduling, progress monitoring, coordination with stakeholders, site coordination, documentation and reporting, as well as logistics including transportation, customs clearance (if applicable), storage, handling, and distribution of all materials and equipment necessary for project completion. Price is for site	Complete	3		

1.2	Project management - samll site	Project planning, scheduling, progress monitoring, coordination with stakeholders, site coordination, documentation and reporting, as well as logistics including transportation, customs clearance (if applicable), storage, handling, and distribution of all materials and equipment necessary for project completion. Price is for site	Complete	7		
1.3	Engineering - big site	Detailed design of each ISS component, integration to full operating system, QA management, Acceptance tests, Reliability tests, System Commissioning, Project Management, general support to the client and all other efforts required to fulfil successfully the ISS project	Complete	3		
1.4	Engineering - small site	Detailed design of each ISS component, integration to full operating system, QA management, Acceptance tests, Reliability tests, System Commissioning, Project Management, general support to the client and all other efforts required to fulfil successfully the ISS project	Complete	7		
1.5	Project documentation	Project documentation including the following: PDR, CDR, FAT, ATP,As Made Drawings, System description, operating instuctions and maintenance manual. Each in 2 printed copies + software copy	Complete	10		
1.6	Training of control room operators	Minimum 3-day on-site training for control room operators - per site	Complete	10		
1.7	Integration and configuration	Integration and configuration of all subsystems into the complete ISS system, including database setup, map configuration, and definition of operational procedures and workflows	Complete	10		
2.4	LPR - UVSS	Development of interfaces between Under Vehicle Surveillance System (UVSS) with the License Plate Recognition (LPR) system. Including all software configurations, interfaces, cabling, testing, and works required to ensure complete functional integration and successful operation.	Complete	1		

C2: CBK - Official

2.5	VMS - RADAR	Development of interfaces between Video Management System with the Radar system. Including all software configurations, interfaces, cabling, testing, and works required to ensure complete functional integration and successful operation.	Complete	2		
3	Physical security information management system					
3.1	PSIM software application - for Main Control Center	Supply and installation of PSIM software for the Main control center. Including all licenses, databases, configuration, customization, and interfaces for full operation. Including licence for Hot backup	Complete	10		
3.2	PSIM software application - for site	Supply and installation of PSIM software for single site. Including all licenses, databases, configuration, customization, and interfaces for full operation. Including licence for Hot backup	Complete	10		
3.3	PSIM site license	PSIM license for site (federation topology)	Complete	20		
3.4	End devices license	Supply of license for End devices (Cameras, IDS sensors, ACS field elements, PA speakers, and other end devices). Price is per End device	Pcs	3,439		
3.5	PSIM Client workstation	Supply and installation of PSIM client workstation with support for six screens, including all hardware, software, licenses, configuration, accessories, cables, and labor for full operation. Including mouse and keyboard	Pcs	52		
3.6	24-inch monitor	Supply and installation of 24" viewing screen, including all accessories and labor for full operation	Pcs	156		
3.7	27-inch monitor	Supply and installation of 27" viewing screen, including all accessories and labor for full operation	Pcs	22		
3.8	PSIM Client license	Supply of PSIM client license, including all required software components, configurations, and works necessary for complete installation and successful operation.	Pcs	52		
3.9	Licence for IDS module	Supply of licence for IDS module	Pcs	20		

C2: CBK - Official

3.10	Licenc for ACS module	Supply of licence for ACS module	Pcs	20		
3.11	Licenc for PA module	Supply of licence for PA module	Pcs	20		
3.12	Licenc for LPR module	Supply of licence for LPR module	Pcs	20		
3.13	Licenc for AI module	Supply of licence for AI module	Pcs	20		
3.14	License for interface with cyber security system	Provision of a software license for interfacing and integration with the cybersecurity system.	Complete	20		
3.15	Licenc for electric Fence module	Supply of licence for electric fence module	Pcs	20		
3.16	GIS engine	Supply, installation, configuration, and commissioning of an enterprise GIS engine including spatial database, map rendering, geospatial analysis, geofencing, and integration APIs, fully integrated with the PSIM platform.Including 6 user licenses	Complete	20		
4	Servers, storage & clients					
4.1	VMS Recording Server	Supply, installation, configuration, testing and commissioning of a complete recording server, including all hardware, operating system, SSDs, enterprise-grade recording HDDs, RAID capacity and accessories, sized for a maximum of 70 cameras per server and a minimum of 30 days continuous recording retention, at the camera resolutions and recording parameters specified in the Technical Specifications. The required retention capacity shall be provided as usable storage after RAID and system overhead.	Pcs	45		
4.2	VMS Management Server	Supply, installation, configuration, testing and commissioning of a complete rack-mounted server for the Video Management System, including operating system and all required server-related licences, hardware, accessories, rack-mounting components, power cords, firmware and configuration, in full accordance with the Technical	Pcs	9		

C2: CBK - Official

		Specifications. All supplied licences shall be registered in the name of the Employer.				
4.3	PSIM Server	Supply, installation, configuration, testing and commissioning of a complete rack-mounted server for the Physical Security Information Management (PSIM) system, including operating system, all required server-related licences, hardware, accessories, rack-mounting components, power cords, firmware and configuration, in full accordance with the Technical Specifications. All supplied server-related licences shall be registered in the name of the Employer.	Pcs	27		
4.4	ACS Server	Supply, installation, configuration, testing and commissioning of a complete server for the Access Control System (ACS), including operating system, database software and all required server-related licences, hardware, monitor, keyboard, mouse, accessories, rack-mounting components where applicable, power cords, firmware and configuration, in full accordance with the Technical Specifications. All supplied server-related licences shall be registered in the name of the Employer.	Pcs	4		
4.5	LPR Server	Supply, installation, configuration, testing and commissioning of a complete server for the License Plate Recognition (LPR) system, including operating system, database software and all required server-related licences, hardware, accessories, rack-mounting components where applicable, power cords, firmware and configuration, in full accordance with the Technical Specifications. All supplied server-related licences shall be registered in the name of the Employer.	Pcs	4		

C2: CBK - Official

4.6	UVSS Server	Supply, installation, configuration, testing and commissioning of a complete server or processing unit for the Under Vehicle Surveillance System (UVSS), including operating system, database software where required, all server-related licences, hardware, accessories, rack-mounting components where applicable, power cords, firmware and configuration, in full accordance with the Technical Specifications. All supplied server-related licences shall be registered in the name of the Employer.	Pcs	1		
4.7	Radar Server	Supply, installation, configuration, testing and commissioning of a complete server for the radar detection and tracking system, including operating system, database software where required, all server-related licences, hardware, accessories, rack-mounting components where applicable, power cords, firmware and configuration, in full accordance with the Technical Specifications. All supplied server-related licences shall be registered in the name of the Employer.	Pcs	1		
4.8	LiDAR Radar Server	Supply, installation, configuration, testing and commissioning of a complete server for the LiDAR radar detection, tracking and analytics system, including operating system, database software where required, all server-related licences, hardware, accessories, rack-mounting components where applicable, power cords, firmware and configuration, in full accordance with the Technical Specifications. All supplied server-related licences shall be registered in the name of the Employer.	Pcs	1		
4.9	Management Out-of-Band server	Management Server - Out-of-Band windows 2023 server, including all adapters required for its operation	Complete	9		

C2: CBK - Official

4.10	NTP server	Supply, installation, configuration, testing, and commissioning of a dedicated time synchronization server to provide accurate and reliable time distribution across all networked systems. Including enterprise-grade server, NTP software/license, network interfaces, rack mounting, power and network connections, configuration of NTP services, synchronization with external reference source (GPS / GNSS / upstream NTP source), integration with servers, VMS, access control, and security systems, testing, commissioning, documentation, and handover in full operational condition, in accordance with manufacturer's recommendations and project requirements. Including outdoor antena	Complete	9		
5	CCTV cameras					
5.1	5 MP AI IR Dome camera	Supply and installation of 5 MP AI Dome camera with built-in AI video analytics, Vari focal 2.8 - 12 MM, with IR capability for up to 15 meters, including all necessary cables, accessories, connectors, power supplies, materials, and labor required for complete installation and full operational functionality.	Pcs	508		
5.2	5 MP AI IR Bullet camera	Supply and installation of 5 MP AI Bullet camera with built-in AI video analytics, Vari focal 2.8 - 12 MM, with IR capability for up to 50 meters, including all necessary cables, accessories, connectors, power supplies, materials, and labor required for complete installation and full operational functionality.	Pcs	372		
5.3	8 MP AI IR Dome camera	Supply and installation of 8 MP AI Dome camera with built-in AI video analytics, Vari focal 2.8 - 12 MM, with IR capability for up to 30 meters, including all necessary cables, accessories, connectors, power supplies, materials, and labor required for complete installation and full operational functionality.	Pcs	119		

C2: CBK - Official

5.4	8 MP AI IR Bullet camera	Supply and installation of 8 MP AI Bullet camera with built-in AI video analytics, Vari focal 2.8 - 12 MM, with IR capability for up to 30 meters, including all necessary cables, accessories, connectors, power supplies, materials, and labor required for complete installation and full operational functionality.	Pcs	209		
5.5	PTZ camera 4 MP	Supply and installation of 4 MP PTZ camera , X30, with IR capability for up to 150 meters, including all necessary cables, accessories, connectors, power supplies, materials, and labor required for complete installation and full operational functionality.	Pcs	20		
5.6	Thermal camera 19/25/35mm	Supply and installation of a fixed thermal camera with 640 × 512 resolution, 19/25/35mm focal length, and built-in analytics suitable for harsh outdoor conditions. The camera shall include audio line input/output, relay input/output, and an IP66-rated enclosure. Including power supply, all works for installation, integration, housing/cabling, and all necessary accessories required for full operation of the camera. The lens will be supplied according to the actual design.	Pcs	70		
5.7	Camera pole, 10 meter	Design, supply, and installation of a 10-meter dedicated camera pole, including all necessary civil design, materials, and labor required for the installation. Price include the base for the pole.	Pcs	2		
5.8	Wall-mounted camera pole	Design, supply, and installation of a wall-mounted camera pole, including all necessary civil design, materials and labour required for the installation. Including grounding	Pcs	581		
6	Video management system					
6.1	VMS base license	VMS base license.	Complete	10		
6.2	Video channel license	License for video channel/Audio	Pcs	2,036		

C2: CBK - Official

6.3	Failover license for VMS server	Supply of a Failover license for the VMS server, enabling automatic failover to a secondary VMS server in the event of primary server failure. The scope includes all necessary configuration, activation, and testing to guarantee full functionality of the Hot Standby setup.	Pcs	10		
6.4	Failover license for video channel	Supply of a Failover license per video channel. Price per video channel	Pcs	2,036		
6.5	VMS client workstation	Supply and installation of a VMS viewing workstation, including hardware, operating system, and all other software required for station operation. Including installation, as well as all cables, materials, accessories, and works necessary for complete installation and proper operation. Including 27'' LED monitor, keyboard and mouse	Complete	22		
6.6	VMS client license	Supply of VMS client license, including all required software components, configurations, and works necessary for complete installation and successful operation.	Pcs	22		
6.7	Virtual matrix license	Supply and installation of a virtual matrix, including software, licenses, and all works necessary for complete installation, configuration, and proper operation.	Pcs	9		
7	Perimeter surveillance radar					
7.1	Site license	Supply of radar system site license, including all required modules and features necessary for full operation and integration of the radar system.	Pcs	1		
7.2	Radar system management software	Supply, installation and commissioning of radar software license including High Availability Hot Standby configuration with automatic failover, multi-sensor fusion engine with unique target ID assignment, AI-based clutter rejection and target classification, and self-calibration Suite with integrated GPS and digital compass. The scope includes full configuration, synchronization	Pcs	1		

C2: CBK - Official

		between primary and secondary servers and system commissioning.				
7.3	Radar unit, 250 meter	Supply, installation and commissioning of radar unit with detection range up to 250 meters, minimum 90-degree azimuth coverage, edge-based AI human and vehicle classification, tracking of minimum 100 targets and position accuracy of one meter or better. The item includes mounting arm or bracket, cabling, connectors, surge protection, power connection, grounding, alignment, calibration and full integration into the radar platform. The unit shall meet IP66 or IP67 protection rating	Complete	6		
7.4	Video channel license	AI license for a camera integrated with the radar system.	Pcs	6		
7.5	Client workstation license	License for operator workstations within a distributed RMS architecture including full integration and configuration.	Pcs	2		
7.6	Client workstation	Supply and installation of a client workstation, including hardware, operating system, and all other software required for station operation. Including installation, as well as all cables, materials, accessories, and works necessary for complete installation and proper operation. Including 27" LED monitor, keyboard and mouse	Pcs	2		
7.7	System integration with VMS	Integration of Radar system with existing Video Management System such as Genetec, Milestone Systems or Hikvision including radar-to-camera auto cueing, alarm mapping and end-to-end testing.	Pcs	1		
8	LiDAR perimeter surveillance radar					
8.1	Site license	Supply of radar system site license, including all required modules and features necessary for full operation and integration of the radar system.	Pcs	1		

C2: CBK - Official

8.2	Radar system management software	Supply, installation and commissioning of radar software license including High Availability Hot Standby configuration with automatic failover, multi-sensor fusion engine with unique target ID assignment, AI-based clutter rejection and target classification, and self-calibration Suite with integrated GPS and digital compass. The scope includes full configuration, synchronization between primary and secondary servers and system commissioning.	Complete	1		
8.3	Long-range 3D LiDAR & AI-based perimeter detection unit	Supply, installation and commissioning of a 3D LiDAR radar unit with high-resolution laser imaging technology (LiDAR) with artificial intelligence (AI) processing, a detection range of at least 450 meters for human detection and 800 meters for vehicle detection. The item includes mounting arm or bracket, cabling, connectors, surge protection, power connection, grounding, alignment, calibration and full integration into the radar platform. The unit shall meet IP66 or IP67 protection rating	Pcs	5		
8.4	Video channel license	AI license for a camera integrated with the radar system.	Pcs	5		
8.5	Client workstation license	License for operator workstations within a distributed RMS architecture including full integration and configuration.	Psc	1		
8.6	Client workstation	Supply and installation of a client workstation, including hardware, operating system, and all other software required for station operation. Including installation, as well as all cables, materials, accessories, and works necessary for complete installation and proper operation. Including 27'' LED monitor, keyboard and mouse	Pcs	1		
8.7	System integration with VMS	Integration of Radar system with existing Video Management System such as Genetec, Milestone Systems or Hikvision including radar-to-camera auto cueing, alarm mapping and end-to-end testing.	Psc	1		

C2: CBK - Official

9	Multimedia					
9.1	HDMI Matrix Switch 4×4 with Scaler	Supply and installation of an HDMI matrix switch 4×4 with built-in scaler, enabling flexible routing of multiple HDMI sources to multiple displays with independent scaling per output. The unit shall support high-resolution video, centralized control, and integration with AV control systems, including all required accessories.	Pcs	7		
9.2	HDMI Matrix Switch 8X8 with Scaler	Supply and installation of an HDMI matrix switch 8X8 with built-in scaler, enabling flexible routing of multiple HDMI sources to multiple displays with independent scaling per output. The unit shall support high-resolution video, centralized control, and integration with AV control systems, including all required accessories.	Complete	2		
9.3	HDMI Matrix Switch 16X16 with Scaler	Supply and installation of an HDMI matrix switch 16X16 with built-in scaler, enabling flexible routing of multiple HDMI sources to multiple displays with independent scaling per output. The unit shall support high-resolution video, centralized control, and integration with AV control systems, including all required accessories.	Pcs	1		
9.6	4K HDMI Cat 6 Extender	Transmits 4K HDMI with zero latency: up to 40 m over Cat 6 Local HDMI output for cascade or monitoring. EDID Copying Mode for optimal resolution. PoC (Power over Cable) – powers receiver from transmitter via Cat 5e/6. Includes supply, installation, and commissioning.	Pcs	52		
9.7	Control box	Supply and installation of a second-generation control box for centralized IP-based control of AV and room systems, compatible with touch panels and peripheral devices, including all required accessories.	Psc	11		

C2: CBK - Official

9.8	10.1" touch control panel	Supply and installation of a 10.1" capacitive touch panel for IP-based control of AV and room systems, supporting PoE and fully compatible with the manufacturer's control system, including all required installation accessories include tabletop kit.	Pcs	18		
9.9	55" Professional video wall display with wall/ cileing mount	Supply, delivery, and installation of professional videio wall display with ultra-thin bezel for seamless video wall layouts, 24/7 operation, dust-proof. Connectivity: HDMI/DP/DVI-D/USB/LAN/RS232C; CMS support	Psc	52		
9.10	High Speed HDMI Cable with Ethernet 20 m	HDMI 2.0/1.4 cable, supports 4K 30Hz, HDMI Ethernet Channel (HEC) compatible, gold-plated HDMI connectors, 26 AWG tinned copper conductors, aluminum foil + PVC jacket, RoHS/UL/CSA rated, flexible for installation	Complete	52		
9.11	USB HDMI KVM Extender	Supply and installation of a USB/HDMI KVM extender for extending video, USB keyboard/mouse, audio and control signals over a single Cat6/6a cable, supporting 4K resolution and long-distance transmission, suitable for control rooms and secure installations, including all required accessories.	Complete	52		
10	AI system					
10.1	AI video channel	Software module for real-time video analysis based on artificial intelligence, enabling object detection and classification, smart alarm generation, and event search within a video management system.	Psc	50		
10.2	AI video forensic analytics channel	Supply of an AI-based software module for post-event video analysis, enabling advanced search, filtering, and forensic investigation of recorded video data on a per-channel basis.	Psc	50		
10.3	Facial recognition software license for camera	Supply and installation of AI-based facial recognition software, integrated with IP cameras, providing real-time alerts, area monitoring, and full connection to central servers. Includes calibration,	Psc	30		

C2: CBK - Official

		functional tests, training, backups, and software updates.				
11	Acsess Control System					
11.1	ACS software application	Supply and installation of Access Control System software application, including database, licenses, software programs, and all works and accessories required for complete installation and successful operation.	Complete	9		
11.2	Client workstation	Supply and installation of a client workstation, including hardware, operating system, and all other software required for station operation. Including installation, as well as all cables, materials, accessories, and works necessary for complete installation and proper operation. Including 27'' LED monitor, keyboard and mouse	Pcs	9		
11.3	ACS Client license	Supply of Access Control System (ACS) client license, including all software components, configurations, and works required for full installation and operation.	Psc	9		
11.4	ACS database/back up system	Supply and installation of ACS database/backup system, including servers, storage devices, network connections, software, and all accessories and works required for complete installation and successful operation.	Psc	9		
11.5	4 doors ACS controller	Supply and installation of 4-door Access Control System (ACS) controller, including ACS cabinet or the relevant part of the cabinet. Including all required power supplies, backup batteries,connections, mounting accessories, and all works necessary for complete installation and successful operation.	Psc	58		

C2: CBK - Official

11.6	2 doors ACS controller	Supply and installation of 2-door Access Control System (ACS) controller, including ACS cabinet or the relevant part of the cabinet. Including all required power supplies, backup batteries,connections, mounting accessories, and all works necessary for complete installation and successful operation.	Psc	423		
11.7	Combined RFID &Finger Print reader	Supply and installation of combined RFID and fingerprint reader, including all required power supplies, cabling, materials, mounting accessories, and works necessary for complete installation and successful operation.	Psc	50		
11.8	Combined Face recognition & RFID & Finger print reader	Supply and installation of combined face recognition, RFID, and fingerprint reader, including all required power supplies, cabling, materials, mounting accessories, and works necessary for complete installation and successful operation.	Psc	38		
11.9	600 lbs Electromagnetic lock, single door configuration	Supply and installation of a 600 lbs electromagnetic lock with LED indicator,for a single door configuration, including mechanical works and adaptations in the door, supply of power, cables, materials, accessories, and all works required for complete installation and successful operation.	Psc	450		
11.10	600 lbs Electromagnetic lock, double door configuration	Supply and installation of a 600 lbs electromagnetic lock with LED indicator for a double door configuration, including mechanical works and adaptations in the door, supply of power, cables, materials, accessories, and all works required for complete installation and successful operation.	Psc	117		
11.11	300 lbs Electromagnetic lock, for installation in communication rack	Supply and installation of a300 lbs electromagnetic lock with LED indicator for installation in a communication rack, including mechanical works and adaptations in the door, supply of power, cables, materials, accessories, and all works required for complete	Psc	25		

C2: CBK - Official

		installation and successful operation.				
11.12	Electric strike lock	Supply, installation, connection, testing, and operation of a "normally open" type electric strike lock.	Psc	115		
11.13	Contactless Push to Exit button	Supply and installation of a contactless Push to Exit button, flash mounted or inside the wall, including supply of power, cables, materials, accessories, and all works required for complete installation and successful operation.	Psc	783		
11.14	Emergency door release unit	Supply and installation of an Emergency Door release unit, including mechanical works and adaptations needed for the installation, supply of power, cables, materials, accessories, and all works required for complete installation and successful operation.	Psc	793		
11.15	High-security magnetic door position switches	Supply and installation of High-security magnetic door position switch for indoor installation, including any mechanical works and adaptations to the door, cabling, materials, mounting accessories, and works necessary for complete installation and successful operation.	Psc	793		
11.16	Hydraulic door closer	Supply and installation of hydraulic door closer, including mechanical works and adaptations in the door, all required accessories, and works necessary for complete installation and successful operation.	Psc	20		
11.17	ACS enrolment and card production workstation	Supply and installation of ACS enrolment and card production workstation, including hardware and software for editing and producing color ID cards for permanent cardholders with personal photographs. Includes all required power supply, network communication, materials, accessories, tuner and works necessary for complete installation and successful operation. Includes biometric enrolment reader for	Psc	2		

C2: CBK - Official

		capturing fingerprints or other biometric data.				
11.18	Enrolment RFID reader	Supply and installation of an enrollment RFID reader for capturing and registering RFID cards or tags. Item includes all necessary hardware, mounting accessories, power supply, cabling, integration with the access control management system, testing, commissioning, and handover in full operational condition.	Psc	9		
11.19	Contactless smart cards	Supply of contactless smart cards with a minimum reading range of 15 cm, including any necessary programming, encoding, and works required for complete operation with the Access Control System.	Psc	1,200		
11.20	Data base	Transferring the database from the existing ACS to the new system, including data migration, configuration, verification, and all works required to ensure complete and successful operation	Complete	10		
11.21	Interface with fire detection system	Supply, installation, and configuration of interface with the the fire detection system, including all required hardware, software, cabling, accessories, and works for complete and proper integration and operation.	Complete	10		
11.22	Door alarm	Supply and installation of door-mounted electronic intrusion alarm with built-in siren (≥85 dB), magnetic contact detection, tamper protection, programmable alarm duration, and integration with access control or security system. Includes all necessary mounting hardware, wiring, and configuration for full operational readiness.	Pcs	15		
11.23	RFID reader	Supply and installation of RFID reader, including all required power supplies, cabling, materials, mounting accessories, and works necessary for complete installation and successful operation.	Pcs	780		

C2: CBK - Official

11.24	Installation and integration of controlled door	Installation and integration of controlled door elements, including all required cabling and connections between the controller and the door elements. Including the required cabling infrastructure between the controller and the controlled door.	Pcs	973		
12	Intrusion Detection System					
12.1	IDS controller, Grade 3	Supply, installation, and configuration of an Intrusion Detection System (IDS) controller, including all required modules and interfaces. Scope includes cabinet, power supply with circuit breaker, tamper switch, backup batteries, grounding, conduits, and all accessories and works necessary for complete installation, connection, and proper operation. The controller shall be certified to EN 50131-1 and EN 50131-3 Grade 3, or equivalent.	Complete	10		
12.2	Internal 8-zone expander, Grade 3	Supply and installation of an internal Grade 3 8-zone expander, including all necessary accessories and works required for full operation with the control panel.	Pcs	10		
12.3	32-zone expander, Grade 3	Supply and installation of a Grade 3, 32-zone expander, including enclosure, tamper, power supply, and all accessories and works required for operation of the expander with the control panel.	Pcs	46		
12.4	Keypad, Grade 3	Supply and installation of an Grade 3 keypad, including all accessories, wiring, and works required for complete installation and operation.	Pcs	25		
12.5	Wall-mounted detector, Grade 3	Supply and installation of a Grade 3 wall-mounted detector anti mask, including all necessary accessories and works required for complete installation and operation.	Pcs	50		
12.6	Ceiling-mounted detector anti mask, 4 m installation height, Grade 3	Supply and installation of a Grade 3, ceiling-mounted detector with an up to 4 m installation height, including all required accessories, mounting, wiring, and works necessary for complete and proper operation.	Pcs	320		

C2: CBK - Official

12.7	Ceiling-mounted detector, Anti mask 8 m installation height, Grade 3	Supply and installation of a Grade 3, ceiling-mounted detector with an up to 8 m installation height, including all required accessories, mounting, wiring, and works necessary for complete and proper operation.	Pcs	18		
12.8	Seismic detector, Grade 3	Supply and installation of a Grade 3 Seismic detector. Including all necessary accessories and works required for complete installation and operation.	Pcs	45		
12.9	Dual technologies detector, outdoor	Supply and installation of an outdoor dual-technology detector (PIR + MW), including all required accessories, mounting, wiring, and works necessary for complete and proper operation.	Pcs	32		
12.10	Panic button, Grade 3	Supply and installation of a Grade 3, Panic button for under-desk installation, with a cover to prevent accidental activation, including all accessories and works required for complete installation and operation.	Pcs	57		
12.11	Curtain detector, 10 meters detection range, Grade 3	Supply and installation of a Grade 3 indoor curtain detector with a detection range of up to 10 meters, including all necessary accessories, mounting hardware, wiring, and labor required for complete installation and full operational functionality.	Pcs	24		
12.12	Laser detector, Grade 3	Supply and installation of a Grade 3 laser detector, 20 × 20 m coverage, including all necessary accessories, hardware, wiring, and labor required for complete installation and full operational functionality.	Pcs	7		
12.13	High-security magnetic switch	Supply and installation of a high-security magnetic switch, including all accessories and works required for complete installation and operation.	Pcs	87		
12.14	Heavy duty magnet	Supply and installation of a Heavy duty magnet, including all accessories and works required for complete installation and operation.	Pcs	45		
12.15	Internal sounder/strobe, Grade 3	Supply and installation of an Grade 3 internal sounder/strobe, including all accessories and works required for complete installation and operation.	Pcs	24		

C2: CBK - Official

12.16	External sounder/strobe, Grade 3	Supply and installation of an Grade 3 external sounder/strobe, including all accessories and works required for complete installation and operation.	Pcs	44		
12.17	Installation and integration of IDS field element	Installation an integration of IDS field element, including all required cabling and connections between the IDS controller and the sensor or element. Including the required cabling infrastructure between the IDS controller and the sensor/element.	Pcs	758		
13	Public address system					
13.1	Horn speaker	Supply and installation of an IP public address (PA) horn speaker for outdoor installation, including all works and accessories required for complete installation and operation.	Pcs	90		
13.2	Indoor ceiling speaker	Supply and installation of an IP indoor ceiling speaker, including all cabling, accessories, and works necessary for complete installation and operation. Includes grille suitable for acoustic ceiling.	Pcs	260		
13.3	PA master station console	Supply and installation of an 8-zone desktop PA master station console, including goosneck microphone, and all works and accessories required for complete installation and operation.	Pcs	20		
13.4	Public address management software	Supply, installation, configuration, and commissioning of IP-based PA management software for centralized control and monitoring of IP horns and loudspeakers, including live announcements via desktop IP microphone station, playback of pre-recorded messages, zone and group management, and full integration with the central management system.	Pcs	10		
14	Intercom system					
14.1	Video intercom door unit	Supply and installation of an IP-based video intercom master station unit with a 7 or 10-inch display, including all required accessories	Pcs	52		

C2: CBK - Official

		and configuration for complete installation and operation.				
14.2	Intercom master station console	Supply and installation of a Intercom master station console with 7-inch display, including all accessories and configuration required for complete installation and operation.	Pcs	10		
14.3	Intercom IP Software	Supply and installation of IP-based intercom software for management and operation of the intercom system, including configuration, user management, integration with door and master stations, and full operational setup.	Pcs	10		
14.4	Intercom pole	Supply and installation of a 2.2 m high, 4-inch diameter steel pole. The pole shall be galvanized and painted in a color specified by the client, with steel anchors for concrete mounting and internal cable routing. Includes preparation for installing two intercom units at two heights (car height and truck height). Price includes pole foundation in the ground.	Pcs	2		
15	LPR system					
15.1	Parking management software	Parking management software, including control of parking occupancy through entry and exit counting, and interface to the barrier/bollard control panel.	Pcs	9		
15.2	Client workstation	Supply and installation of a client workstation, including hardware, operating system, and all other software required for station operation. Including installation, as well as all cables, materials, accessories, and works necessary for complete installation and proper operation. Including 27" LED monitor, keyboard and mouse	Pcs	9		

C2: CBK - Official

15.3	Control and communicatio n cabinet	Supply and installation of a control and communication cabinet made of reinforced polyester, IP65, suitable for outdoor environment. Includes concrete foundation, conduit in the concrete base, electrical panel including a panel with 6 sockets, 12-channel PoE switch, communication and control unit, software, fiber optic communication unit, optical connectors and jumpers as required, and installation and wiring only of the LPR computer (measured separately in the LPR station item). Includes power supply, battery charger, batteries, UPS system, I/O units, and all necessary wiring, cable labeling. The cabinet with lockable door, fans with filters, heating elements with thermostat. Complete installation, connection, and commissioning.	Pcs	9		
15.4	LPR camera	Supply and installation of a dedicated LPR (License Plate Recognition) camera for day and night operation, including IR illumination, outdoor vandal-resistant enclosure. The camera is standalone and includes built-in software that can be remotely programmed and manages vehicle access to the parking area.	Pcs	9		
15.5	Arm barrier	Supply and installation of a heavy-duty rapid arm barrier, with a vertical operation for vehicles, arm length up to 6 m, operating speed 0.9–2seconds. Equipped with reflectors and LED lighting. Includes concrete foundation, electrical and control panel, localoperating control pannel, pedestrian safety sensor, vehicle detection system including flashing light, warning buzzer, road loop detector, arm position indication for control, wiring, commissioning, and all equipment and accessories required for full operation.	Pcs	2		

C2: CBK - Official

15.6	Anti-tailgating system for car parking	Advanced system to prevent unauthorized vehicles from following authorized vehicles into the parking area, including sensors, cameras, access control, and integration with the parking management system connected via Interlock including all items and settings for Interlock operation	Pcs	2		
15.7	LPR control interface card	Supply, installation, and configuration of a dedicated LPR control interface card for installation in the control panel of barriers/bollards	Pcs	10		
15.8	Inductive loop detector	Supply and installation of an inductive loop detector system, including loop controller and inductive loop for barrier installation. Includes asphalt/concrete cutting, compatible cabling, and connection to the control panel/controller, as well as all works and accessories required for complete and proper operation.	Pcs	25		
15.9	LPR pole	Supply and installation of a heavy-duty galvanized steel LPR pole, painted in a color specified by the clinet, with steel anchors for concrete mounting and internal cable routing. Includes preparation for the installation of at least two cameras and foundation of the pole in the ground.	Pcs	10		
15.10	One-way trafic spike barrier	Supply and installation of a one-way metal spike barrier with lockable spikes. The spikes operate by weights, not springs, with a length of up to 6m. For outdoor installation, corrosion-protected by hot-dip galvanization, installed and anchored in an asphalt channel, ready for operation.	Pcs	3		
15.11	Integration	Integration of the LPR parking access control system, including input of client data into the system, programming according to client requirements, creation of user interfaces, and performing full system functional tests.	Complete	10		

C2: CBK - Official

16	Under Vehicle Surveillance System (UVSS)					
16.1	Under vehicle surveillance system	Supply and installation of Under Vehicle Surveillance System (UVSS), including high-resolution cameras, LED/halogen lighting panels, protective housings, vehicle presence sensors, triggering system, central controller, image processing and database software, All cabling, connectors, mounting hardware, and all accessories and works required for complete installation, integration, commissioning, and successful operation. Price of unit is for 3 meters lane.	Complete	1		
16.2	Client workstation	Supply and installation of a client workstation, including hardware, operating system, and all other software required for station operation. Including installation, as well as all cables, materials, accessories, and works necessary for complete installation and proper operation. Including 27'' LED monitor, keyboard and mouse	Pcs	1		
17	Visitors' management system					
17.1	Visitors management software	Supply and installation of a visitor management system software application, including database setup, software licenses, and all required programs, configurations, accessories, and works necessary to ensure complete installation, integration, and successful operation of the system.	Complete	1		
17.2	Client Workstation	Supply and installation of a system administrator workstation, including hardware, software, full configuration for managing and monitoring all systems, access permissions, and support for daily operation. Including 24' monitor	Pcs	1		
17.3	Licence for installation on computers	Supply and installation of software licenses for installation on 10 computers in the site. Including license keys, activation, documentation, and support in	Complete	1		

C2: CBK - Official

		accordance with manufacturer's terms and project requirements.				
17.4	Visitor management system server	Supply and installation of server for the visitor management system, including all required hardware and software components, licenses, and power supplies. Including a 24" monitor, all accessories, cabling, configurations, and works required for complete installation, integration, and successful operation of the system.	Pcs	1		
17.5	Self-service visitors kiosk	Supply and installation of self check-in Visitor Kiosk, including computer, 19" touch screen, document scanner, badge printer, and camera. The price shall include all required hardware, software, accessories, cabling, and works necessary for complete installation, configuration, and successful operation of the kiosk.	Pcs	2		
17.6	Desktop visitors registration unit	Supply and installation of desktop visitors registration unit, including computer, monitor, document scanner, badge printer, and camera. The price shall include all required hardware, software, accessories, cabling, and works necessary for complete installation, configuration, and successful operation of the kiosk.	Pcs	2		
17.7	Computer serial number scanner	Supply and install a scanner for reading and capturing computer serial numbers. Including the scanning device, necessary software or drivers, cabling or wireless connectivity, configuration, testing, and handover in full operational condition.	Pcs	2		
17.8	QR reader	Supply and installation of QR code readers, including all required accessories, cabling, configurations, and works necessary for complete installation and successful operation.	Pcs	2		

C2: CBK - Official

17.9	Email/SMS notification module	Supply and installation of a module for sending notifications via email and SMS, including full configuration and integration with all relevant systems.	Pcs	1		
17.10	Guest scheduling module	Supply of a guest scheduling module enabling the invitation and management of guests directly from the Outlook Calendar, including integration with the access control system. The module shall support installation and use on computers, including all required licenses, configuration, and integration for full operational functionality.	Complete	1		
17.11	4 doors controller	Supply and installation of a 4-door access controller, including a cabinet (or the corresponding section of a shared cabinet), power supply, socket strip, backup batteries, grounding, cables, and all required accessories, works, and configurations necessary for complete installation and successful operation of the controller.	Pcs	1		
17.12	Visitors' badges	Supply of a roll of 10,000 thermal visitor badges.	Complete	1		
18	Speed gates					
18.1	Speed gate, 55 - 65 CM pass width	Supply and installation of a speed gate with a cabinet length of 100cm, in accordance with the technical specification. Pass width 65 - 55 CN. Includes all electrical and control cabling from the gate to the nearest cabinet, as well as all required power and control cables, accessories, and works necessary for complete installation, commissioning, and operation.	Pcs	1		
18.2	Speed gate, 90 - 180 CM pass width	Supply and installation of a speed gate with a cabinet length of 100cm, in accordance with the technical specification. Pass width 90 - 180 CM. Includes all electrical and control cabling from the gate to the nearest cabinet, as well as all required power and control cables, accessories, and works necessary	Pcs	1		

C2: CBK - Official

		for complete installation, commissioning, and operation.				
18.3	Disabled persons access gate	Supply and installation of a disabled-access gate with a pass width of 100 - 120 CM, in accordance with the technical specification. Includes all electrical and control cabling from the gate to the nearest cabinet, all required power and control cables, and all accessories and works necessary for complete installation, commissioning, and operation.	Pcs	1		
18.4	Glass partition	Supply and installation of a glass partition to close the gap between the speed gates, disabled-access gate, and adjacent walls. Includes 2 stainless steel posts and glass panels of matching height.	Meter	2		
18.5	Full height turnstile	Supply and installation of full-height turnstile with electrical controller, including all civil works, infrastructure, cabling, power supply, accessories, and works necessary for complete installation, commissioning, and successful operation.	Pcs	1		
18.6	Indoor glass turnstile	Supply, delivery, and installation of a high-end indoor turnstile with tempered laminated glass arms (~12 mm), motorized bi-directional control, programmable one-way/two-way operation, and red-green user signals. Durable electro-mechanical drive suitable for continuous heavy-duty use	Pcs	2		
18.7	Control panel	Supply and installation of manual opening panel for the speed gates and disabled-access gate, including all electrical and control cabling from the gates to the reception desk workstation. Includes all required power and control cables, accessories, and works necessary for complete installation, commissioning, and operation.	Pcs	7		

C2: CBK - Official

19	Data communication network					
19.1	Backbone switch, Layer 3	Supply and installation of a Layer-3 Core switch with 24x GE SFP and 4x 10GE SFP+ ports, including power supply, DIN-rail mounting kit, all required accessories, cabling, configuration, testing, and documentation for complete installation and successful operation.	Pcs	9		
19.2	24 ports managed access switch	Supply and installation of a Layer 2 24-port Ethernet switch with 24x GE RJ45 ports, 4 x 10GE SFP+. Including power supply, all required accessories, configuration, customization, cabling, and works necessary for complete installation and operation as specified.	Pcs	98		
19.3	Industrial 16 ports managed PoE switch	Supply and installation of an industrial 16-port Ethernet switch (16 × 10M/100M/1G RJ45, 4 × 1G/10G SFP/SFP+), including power supply, DIN-rail mounting kit, all required accessories, configuration, customization, cabling, and all works necessary for complete installation and operation as specified in the technical specification.	Pcs	3		
19.4	Industrial 8 ports managed PoE switch	Supply and installation of an industrial 8-port Ethernet switch (8xGE RJ45 + 2 SFP ports), including power supply, DIN-rail mounting kit, all required accessories, configuration, customization, cabling, and all works necessary for complete installation and operation as specified in the technical specification.	Pcs	11		
19.5	Optical patch panel, 24 ports	Supply and installation of an optical patch panel, 24 ports. Including fiber patch panel, jumpers, SFP module adapters, installation wiring with labeling, and OTDR testing. Including all accessories, connections, works and cabling	Pcs	90		
19.6	Patch panel RJ45, 24 ports	Supply and installation of an patch panel RJ45, 24 ports. Including all accessories, connections, works and cabling	Pcs	88		

C2: CBK - Official

19.7	Single mode fiber optic cable, 12-strand	Supply and installation of a single mode fiber optic cable, 12-strand , including splicing. Including all required accessories, cabling, and works necessary for complete installation and operation.	Meter	7,350		
19.8	Communication point for indoor or outdoor installations	Supply and installation of a communication point for indoor and/or outdoor use, including all necessary mounting, wiring, terminations, accessories, and works required for complete and proper operation. The unit price includes full connection for end-device operation, covering supply of CAT 7 cable, threading, labeling, wall drilling, ceiling openings, and any other works required to connect the end devices for full operation, for a maximum distance of 90 meters.	Pcs	2,568		
19.9	44U Equipment rack	Supply and installation of a 44U equipment rack, including all required cabling, power connections, mounting accessories, and all works necessary for complete installation and successful operation.	Pcs	9		
19.10	22U Equipment rack	Supply and installation of a 22U equipment rack, including all required cabling, power connections, mounting accessories, and all works necessary for complete installation and successful operation. The unit shall include preparation for installation of an access control reader	Pcs	27		
19.11	15U Communication cabinet	Supply and installation of a 15U communication cabinet, including all required cabling, power connections, mounting accessories, and all works necessary for complete installation and successful operation.	Pcs	22		
19.12	6U Communication cabinet	Supply and installation of a 6U communication cabinet, including all required cabling, power connections, mounting accessories, and all works necessary for complete installation and successful operation.	Pcs	58		

C2: CBK - Official

19.13	Outdoor communicatio n cabinet	Supply and installation of a freestanding outdoor communication cabinet, including the preparation of a concrete base for the cabinet. The unit price includes a lock, service lamp, electrical panel, residual current breaker (RCCB), tester, 2 vandal-resistant 220V power outlets, and all accessories and works required for complete installation and operation.	Pcs	14		
19.14	Outdoor electricity backup system	Supply and installation of a 120 minutes power backup system for an outdoor communication cabinet, mounted on a DIN rail. Including DIN rails, power supplies, batteries, electrical connections, and all works and accessories necessary for complete installation and operation.	Pcs	14		
19.15	UPS for indoor communicatio n cabinets	Supply and installation of a single-phase 1kVA online UPS system, including batteries, surge protection rated at 600 J, and dry-contact set, capable of supporting 50% load for 120 minutes, including installation and connection. 60 minutes backup	Pcs	116		
19.16	UPS 10 KVA	Supply and installation of a 10kVA UPS in the server room, designed to provide 120 minutes of backup power to connected equipment. Including all cables, batteries, power connections, accessories, and all works required for complete installation and operation	Pcs	10		
19.17	Industrial-grade 6-channel digital I/O ethernet-based controller	Supply, installation, and configuration of an industrial-grade, Ethernet-enabled remote I/O module. The unit shall serve as a gateway for digital sensing and relay-based control over a standard TCP/IP network.I/O Configuration 6 DI / 6 Relay Outputs.	Pcs	130		
19.18	OTDR test	OTDR (Optical Time-Domain Reflectometer) Testing, including measurement of fiber optic links, fault location, insertion loss, return loss, documentation of results, and all works required for complete verification and certification of proper fiber operation, including	Complete	10		

C2: CBK - Official

		submission of test results to the clientFor each site.				
19.19	Rodent repellent system	Supply and installation of an electronic rodent repellent system in the communication room, including an ultrasonic/electromagnetic repellent unit, electrical connection, installation accessories, and everything required for proper and continuous operation of the system. The system will be installed in a manner that does not damage existing infrastructure and will provide full coverage of the room, fully functional and ready for operation.	Pcs	130		
19.20	Environmental monitoring system	Supply and install a environmental monitoring system for the server rooms.Provide real-time monitoring and historical data storage. Alerts via SMS and optional email. Optional features: relay output for buzzer/fan/AC, backup battery, door status monitoring, flood sensor. System to be installed without damage to existing infrastructure and fully operational.	Pcs	9		
20	Communication and electricity infrastructure					
20.1	Metal cable tray, 200mm x 100mm	Supply and installation of a 200mm x 100mm galvanized cable tray for outdoor use, including internal dividers, conduit covers, angle adapters, end covers, shutters, and all accessories and works required for complete installation and operation.	Meter	4,190		
20.2	120mm wide PVC duct	Supply and installation of 120mm wide PVC duct, intended for indoor installation. The price includes duct covers, angle connectors, end caps, reinforcement brackets, and all accessories and works necessary for complete installation as specified in the technical specification.	Meter	925		

C2: CBK - Official

20.3	60mm wide PVC duct	Supply and installation of 60mm wide PVC duct, intended for indoor installation. The price includes duct covers, angle connectors, end caps, reinforcement brackets, and all accessories and works necessary for complete installation as specified in the technical specification.	Meter	950		
20.4	50 mm HDPE mult-ilayer conduit	Supply and installation of 50mm HDPE multilayer conduit with an inner silicone layer providing low friction for communication cables and optical fibers,UV protected. Including all required mounting, connectors, 8 mm braided polypropylene pull cord, and all works necessary for complete and proper installation and operation.	Meter	850		
20.5	75 mm HDPE multi-layer conduit	Supply and installation of 75mm HDPE multilayer conduit with an inner silicone layer providing low friction for communication cables and optical fibers, UV-resistant. Including all required mounting, connectors, 8 mm braided polypropylene pull cord, and all works necessary for complete and proper installation and operation.	Meter	152		
20.6	50 mm polyethylene/PVC flexible conduit (Cobra)	Supply and installation of 50 mm flexible (Cobra) conduit made of polyethylene/PVC, designed for threading electrical, communication, and security camera cables for outdoor or underground use. UV-resistant. Includes all required accessories, mounting, and works necessary for complete installation and operation	Meter	700		
20.7	25 mm rigid PVC conduit	Supply and installation of a 25 mm rigid conduit (Mariron type) for indoor installation. The price includes fish tape inside the conduit, mounting brackets, connectors between conduit sections, and all works and accessories required for complete installation.	Meter	7,000		

C2: CBK - Official

20.8	25mm flexible PVC conduits	Supply and installation of 25mm flexible plastic conduits (Mericaf), flush-mounted, including pull cord (if required), junction boxes, and all necessary accessories and materials.	Meter	12,000		
20.9	Excavation of cable trenches	Excavation of cable trenches 60cm wide and 100cm deep, including bedding and sand cover, warning tapes, backfilling, final compaction, and removal of surplus soil.	Meter	480		
20.10	Saw-cutting of asphalt pavement	Saw-cutting of asphalt pavement for the installation of conduits and restoration to original condition, including structural repair, for a width of 60 cm.	Meter	180		
20.11	Removal of existing paved sidewalk	Removal of existing paved sidewalk for the installation of conduits and restoration to original condition, including reinstallation of the removed paving and structural repair, for a width of 60 cm.	Meter	270		
20.12	Chiseling of block wall	Chiseling of block wall for the installation of communication conduits up to 32 mm diameter, including complete plaster repairs.	Meter	120		
20.13	Chiseling of concrete wall or floor	Chiseling of concrete wall or floor up to 20 cm thick for the passage of communication conduits, with dimensions up to 20 × 25 cm, including complete plaster repairs.	Meter	210		
20.14	Drilling concrete or bricks wall	Drilling of passage through reinforced concrete wall or Brick wall up to 40 cm thick for a 4-inch conduit, including supply and installation of the conduit.	Complete	35		
20.15	20 mm stainless steel conduit	Supply and installation of 20 mm stainless steel conduits, wall- or ceiling-mounted, including pull cord (if required), junction boxes, and all necessary accessories and materials.	Meter	280		
20.16	Manhole, 60cm	Supply and installation of a round concrete inspection chamber, 60cm in diameter and 100cm deep, including excavation or chiseling, installation, base construction, suitable 12.5-ton cover, signage, preparation of openings, sealing, and gravel bedding at the bottom.	Pcs	31		

C2: CBK - Official

20.17	Wire mesh cable tray	Supply and installation of wire mesh cable trays for routing power and communication cabling, including all required accessories such as supports, brackets, suspension rods, connectors, bends, tees, reducers, fixing elements, grounding, and all ancillary works required for complete installation. Installation shall include cutting, forming, on-site adjustments, fastening to ceiling/wall/structure, and integration with existing infrastructure, complete and ready for operation.	Meter	85		
20.18	Underground conduit installation	Supply and installation of underground conduits (PVC, HDPE, or specified types) for cables, including connections, fittings, labeling, and backfilling to restore the site to its original condition.	Complete	685		
20.19	Electrical power cable	Supply, laying, installation, termination, testing and commissioning of electrical power cable for feeding communication cabinets and anti-ram barriers, including all necessary accessories such as cable glands, lugs, conduits/trunking, supports, excavation/backfilling (if underground), identification tags, and complete connection to the power source and equipment, as per specifications and drawings.	Meter	1,756		
21	Control room					
21.1	Operators control desk module for 1 operator	Supply and installation of control desk module for one operator. Including installation of communication and & control equipment in the desk, installation of monitors on the desk, installation of electrical outlets, IP communication access points and any other required accessories and works to deliver to the Client fully operational control desk.	Pcs	2		

C2: CBK - Official

21.2	Monitors arms	Supply and installation of monitor arms to connect 3 monitors to the control desk module, including all mounting hardware, accessories, and works required for complete installation and stable operation.	Pcs	27		
21.3	Operators chairs	Supply of operators chairs for the control room	Pcs	2		
22	Scanning devices					
22.1	Archway metal detector	Supply and installation of archway metal detector, including calibration, power cables, power supply and connection to a power source. Includes cabling, accessories, and works necessary for complete installation, configuration, and successful operation.	Pcs	1		
22.2	X-ray Bags and Parcels Inspection Machine	Supply and installation of X-ray Bags and Parcels Inspection Machine, including calibration, power cables, and connection to a power source. Includes all required infrastructure, cabling, power supply, accessories, and works necessary for complete installation, configuration, and successful operation. The price shall include obtaining approval of the unit from the local health or other relevant authorities.	Pcs	1		
23	Barriers, gates and turnstiles					
23.1	Hydro-electric bollards (K-4)	Supply and installation of hydro-electric bollards complying with K-4 standard. Including caontrol cabinet, safety loops, control box, traffic lights, and full synchronization with other installed elements such as arm barriers. Includes all civil works, infrastructure, cabling, power supply, accessories, and works necessary for complete installation, commissioning, and successful operation. The price of one unit includes three bollards to cover a vehicle lane.	Vehicle lane	1		

C2: CBK - Official

23.2	Anti – ram arm barrier, K4	Supply and installation of K4 Anti-Ram Arm Barrier, maximum width 6 meters. Including coantrol cabinet, all required civil works, infrastructure, magnetic road loop, safety accessories, cabling, power supply, accessories, and works necessary for complete installation, commissioning, and successful operation.	Pcs	1		
23.3	Cantilever sliding gate	Supply and installation of a complete cantilever (console) sliding electric vehicle gate system, including cantilever gate leaf and structural steel frame, guide rollers, support posts, counterbalance section, electric motor and gearbox, control panel, limit switches, safety devices (photocells, obstacle detection, emergency stop), manual override mechanism, access control interfaces, cabling, conduits, mounting accessories, foundations and anchor bolts, and all associated mechanical and electrical components.Including supply of electricity from nearest electric board in the facility	Pcs	1		
23.4	Operating control panel	Supply and installation of manual opening panel for the Bollards and Anti - ram gates. Including all electrical and control cabling from the gates to the reception desk workstation. Includes all required power and control cables, accessories, and works necessary for complete installation, commissioning, and operation.	Pcs	3		
24	Electronic Key Management System					
24.1	Electronic key management system, 60 Keys	Supply, installation, configuration, and commissioning of an Electronic Key Management System for secure storage, tracking, and controlled access of up to 60 keys, including all required hardware, software licenses, cabinets, receptor strips, power supply, cabling, and full operational functionality.	Pcs	5		
25	Doors, and Security Grilles					

C2: CBK - Official

25.1	5-Minute forced entry rated door	Supply and installation of a door rated to resist forced entry for 5 minutes, including frame, hardware, and all accessories required for proper operation and compliance.	Pcs	3		
25.2	5-Minute forced entry rated security grille	Supply and installation of a security grille rated to resist forced entry for 5 minutes. The diameter and spacing of the iron bars shall comply with the instructions of the approving authority. The grille shall be coated with industrial zinc-rich primer to prevent corrosion, with a topcoat in a color selected by the client. Alternatively, oven-baked painting may be applied following a process approved by the client.	Pcs	2		
26	Dismantling of equipment					
26.1	Dismantling of bollards	Dismantling and removal from site of existing bollards, including all components and associated cabling. Including proper disposal and all works required for complete removal. Price is for lane (3 - 4 bollards)	Lane	2		
26.2	Dismantling of existing security systems - big site	Dismantling and removal of existing CCTV cameras, ACS, IDS, servers, PA systems, intercoms, control consoles, and racks, including all components and associated cabling. All works shall include proper disposal and all labor required to ensure complete and safe removal from the site.	Complete	2		
26.3	Dismantling of existing security systems - small site	Dismantling and removal of existing CCTV cameras, ACS, IDS, servers, PA systems, intercoms, control consoles, and racks, including all components and associated cabling. All works shall include proper disposal and all labor required to ensure complete and safe removal from the site.	Complete	1		
26.4	Dismantling and reinstalling of acoustic ceiling tiles	Dismantling and reinstalling of acoustic ceiling tiles	Meter	2,500		

C2: CBK - Official

26.5	Technical floor	Supply and installation of Technical floor system for routing power and communication cabling beneath the floor, including floor panels, supporting structure, adjustable pedestals, grounding, and all necessary installation accessories, complete and ready for use. Load capacity up to 3,000 kg	Meter	27		
27	Cyber security					
27.1	Cyber security monitoring system	Supply, installation and configuration of cyber system for detection, warning and prevention of cyber threats on physical security and control system networks		9		
27.2	Overall coordination of cybersecurity systems integration	The bidder shall be responsible for carrying out all required coordination and integration of the cyber systems, including coordination and integration throughout the entire establishment and implementation of the systems within the project, up to final delivery. The contractor shall bear full responsibility until full integration is achieved between the security and control systems and the cyber defense systems, ensuring their complete functionality during the construction and maintenance phases	Complete	9		
27.3	Cybersecurity experts supporting design and deployment	The security contractor shall be responsible for employing experts on its behalf in the field of cyber systems, who will accompany the project on its behalf from the planning and design stages through execution (CDR/HLD), installation and integration, and up to the final delivery and testing phases. This includes performing configuration and system settings for the cyber systems, preparation of professional documentation, and execution-oriented system design throughout all stages of integration between the security and control systems and the cyber systems	Complete	9		

C2: CBK - Official

27.4	IT and network specialists for infrastructure integration	The contractor is responsible for experts in IT infrastructure, communications, and virtualized environments to support the project on its behalf from the planning and design stage through execution (CDR), installation and integration, and up to final delivery and testing. This includes configuration and setup of the entire IT environment, preparation of professional documentation, and execution-oriented system design. The experts shall also support all stages of integration between the security and control systems and the cyber systems	Complete	9		
27.5	Preparation of detailed network architecture documentation	Completion of a detailed Design-for-Execution chapter as part of the CDR, describing the implementation of the cyber systems, including a textual description of all cyber system components in both environments (security and control). This shall include professional logical and physical LLD diagrams of the IT infrastructure, prepared using Visio (or equivalent), as well as detailed communication diagrams down to the IP address level for each core network component. A detailed IP addressing table, organized by switches and ports, shall be included. The diagrams and the table shall be updated throughout the project until completion and configuration freeze	Complete	9		
27.6	Technical support during penetration testing activities	Participation in the Penetration Testing Process- The contractor and its relevant representatives shall be required to participate in the penetration testing process during which the client conducts exercises and tests on all systems. The contractor shall participate in these tests in order to provide support for all matters related to the security systems and their integration with the cyber systems. The contractor shall assign all required technical personnel for this purpose during	day	84		

C2: CBK - Official

		this period. one (1) working day of an enginer				
27.7	Additional engineering support for security testing	Additional day for supporting the contractor's team during the client's testing activities. The day shall include the relevant technical representatives required for the necessary tests	day	5		
27.8	Remediation and hardening after penetration testing	Implementation of fixes and adjustments to the configuration of the cyber systems, communication infrastructure, computers, servers, and any other component requiring correction or changes to configuration and/or additional hardening, in accordance with the recommendations of the penetration testing team identified during testing of the security and cyber security systems. one (1) working day of an enginer	day	49		
27.9	SIEM security monitoring platform	SIEM software for management, monitoring, and control of cyber events and operational continuity including all sub sysytems such as: IDS, IPS, NAC, XDR/NDR, FIREWALL, NOC, HEALTH MONITORING,EPS	Complete	9		
27.10	Network intrusion detection and threat monitoring & IOT DPI	IDS - License for monitoring one (1) IP device, including DPI	pcs	2,474		
27.11	Client Software License	Client Software license for an investigation and monitoring workstation	pcs	15		
27.12	Network Access Control for IOT & device authentication	NAC IPS - license for a switch port, including RADIUS configuration, one (1) port	pcs	8,798		
27.13	Multi user access capability for security system	MultiClient license for the monitoring system remote sites.	Complete	1		
27.14	Multi Site management for multiple bank sites License	Add on MultiSite License for multi site management of up to one (1) site add-on (scalable with no limitation)	pcs	15		

C2: CBK - Official

27.15	Protection against unauthorized USB device usage	Monitoring and protection of USB connection interfaces- for workstations and servers, per one (1) worktation / server	pcs	187		
27.16	Continuous vulnerability and CVE monitoring system	Monitoring and protection against vulnerabilities (CVE) per one (1) single asset,	pcs	2,918		
27.17	System health & IOT Health monitoring sensors	Health Monitoring - Sensors for assest health monitoring , per one (1) sensor	pcs	13,756		
27.18	Operator workstations	I9 workstation for the monitoring system, including two (2) "27 monitors including all adapters required for its operation	Complete	9		
27.19	Network traffic probe appliances for analysis	Hardware PROB appliance for network traffic collection, supporting connection to up to seven (7) edge/core switches (up to 48 ports per switch)	Complete	35		
27.20	Network traffic probe appliances for analysis	Hardware PROB appliance for network traffic collection, supporting connection to up to seven (1) edge/core switches (up to 48 ports per switch)	Complete	62		
27.21	Out of Band switches for High secure management	Managed 48 ports Layer 2 (L2) switch for the out-of-band network	Complete	9		
27.22	Management Servers	Management Server - Out-of-Band windows 2023 server, including all adapters required for its operation	Complete	9		
27.23	EPS Platform	EPS - Supply, installation, and configuration of a centrally managed EPS system tailored for a closed environment. The solution shall include a central management server (VM), all licenses required to enable the full set of required capabilities, and a central management interface. The system shall provide the ability to block and neutralize viruses, spyware, and all types of malware; capabilities for traffic and file inspection; EDR/XDR capabilities for behavioral and anomaly detection; Application Control; Device Control; and host-	Complete	9		

C2: CBK - Official

		based firewall (PFW) capabilities. The required solution shall emphasize detection of unauthorized behavior, anomalies, and heuristic analysis, with minimal dependency on frequent signature updates. The solution shall be suitable for a closed environment with a small number of users and minimal need for frequent changes. The contractor shall install all system components, including all required licenses, in accordance with the requirements of the designer and the client. The solution shall be comprehensive and include detection, protection, response, analysis, and recovery capabilities. The system shall support centralized, managed, proactive, and automatic deployment of software components. All installation and licensing shall be performed in full compliance with the technical specification requirements				
27.24	Endpoint security licenses for Worketation/Server protection	EPS Licenses for all required capabilities and endpoint security software – endpoint software for workstations and servers, including EDR capabilities and Application Control and Device Control, and all other capabilities required in accordance with the technical specification. The price shall include all licenses for all products required for implementation in full compliance with the technical specification	pcs	158		
27.25	EPS Setup & Configuration	Full configuration and tuning of all system components, and adaptation of the configuration to the applications and the environment in which the system is deployed. This includes integration with the security systems to ensure no adverse impact on the security systems protected by the solution. The scope includes configuration and tuning of all tools and engines. The contractor shall perform the	Complete	9		

C2: CBK - Official

		configuration in accordance with best practice requirements as recommended by the manufacturers of the applications installed on the server and/or workstation				
27.26	Endpoint Detection and Response system deployment	Implementation and configuration of an EDR solution- The implementation of the solution shall enable enforcement of application execution on endpoints by defining which applications are permitted to run on each workstation and/or server. This includes full configuration across all workstations and servers within the security environment. The contractor shall submit the hardening and configuration settings for the client's approval. The contractor shall also provide a procedure document describing the configuration and setup of the component.	Complete	9		
27.27	Application execution control for endpoints	Implementation and configuration of an Application Control solution- The component shall include learning capabilities of the existing state, running systems, protocols, and similar elements, after which configuration freeze shall be enabled with minimal dependency on updates and/or signatures. This includes full configuration across all workstations and servers within the security environment. The contractor shall submit the hardening and configuration settings for the client's approval. It is hereby clarified that the contractor is responsible for ensuring that there is no impact on the operation of the security systems. The contractor shall also provide a procedure document describing the configuration and setup of the component	Complete	9		

C2: CBK - Official

27.28	Host firewall configuration for system protection	Implementation of a host-based firewall solution on endpoints – Configuration and setup of the firewall on all workstations and servers as part of endpoint hardening activities. This includes restricting and hardening the range of IP addresses that each workstation and/or server is permitted to access within the security network. The contractor shall submit the hardening and configuration settings for the client's approval. This includes full configuration across all workstations and servers within the security environment. The contractor shall also provide a procedure document describing the configuration and setup of the component.	Complete	9		
27.29	Integration of security alerts into SIEM	Configuration of the system to send alerts and reports to the central SIEM cyber alert management system	Complete	9		
27.30	PKI infrastructure for encryption and certificates	The bidder shall utilize the built-in capabilities of the security and/or control systems for managing encrypted communications and for creating and managing cryptographic signatures within the security environment, in order to implement secure communications, and/or in combination with a dedicated CA server (which may be integrated with the Active Directory server). The contractor shall implement and configure digital signatures in security components that have built-in capabilities for signature management and deployment. All activities shall be performed in accordance with the technical specification, including all required hardware and software licenses and full configuration.	Complete	9		

C2: CBK - Official

27.31	Centrazlized Next Generation Firewall	FIREWALL - Supply, installation, and configuration of an NGFW system (bundle) for the security environment, including hardware, software, and licenses, for secure traffic routing between subnets. The solution shall be sized to the expected traffic volumes and provide QoS capabilities adapted to the environment. The contractor shall present a traffic calculation together with the proposed firewall component. The solution shall include at least: Eight (8) 10/100/1000 Base-T RJ45 interfaces Four (4) 10Gb SFP+ interfaces Implementation of a clustered configuration, including connection, configuration, and DAC cabling Two (2) redundant power supplies Performance requirements (minimum): 3.5 Gbps Threat Prevention throughput 6 Gbps NGFW throughput 10 Gbps IPS throughput 15 Gbps Gen2 Firewall throughput The solution shall include an NGFW license bundle for a minimum of 36 months, including all licenses required to operate all security engines of the NGFW component, all as detailed in the technical specification.	Complete	12		
27.32	Additional firewall interfaces for network connectivity	10Gb interfaces for the firewall component for connection to core switches and server switches.	pcs	24		

C2: CBK - Official

27.33	Segmatation NGFW	Supply, installation, and configuration of an NGFW system (bundle) for the OOB security environment for connection to the cyber control center, including hardware, software, and licenses. The solution shall enable secure traffic routing between subnets, be sized to the expected traffic volumes, and provide QoS capabilities adapted to the environment. The contractor shall present a traffic calculation together with the proposed firewall component.The solution shall include at least:Sixteen (16) 10/100/1000 Base-T RJ45 interfacesTwo (2) 1Gb SFP interfacesImplementation of a clustered configuration, including connection, configuration, and DAC cablingPerformance requirements (minimum):1.5 Gbps Threat Prevention throughput3 Gbps NGFW throughput3.5 Gbps IPS throughput4.5 Gbps Gen2 Firewall throughputThe solution shall include an NGFW license bundle for a minimum of 36 months, including all licenses required to operate all security engines of the NGFW component,all in accordance with the technical specification	pcs	9		
27.34	Firewall security policy design and implementation	Definition of the security policy and execution of a configuration tuning process for all NGFW components in the security environment by a qualified expert, including alignment with cybersecurity requirements and network segmentation. Policy definition, tuning, enforcement testing, and configuration shall be performed in accordance with cybersecurity protection needs and in accordance with best practices, and the guidance of the cybersecurity consultant. This includes configuration and tuning of additional security engines (Threat Prevention and IPS) as required, as well as preparation of a	Complete	9		

C2: CBK - Official

		professional document describing the configuration and setup of the components. The scope also includes filtering and forwarding of alerts to the central cyber management system in accordance with the cybersecurity consultant's requirements. Configuration tuning shall be performed throughout the project and upon its completion. All activities shall be carried out in accordance with the technical specification requirements				
27.35	Firewall management system deployment	Supply, installation, and configuration of a centralized management software for firewall components, to be deployed as a VM in the virtual environment on a separate and dedicated network, including the capability to manage up to five (5) firewall devices. The solution shall include the capability to retain logs for a minimum of one hundred (100) days, and shall include all required installation and configuration licenses. The solution may be based on products such as Check Point or equivalent, in accordance with the requirements of the technical specification	Complete	9		
27.36	Firewall infrastructure support and maintenance services	Extended warranty- Care Plus / support for all firewall components for the warranty period, including license renewal and software version updates for a minimum of 36 months	Complete	1		

C2: CBK - Official

27.37	Monitoring system for IT infrastructure health	Supply, installation, and configuration of an IT infrastructure monitoring and management system, including all licenses required to monitor and manage all elements of the security organization's IT environment, including but not limited to: all network devices (such as switches and similar equipment), endpoint devices, servers, workstations, network traffic, CPU utilization, and storage and memory usage. The system shall classify alerts into multiple severity levels (low, medium, high) and present all information through a user-friendly interface. The software shall provide monitoring capabilities, configuration management, network component management, application monitoring, and server and workstation monitoring. The system shall generate alerts for faults, alerts, and any issues within the communication infrastructure, server environment, and the overall IT environment, in order to provide a comprehensive operational view. The system shall be deployed as a VM server within the virtual environment provided by the bidder	Complete	9		
27.38	Full system configuration and setup	Full system configuration and setup, including creation of a graphical dashboard tailored to the security environment and the client's operational needs, in accordance with the client's requirements	Complete	9		
27.39	Cybersecurity software updates and license upgrades	NGFW License renewal and version upgrades, including software and hardware updates, for all cyber components (FW, data sanitization, AV, and dedicated security systems). The contractor shall be responsible, at its own expense, for renewing licenses and performing version upgrades for all cyber components as part of the service and maintenance contract, and in accordance with the defined SLA. All	Complete	9		

C2: CBK - Official

		components shall be covered by a minimum of two (2) years of full warranty				
27.40	Operational training for system administrators	Training of system users on all cyber components and systems	Complete	9		
27.41	Technical documentation for system deployment	Preparation of documentation and configuration documents for the cyber systems as part of the as-made dossier, documenting all cyber components, configurations, and user training manuals	Complete	9		
27.42	Service laptops for maintenance operations	Service laptop for use by a technician- a hardened and secured laptop with at least a 12th-generation Intel i9 processor, 17-inch display, including all software required for service delivery, securely installed within a communications cabinet	pcs	9		
27.43	Portable laptops for field technical support	Portable on-site service laptop for technician use- a hardened and secured laptop with at least a 12th-generation Intel i9 processor, 24-inch display, including all software required for service delivery	pcs	9		
27.44	ACL configurations & Implementation	Implementation of ACL configurations as required by the consultant and the client, one (1) working day	Day	9		
27.45	Content Disarm and Reconstruction	CDR (Content Disarm and Reconstruction) - Supply and installation of a CDR solution- data sanitization workstation (full solution), including hardware, software, licenses, and all components required for full operation, in accordance with the technical specification. The system shall enable scanning of all files intended for introduction into the security environment for the detection of malicious code. The solution shall be provided as a	Complete	9		

C2: CBK - Official

		standalone workstation/kiosk, including all required associated equipment				
Sub-Total - 1						
Allow for 5 % of `Sub-Total - 1 Above as Contingency						
Allow for Provisional sum of Kenya Shilling Thirty Million (30,000,000.00) to be used in whole or part after express approval by the Client against verified quotation for Factory acceptance visit and User Training						30,000,000.00
Sub Total - 2 (Inclusive of Contingency and Provisional Sum)						
Add 0.03% of Sub Total - 2 above as PPRA Capacity Building Levy						
Sub Total - 3 (Contingency + Provisional Sum + Levy						
VAT 16%						
Grand Total Carried Forward to Form of Tender						
27 Maintenance service						
27	Comprehensive Maintenance service	Comprehensive maintenance of the system for a period of three-years after One year warranty covering all supplied equipment and works. After the initial warranty period, annual maintenance service, including all labour, travel, and spare parts required for proper operation. This figure will be used to evaluate the Total Cost of Ownership of the solution and will form the basis of negotiating a Maintenance Contract	years	3		

Note: Tenderers are required to provide comprehensive list of spare parts and their unit cost covering the three years of maintenance contract.

C2: CBK - Official

PART 3 – CONDITIONS OF CONTRACT AND CONTRACT FORMS

C2: CBK - Official

SECTION VI - GENERAL CONDITIONS OF CONTRACT

A. CONTRACT AND INTERPRETATION

1. Definitions

1.1 In this Contract, the following terms shall be interpreted as indicated below.

a) Contract Elements

i) "Contract" means the Contract Agreement entered into between the Procuring Entity and the Supplier, together with the Contract Documents referred to therein. The Contract Agreement andthe Contract Documents shall constitute the Contract, and the term "the Contract" shall in all suchdocuments be construed accordingly.

ii) "Contract Documents" means the documents specified in Article1.1(Contract Documents) of theContract Agreement (including any amendments to these Documents).

iii) "Contract Agreement" means the agreement entered into between the Procuring Entity and the Supplier using the form of Contract Agreement contained in the Sample Contractual Forms Section of the tender documents and any modifications to this form agreed to by the Procuring Entity and the Supplier. The date of the Contract Agreement shall be recorded in the signed form.

iv) "GCC" means the General Conditions of Contract.

v) "SCC" means the Special Conditions of Contract.

vi) "Technical Requirements" means the Technical Requirements in Section VII of the tendering documents.

vii) "Implementation Schedule" means the Implementation Schedule in Section VII of the tendering documents.

viii) "Contract Price" means the price or prices defined in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

ix) "Procurement Regulations" refers to the Regulations issued under the Public Procurement and Asset Disposal Act (2015).

x) "Tendering documents" refers to the collection of documents issued by the Procuring Entity to instruct and inform potential suppliers of the processes for tendering, selection of the winning tender, and Contract formation, as well as the contractual conditions governing the relationship between the Procuring Entity and the Supplier. The General and Special Conditions of Contract, the Technical Requirements, and all other documents included in the tendering documents reflectthe Procurement Regulations that the Procuring Entity is obligated to follow during procurementand administration of this Contract.

b) Entities

i) "Procuring Entity" means the entity purchasing the Information System, as **specified in the SCC.**

ii) "Project Manager" means the person **named as such in the SCC** or otherwise appointed by the Procuring Entity in the manner provided in GCC Clause 18.1 (Project Manager) to perform the duties delegated by the Procuring Entity.

iii) "Supplier" means the firm or Joint Venture whose tender to perform the Contract has been accepted by the Procuring Entity and is named as such in the Contract Agreement.

iv) "Supplier's Representative" means any person nominated by the Supplier and named as such in the Contract Agreement or otherwise approved by the Procuring Entity in the manner provided inGCC Clause18.2 (Supplier's Representative) to perform the duties delegated by the Supplier.

v) "Subcontractor" means any firm to whom any of the obligations of the Supplier, including preparation of any design or supply of any Information Technologies or other Goods or Services,

C2: CBK - Official

is subcontracted directly or indirectly by the Supplier.

vi) "Adjudicator" means the person named in Appendix 2 of the Contract Agreement, appointed by agreement between the Procuring Entity and the Supplier to make a decision on or to settle any Dispute between the Procuring Entity and the Supplier referred to him or her by the parties, pursuant to GCC Clause 43.1 (Adjudication).

c) Scope

i) "Information System," also called "the System," means all the Information Technologies, Materials, and other Goods to be supplied, installed, integrated, and made operational (exclusive of the Supplier's Equipment), together with the Services to be carried out by the Supplier under the Contract.

ii) "Subsystem" means any subset of the System identified as such in the Contract that may be supplied, installed, tested, and commissioned individually before Commissioning of the entire System.

iii) "Information Technologies" means all information processing and communications-related hardware, Software, supplies, and consumable items that the Supplier is required to supply and install under the Contract.

iv) "Goods" means all equipment, machinery, furnishings, Materials, and other tangible items that the Supplier is required to supply or supply and install under the Contract, including, without limitation, the Information Technologies and Materials, but excluding the Supplier's Equipment.

v) "Services" means all technical, logistical, management, and any other Services to be provided bythe Supplier under the Contract to supply, install, customize, integrate, and make operational the System. Such Services may include, but are not restricted to, activity management and quality assurance, design, development, customization, documentation, transportation, insurance, inspection, expediting, site preparation, installation, integration, training, data migration, Pre- commissioning, Commissioning, maintenance, and technical support.

vi) "The Project Plan" means the document to be developed by the Supplier and approved by the Procuring Entity, pursuant to GCC Clause 19, based on the requirements of the Contract and the Preliminary Project Plan included in the Supplier's tender. The "Agreed Project Plan" is the version of the Project Plan approved by the Procuring Entity, in accordance with GCC Clause 19.2. Should the Project Plan conflict with the Contract in any way, the relevant provisions of theContract, including any amendments, shall prevail.

vii) "Software" means that part of the System which are instructions that cause information processingSub systems to perform in a specific manner or execute specific operations.

viii) "System Software" means Software that provides the operating and management instructions forthe underlying hardware and other components and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Systems Software. Such System Software includes, but is not restricted to, micro-code embedded in hardware (i.e., "firmware"), operating systems, communications, system and network management, and utility software.

ix) "General-Purpose Software" means Software that supports general-purpose office and software development activities and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be General-Purpose Software. Such General- Purpose Software may include, but is not restricted to, word processing, spreadsheet, generic database management, and application development software.

x) "Application Software" means Software formulated to perform specific business or technical functions and interface with the business or technical users of the System and is identified as suchin Appendix4 of the Contract Agreement and such other Software as the parties may agree in writing to be Application Software.

xi) "Standard Software" means Software identified as such in Appendix 4 of the Contract Agreementand such other Software as the parties may agree in writing to be Standard Software.

C2: CBK - Official

xii) "Custom Software" means Software identified as such in Appendix 4 of the Contract Agreementand such other Software as the parties may agree in writing to be Custom Software.

xiii) "Source Code" means the database structures, dictionaries, definitions, program source files, and any other symbolic representations necessary for the compilation, execution, and subsequent maintenance of the Software (typically, but not exclusively, required for Custom Software).

xiv) "Materials" means all documentation in printed or printable form and all instructional and informational aides in any form (including audio, video, and text) and on any medium, provided to the Procuring Entity under the Contract.

xv) "Standard Materials" means all Materials not specified as Custom Materials.

xvi) "Custom Materials" means Materials developed by the Supplier at the Procuring Entity's expenseunder the Contract and identified as such in Appendix 5 of the Contract Agreement and such otherMaterials as the parties may agree in writing to be Custom Materials. Custom Materials includesMaterials created from Standard Materials.

xvii) "Intellectual Property Rights" means any and all copyright, moral rights, trademark, patent, and other intellectual and proprietary rights, title and interests worldwide, whether vested, contingent,or future, including without limitation all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works from, extractor re-utilize data from, manufacture, introduce into circulation, publish, distribute, sell, license, sub license, transfer, rent,lease, transmit or provide access electronically, broadcast, display, enter in to computer memory,or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or toauthorize or assign others to do so.

xviii) "Supplier's Equipment" means all equipment, tools, apparatus, or things of every kind required inor for installation, completion and maintenance of the System that are to be provided by the Supplier, but excluding the Information Technologies, or other items forming part of the System.

d) Activities

i) "Delivery" means the transfer of the Goods from the Supplier to the Procuring Entity in accordance with the current edition Incoterms specified in the Contract.

ii) "Installation" means that the System or a Subsystem as specified in the Contract is ready forCommissioning as provided in GCC Clause 26 (Installation).

iii) "Pre-commissioning" means the testing, checking, and any other required activity that may be specified in the Technical Requirements that are to be carried out by the Supplier in preparation for Commissioning of the System as provided in GCC Clause 26 (Installation).

iv) "Commissioning" means operation of the System or any Subsystem by the Supplier following Installation, which operation is to be carried out by the Supplier as provided in GCC Clause27.1(Commissioning), for the purpose of carrying out Operational Acceptance Test (s).

v) "Operational Acceptance Tests" means the tests specified in the Technical Requirements and Agreed Project Plan to be carried out to ascertain whether the System, or a specified Sub system, is able to attain the functional and performance requirements specified in the Technical Requirements and Agreed Project Plan, in accordance with the provisions of GCC Clause 27.2 (Operational Acceptance Test).

vi) "Operational Acceptance" means the acceptance by the Procuring Entity of the System (or any Subsystem(s) where the Contract provides for acceptance of the System in parts), in accordance with GCC Clause27.3(Operational Acceptance).

e) Place and Time

i) "Supplier's Country" is the country in which the Supplier is legally organized, as named in theContract Agreement.

ii) **Unless otherwise specified in the SCC** "Project Site (s)" means the place (s) in the Site Table inthe Technical Requirements Section for the supply and installation of the System.

C2: CBK - Official

iii) "Eligible Country" means the countries and territories eligible for participation in procurements.

iv) "Day" means calendar day of the Gregorian Calendar.

v) "Week" means seven (7) consecutive Days, beginning the day of the week as is customary in Kenya.

vi) "Month" means calendar month of the Gregorian Calendar.

vii) "Year" means twelve (12) consecutive Months.

viii) "Effective Date" means the date of fulfillment of all conditions specified in Article 3 (Effective Date for Determining Time for Achieving Operational Acceptance) of the Contract Agreement, for the purpose of determining the Delivery, Installation, and Operational Acceptance dates for the System or Sub system(s).

ix) "Contract Period" is the time period during which this Contract governs the relations and obligations of the Procuring Entity and Supplier in relation to the System, as **unless otherwise specified in the SCC,** the Contract shall continue in force until the Information System and all the Services have been provided, unless the Contract is terminated earlier in accordance with theterms set out in the Contract**.**

x) "Defect Liability Period" (also referred to as the "Warranty Period") means the period of validityof the warranties given by the Supplier commencing at date of the Operational Acceptance Certificate of the System or Sub system(s), during which the Supplier is responsible for defects with respect to the System (or the relevant Sub-system[s]) as provided in GCC Clause 29 (DefectLiability).

xi) "The Coverage Period" means the Days of the Week and the hours of those Days during which maintenance, operational, and/ or technical support services (if any) must be available.

xii) The Post-Warranty Services Period" means the number of years **defined in the SCC** (if any), following the expiration of the Warranty Period during which the Supplier may be obligated to provide Software licenses, maintenance, and/ or technical support services for the System, underthis Contract or under separate contract(s).

2. Contract Documents

2.1 Subject to Article 1.2 (Order of Precedence) of the Contract Agreement, all documents forming part of the Contract (and all parts of these documents) are intended to be correlative, complementary, and mutually explanatory. The Contract shall be read as a whole.

3. Interpretation

3.1 Governing Language

3.1.1 All Contract Documents and related correspondence exchanged between Procuring Entity and Supplier shall be written in **the English Language** of these tendering documents**,** and the Contract shall be construed and interpreted in accordance with that language.

3.1.2 If any of the Contract Documents or related correspondence are prepared in a language other than the EnglishLanguage under GCC Clause 3.1.1 above, the translation of such documents into the **English** language shall prevail in matters of interpretation. The originating party, with respect to such documents shall bear the costsand risks of such translation.

3.2 Singular and Plural The singular shall include the plural and the plural the singular, except where thecontext otherwise requires.

3.3 Headings
The headings and marginal notes in the GCC are included for ease of reference and shall neither constitute apart of the Contract nor affect its interpretation.

3.4 Persons
Words importing persons or parties shall include firms, corporations, and government entities.

C2: CBK - Official

3.5 Incoterms

Unless inconsistent with any provision of the Contract, the meaning of any trade term and the rights and obligations of parties thereunder shall be as prescribed by the Incoterms.

Incoterms means international rules for interpreting trade terms published by the International Chamber of Commerce (latest edition), 38 Cours Albert 1er, 75008 Paris, France.

3.6 Entire Agreement

The Contract constitutes the entire agreement between the Procuring Entity and Supplier with respect to the subject matter of Contract and supersedes all communications, negotiations, and agreements (whether writtenor oral) of parties with respect to the subject matter of the Contract made prior to the date of Contract.

3.7 Amendment

No amendment or other variation of the Contract shall be effective unless it is in writing, is dated, expressly refers to the Contract, and is signed by a duly authorized representative of each party to the Contract.

3.8 Independent Supplier

The Supplier shall be an independent contractor performing the Contract. The Contract does not create any agency, partnership, joint venture, or other joint relationship between the parties to the Contract.

Subject to the provisions of the Contract, the Supplier shall be solely responsible for the manner in which theContract is performed. All employees, representatives, or Sub contractors engaged by the Supplier inconnection with the performance of the Contract shall be under the complete control of the Supplier and shallnot be deemed to be employees of the Procuring Entity, and nothing contained in the Contractor in any subcontract awarded by the Supplier shall be construed to create any contractual relationship between any such employees, representatives, or Sub contractors and the Procuring Entity.

3.9 Joint Venture

If the Supplier is a Joint Venture of two or more firms, all such firms shall be jointly and severally bound to the Procuring Entity for the fulfillment of the provisions of the Contract and shall designate one of such firmsto act as a leader with authority to bind the Joint Venture. The composition or constitution of the Joint Ventureshall not be altered without the prior consent of the Procuring Entity.

3.10 Non-waiver

3.10.1 Subject to GCC Clause 3.10.2 below, no relaxation, forbearance, delay, or indulgence by either party in enforcing any of the terms and conditions of the Contractor the granting of time by either party to the other shall prejudice, affect, or restrict the rights of that party under the Contract, nor shall any waiver by either party of any breach of Contract operate as waiver of any subsequent or continuing breach of Contract.

3.10.2 Any waiver of a party's rights, powers, or remedies under the Contract must be in writing, must be dated and signed by an authorized representative of the party granting such waiver, and must specify the right and the extent to which it is being waived.

3.11 Severability

If any provision or condition of the Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity, or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of the Contract.

3.12 Country of Origin

"Origin" means the place where the Information Technologies, Materials, and other Goods for the System were produced or from which the Services are supplied. Goods are produced when, through manufacturing, processing, Software development, or substantial and major assembly or integration of components, a commercially recognized product results that is substantially different in basic

C2: CBK - Official

characteristics or in purpose orutility from its components. The Origin of Goods and Services is distinct from the nationality of the Supplierand may be different.

4. Notices

4.1 Unless otherwise stated in the Contract, all notices to be given under the Contract shall be in writing and shallbe sent, pursuant to GCC Clause 4.3 below, by personal delivery, air mail post, special courier, facsimile, electronic mail, or Electronic Data Interchange (EDI), with the following provisions.

4.1.1 Any notice sent by facsimile, electronic mail, or EDI shall be confirmed within two (2) days after dispatch bynotice sent by air mail post or special courier, except as otherwise specified in the Contract.

4.1.2 Any notice sent by air mail post or special courier shall be deemed (in the absence of evidence of earlier receipt) to have been delivered ten (10) days after dispatch. In proving the fact of dispatch, it shall be sufficient to show that the envelope containing such notice was properly addressed, stamped, and conveyed to the postalauthorities or courier service for transmission by air mail or special courier.

4.1.3 Any notice delivered personally or sent by facsimile, electronic mail, or EDI shall be deemed to have beendelivered on the date of its dispatch.

4.1.4 Either party may change its postal, facsimile, electronic mail, or EDI addresses for receipt of such notices by ten
(10) days' notice to the other party in writing.

4.2 Notices shall be deemed to include any approvals, consents, instructions, orders, certificates, information andother communication to be given under the Contract.

4.3 Pursuant to GCC Clause 18, notices from/to the Procuring Entity are normally given by, or addressed to, the Project Manager, while notices from/to the Supplier are normally given by, or addressed to, the Supplier's Representative, or in its absence its deputy if any. If there is no appointed Project Manager or Supplier's Representative (or deputy), or if their related authority is limited by the SCC for GCC Clauses 18.1 or 18.2.2,or for any other reason, the Procuring Entity or Supplier may give and receive notices at their fall-back addresses. The address of the Project Manager and the fall-back address of the Procuring Entity are as **specifiedin the SCC** or as subsequently established/ amended. The address of the Supplier's Representative and the fallback address of the Supplier are as specified in Appendix 1 of the Contract Agreement or as subsequently established/amended.

5. Governing Law

5.1 The Contract shall be governed by and interpreted in accordance with the laws of Kenya.

5.2 Throughout the execution of the Contract, the Supplier shall comply with the import of goods and servicesprohibitions in Kenya when

a As a matter of law or official regulations, Kenya prohibits commercial relations with that country; or

b by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of theCharter of the United Nations, Kenya prohibits any import of goods from that country or any payments to any country, person, or entity in that country.

6 Fraud and Corruption

6.1 The Procuring Entity requires compliance with the laws of Kenya on Anti-Corruption Guidelines and itsprevailing sanctions policies and procedures as set forth in its statutes.

6.2 The Procuring Entity requires the Suppliers to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the tendering process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee.

C2: CBK - Official

B. SUBJECT MATTER OF CONTRACT

7 Scope of the System

7.1 Unless otherwise expressly **limited in the SCC** or Technical Requirements, the Supplier's obligations cover the provision of all Information Technologies, Materials and other Goods as well as the performance of all Services required for the design, development, and implementation (including procurement, quality assurance,assembly, associated site preparation, Delivery, Pre-commissioning, Installation, Testing, and Commissioning) of the System, in accordance with the plans, procedures, specifications, drawings, codes, and any other documents specified in the Contract and the Agreed Project Plan.

7.2 The Supplier shall, unless specifically excluded in the Contract, perform all such work and/or supply all such items and Materials not specifically mentioned in the Contract but that can be reasonably inferred from the Contract as being required for attaining Operational Acceptance of the System as if such work and/or items and Materials were expressly mentioned in the Contract.

7.3 The Supplier's obligations (if any) to provide Goods and Services as implied by the Recurrent Cost tables of the Supplier's tender, such as consumables, spare parts, and technical services (e.g., maintenance, technical assistance, and operational support), are as **specified in the SCC,** including the relevant terms, characteristics,and timings.

8 Time for Commencement and Operational Acceptance

8.1 The Supplier shall commence work on the System within the period **specified in the SCC,** and without prejudice to GCC Clause 28.2, the Supplier shall there after proceeding with the System in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan.

8.2 The Supplier shall achieve Operational Acceptance of the System (or Subsystem(s) where a separate time forOperational Acceptance of such Sub system (s) is specified in the Contract) in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan, or within such extended time to which the Supplier shall be entitled under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

9 Supplier's Responsibilities

9.1 The Supplier shall conduct all activities with due care and diligence, in accordance with the Contract and withthe skill and care expected of a competent provider of information technologies, information systems, support,maintenance, training, and other related services, or in accordance with best industry practices. In particular, the Supplier shall provide and employ only technical personnel who are skilled and experienced in the irrespective callings and supervisory staff who are competent to adequately supervise the work at hand.

9.2 The Supplier confirms that it has entered into this Contract on the basis of a proper examination of the data relating to the System provided by the Procuring Entity and on the basis of information that the Supplier couldhave obtained from a visual inspection of the site (if access to the site was available) and of other data readilyavailable to the Supplier relating to the System as at the date twenty-eight (28) days prior to tender submission.The Supplier acknowledges that any failure to acquaint itself with all such data and information shall not relieve its responsibility for properly estimating the difficulty or cost of successfully performing the Contract.

9.3 The Supplier shall be responsible for timely provision of all resources, information, and decision making underits control that are necessary to reach a mutually Agreed Project Plan (pursuant to GCC Clause 19.2) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision-making may constitute grounds for termination pursuant to GCC Clause 41.2.

9.4 The Supplier shall acquire in its name all permits, approvals, and/or licenses from all local, state, or national government authorities or public service undertakings in Kenya that are necessary for the

C2: CBK - Official

performance of theContract, including, without limitation, visas for the Supplier's and Subcontractor's personnel and entry permitsfor all imported Supplier's Equipment. The Supplier shall acquire all other permits, approvals, and/or licensesthat are not the responsibility of the Procuring Entity under GCC Clause 10.4 and that are necessary for the performance of the Contract.

9.5 The Supplier shall comply with all laws in force in Kenya. The laws will include all national, provincial, municipal, or other laws that affect the performance of the Contract and are binding upon the Supplier. The Supplier shall indemnify and hold harmless the Procuring Entity from and against any and all liabilities, damages, claims, fines, penalties, and expenses of whatever nature a rising or resulting from the violation of such laws by the Supplier or its personnel, including the Sub contractors and their personnel, but without prejudice to GCC Clause 10.1. The Supplier shall not indemnify the Procuring Entity to the extent that such liability, damage, claims, fines, penalties, and expenses were caused or contributed to by a fault of the Procuring Entity.

9.6 The Supplier shall, in all dealings with its labor and the labor of its Subcontractors currently employed on or connected with the Contract, pay due regard to all recognized festivals, official holidays, religious or other customs, and all local laws and regulations pertaining to the employment of labor.

9.7 Any Information Technologies or other Goods and Services that will be incorporated in or be required for theSystem and other supplies shall have their Origin, as defined in GCC Clause 3.12, in a country that shall be anEligible Country, as defined in GCC Clause 1.1 (e) (iv).

9.8 Pursuant to paragraph 2.2e. of Appendix B to the General Conditions the Supplier shall permit and shall causeits subcontractors and sub-consultants to permit, the PPRA and/or persons appointed by the PPRA to inspect the Site and/or the accounts and records relating to the procurement process, selection and/or contract execution, and to have such accounts and records audited by auditors appointed by the PPRA if requested by the PPRA. The Supplier's and its Sub contractors' and sub-consultants' attention is drawn to Sub-Clause 6.1 which provides, inter alia, that acts intended to materially impede the exercise of the PPRA's inspection and audit rights constitute a prohibited practice subject to contract termination (as well as to a determination of ineligibility pursuant to the PPRA's prevailing sanctions procedures).

9.9 The Supplier shall conform to the sustainable procurement contractual provisions, if and as **specified in the SCC.**

9.10 **Unless otherwise specified in the SCC** the Supplier shall have no other Supplier responsibilities.

10 Procuring Entity's Responsibilities

10.1 The Procuring Entity shall ensure the accuracy of all information and/or data to be supplied by the Procuring Entity to the Supplier, except when otherwise expressly stated in the Contract.

10.2 The Procuring Entity shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach an Agreed Project Plan (pursuant to GCC Clause 19.2) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision making may constitute grounds for Termination pursuant to GCC Clause 41.3.1(b).

10.3 The Procuring Entity shall be responsible for acquiring and providing legal and physical possession of the siteand access to it, and for providing possession of and access to all other are as reasonably required for the proper execution of the Contract.

10.4 If requested by the Supplier, the Procuring Entity shall use its best endeavors to assist the Supplier in obtainingin a timely and expeditious manner all permits, approvals, and/or licenses necessary for the execution of the Contract from all local, state, or national government authorities or public service undertakings that such authorities or under takings require the Supplier or Sub contractors or the personnel of the Supplier or Sub contractors, as the case may be, to obtain.

10.5 In such cases where the responsibilities of specifying and acquiring or upgrading telecommunications and/or electric power services falls to the Supplier, as specified in the Technical Requirements, SCC,

C2: CBK - Official

Agreed ProjectPlan, or other parts of the Contract, the Procuring Entity shall use its best endeavors to assist the Supplier in obtaining such services in a timely and expeditious manner.

10.6 The Procuring Entity shall be responsible for timely provision of all resources, access, and information necessary for the Installation and Operational Acceptance of the System (including, but not limited to, any required telecommunications or electric power services), as identified in the Agreed Project Plan, except whereprovision of such items is explicitly identified in the Contract as being the responsibility of the Supplier. Delay by the Procuring Entity may result in an appropriate extension of the Time for Operational Acceptance, at theSupplier's discretion.

10.7 Unless otherwise specified in the Contractor agreed upon by the Procuring Entity and the Supplier, the Procuring Entity shall provide sufficient, properly qualified operating and technical personnel, as required by the Supplier to properly carry out Delivery, Pre-commissioning, Installation, Commissioning, and OperationalAcceptance, at or before the time specified in the Implementation Schedule and the Agreed Project Plan.

10.8 The Procuring Entity will designate appropriate staff for the training courses to be given by the Supplier and shall make all appropriate logistical arrangements for such training as specified in the Technical Requirements,SCC, the Agreed Project Plan, or other parts of the Contract.

10.9 The Procuring Entity assumes primary responsibility for the Operational Acceptance Test (s) for the System, in accordance with GCC Clause 27.2, and shall be responsible for the continued operation of the System afterOperational Acceptance. However, this shall not limit in anyway the Supplier's responsibilities after the date of Operational Acceptance otherwise specified in the Contract.

10.10 The Procuring Entity is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles, except where such responsibility is clearly assigned to the Supplier elsewhere in the Contract.

10.11 All costs and expenses involved in the performance of the obligations under this GCC Clause 10 shall be the responsibility of the Procuring Entity, save those to be incurred by the Supplier with respect to the performanceof the Operational Acceptance Test (s), in accordance with GCC Clause 27.2.

10.12 **Unless otherwise specified in the SCC** the Procuring Entity shall have no other Procuring Entity responsibilities

C. Payment

11 Contract Price

11.1 The Contract Price shall be as specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

11.2 Unless an adjustment clause is **provided for in the SCC,** the Contract Price shall be a firm lump sum not subject to any alteration, except in the event of a Change in the System pursuant to GCC Clause 39 or to otherclauses in the Contract.

11.3 The Supplier shall be deemed to have satisfied itself as to the correctness and sufficiency of the Contract Price,which shall, except as otherwise provided for in the Contract, cover all its obligations under the Contract.

11.4 Where the contract price is different from the corrected tender price, in order to ensure the contractor is not paid less or more relative to the contract price (*which would be the tender price*), payment valuation certificatesand variation orders on omissions and additions valued based on rates in the Bill of Quantities or schedule of rates in the Tender, will be adjusted by a plus or minus percentage. The percentage already worked out duringtender evaluation is worked out as follows: *(corrected tender price–tender price)/ tender price X 100*.

C2: CBK - Official

12 Terms of Payment

12.1 The Supplier's request for payment shall be made to the Procuring Entity in writing, accompanied by an invoicedescribing, as appropriate, the System or Subsystem(s), Delivered, Pre-commissioned, Installed, and Operationally Accepted, and by documents submitted pursuant to GCC Clause 22.5 and upon fulfillment of other obligations stipulated in the Contract. The Contract Price shall be paid as **specified in the SCC.**

12.2 No payment made by the Procuring Entity herein shall be deemed to constitute acceptance by the Procuring Entity of the System or any Sub system (s).

12.3 Payments shall be made promptly by the Procuring Entity, but in no case later than (sixty (60) days after submission of a valid invoice and upon satisfactorily performance of the contractual obligations by the Supplier. In the event that the Procuring Entity fails to make any payment by its respective due date or withinthe period set forth in the Contract, the Procuring Entity shall pay to the Supplier interest on the amount of such delayed payment at the rate (s) **specified in the SCC** for the period of delay until payment has been madein full, whether before or after judgment or arbitration award.

12.4 Payments shall be made in the currency (ies) specified in the Contract Agreement, pursuant to GCC Clause 11.For Goods and Services supplied locally, payments shall be made **as specified in the SCC.**

12.5 **Unless otherwise specified in the SCC,** payment of the foreign currency portion of the Contract Price for Goods supplied from outside Kenya shall be made to the Supplier through an irrevocable Form of credit opened by an authorized bank in the Supplier's Country and will be payable on presentation of the appropriatedocuments. It is agreed that the Form of credit will be subject to Article10 of the latest revision of *Uniform Customs and Practice for Documentary Credits*, published by the International Chamber of Commerce, Paris.

13 Securities

13.1 Issuance of Securities

The Supplier shall provide the securities specified below in favor of the Procuring Entity at the times and in theamount, manner, and form specified below.

13.2 Advance Payment Security

a) Unless otherwise specified in the SCC, the Supplier shall provide within twenty-eight (28) days of the notification of Contract award an Advance Payment Security in the amount and currency of the Advance Payment specified in SCC for GCC Clause 12.1 above and valid until the System is Operationally Accepted.

b) The security shall be in the form provided in the tendering documents or in another form acceptable to the Procuring Entity. The amount of the security shall be reduced in proportion to the value of the System executedby and paid to the Supplier from time to time and shall automatically become null and void when the full amount of the advance payment has been recovered by the Procuring Entity. **Unless otherwise specified in the SCC,** the reduction in value and expiration of the Advance Payment Security are calculated as follows:

P*a/(100-a), where “P” is the sum of all payments effected so far to the Supplier (excluding the Advance Payment), and “a” is the Advance Payment expressed as a percentage of the Contract Price pursuant to the SCC for GCC Clause12.1.

The security shall be returned to the Supplier immediately after its expiration.

C2: CBK - Official

13.3 Performance Security

13.3.1 The Supplier shall, within twenty-eight (28) days of the notification of Contract award, provide a security for the due performance of the Contract in the amount and currency **specified in the SCC**.

13.3.2 The security shall be a bank guarantee in the form provided in the Sample Contractual Forms Section of thetendering documents, or it shall be in another form acceptable to the Procuring Entity.

13.3.3 The security shall automatically become null and void once all the obligations of the Supplier under the Contract have been fulfilled, including, but not limited to, any obligations during the Warranty Period and any extensions to the period. The security shall be returned to the Supplier no later than twenty-eight (28) days after its expiration.

13.3.4 Upon Operational Acceptance of the entire System, the security shall be reduced to the amount specified in the SCC, on the date of the Operational Acceptance, so that the reduced security would only cover the remaining warranty obligations of the Supplier.

14 Taxes and Duties

14.1 For Goods or Services supplied from outside and inside Kenya, the Supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside Kenya and inside Kenya, and theseduties or taxes shall be made part of the Contract Price in Article 2 of the Contract Agreement and the Price Schedule it refers to, in which case the duties and taxes will be the Supplier's responsibility.

14.2 For Goods or Services supplied locally, the Supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods or Services to the Procuring Entity. The only exception are taxes or duties, such as value-added or sales tax or stamp duty as apply to, or are clearly identifiable, on the invoices and provided they apply in Kenya, and only if these taxes, levies and/or duties arealso excluded from the Contract Price in Article 2 of the Contract Agreement and the Price Schedule it refersto.

14.3 If any tax exemptions, reductions, allowances, or privileges may be available to the Supplier in Kenya, the Procuring Entity shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent.

14.4 For the purpose of the Contract, it is agreed that the Contract Price specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement is based on the taxes, duties, levies, and charges prevailing at the date twenty-eight (28) days prior to the date of tender submission in Kenya (also called "Tax" in this GCCClause 14.4). If any Tax rates are increased or decreased, a new Tax is introduced, an existing Tax is abolished,or any change in interpretation or application of any Tax occurs in the course of the performance of the Contract, which was or will be assessed on the Supplier, its Sub contractors, or their employees in connectionwith performance of the Contract, an equitable adjustment to the Contract Price shall be made to fully take into account any such change by addition to or reduction from the Contract Price, as the case may be.

D. Intellectual Property

15 Copyright

15.1 The Intellectual Property Rights in all Standard Software and Standard Materials shall remain vested in the owner of such rights.

15.2 The Procuring Entity agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause16, except that additional copies of Standard Materials may be madeby the Procuring Entity for use within the scope of the project of which the System is apart, in the event that the Supplier does not deliver copies within thirty (30) days from

C2: CBK - Official

receipt of a request for such Standard Materials.

15.3 The Procuring Entity's contractual rights to use the Standard Software or elements of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with the relevant license agreement or **unless otherwise specified in the SCC** to a legally constituted successor organization (e.g., a reorganization of a public entity formally authorized by the government or through a merger or acquisition of a private entity)**.**

15.4 **Unless otherwise specified in the SCC,** the Intellectual Property Rights in all Custom Software and Custom Materials specified in Appendices 4 and 5 of the Contract Agreement (if any) shall, at the date of this Contract or on creation of the rights (if later than the date of this Contract), vest in the Procuring Entity. The Supplier shall do and execute or arrange for the doing and executing of each necessary act, document, and thing that the Procuring Entity may consider necessary or desirable to perfect the right, title, and interest of the Procuring Entity in and to those rights. In respect of such Custom Software and Custom Materials, the Supplier shall ensure that the holder of am or alright in such an item does not assert it, and the Supplier shall,if requested to do so by the Procuring Entity and where permitted by applicable law, ensure that the holder ofsuch a moral right waives it.

15.5 **Unless otherwise specified in the SCC**, escrow arrangements shall NOT be required.

16 Software License Agreements

16.1 Except to the extent that the Intellectual Property Rights in the Software vest in the Procuring Entity, the Supplier here by, subject to the terms, conditions and limitations issued by the manufacturer of the software, grants to the Procuring Entity license to access and use the Software, including all inventions,designs, and marks embodied in the Software.

i. Such license to access and use the Software shall:

a) Permit the Software to be:

i. used or copied for use on or with the computer (s) for which it was acquired (if specified in the Technical Requirements and/or the Supplier's tender), plus a backup computer (s) of the same or similar capacity, if the primary is (are) in operative, and during a reasonable transitional period when use is being transferred betweenprimary and back up.

ii. used or copied for use on or transferred to are placement computer (s), (and use on the original and replacementcomputer(s) may be simultaneous during a reasonable transitional period) provided that, if the Technical Requirements and/or the Supplier's tender specifies a class of computer to which the license is restricted, the replacement computer (s) is (are) within that class.

iii. if the nature of the System is such as to permit such access, accessed from other computers connected to the primary and/or back up computer (s) by means of a local or wide-area network or similar arrangement, and used on or copied for use on those other computers to the extent necessary to that access.

iv. reproduced for safe keeping or back up purposes.

v. customized, adapted, or combined with other computer software for use by the Procuring Entity, provided thatderivative software incorporating any substantial part of the delivered, restricted Software shall be subject to same restrictions as a reset forth in this Contract.

vi. **unless otherwise specified in the SCC,** disclosed to, and reproduced for use by, support service suppliers and their sub-contractors, (and the Procuring Entity may sub-license such persons to use and copy for use the Software) to the extent reasonably necessary to the performance of their support service contracts, subject to the same restrictions as a reset forth in this Contract; and

vii. **unless otherwise specified in the SCC** disclosed to, and reproduced for use by, NO other parties.

16.2 The Supplier has the right to audit the Standard Software to verify compliance with the above license agreements.
Unless otherwise specified in the SCC, the Procuring Entity will make available to the Supplier, within seven(7) days of a written request, accurate and up-to-date records of the number and location of copies,

C2: CBK - Official

the number of authorized users, or any other relevant data required to demonstrate use of the Standard Software as per the license agreement. If and only if, expressly agreed in writing between the Procuring Entity and the Supplier, Procuring Entity will allow, under a pre-specified agreed procedure, the execution of embedded software functions under Supplier's control, and unencumbered transmission of resulting information on software usage.

17 Confidential Information

17.1 **Unless otherwise specified in the SCC,** the" Receiving Party" (either the Procuring Entity or the Supplier) shall keep confidential and shall not, without the written consent of the other party to this Contract ("the Disclosing Party"), divulge to any third party any documents, data, or other information of a confidential nature("Confidential Information") connected with this Contract, and furnished directly or indirectly by the Disclosing Party prior to or during performance, or following termination, of this Contract.

17.2 For the purposes of GCC Clause 17.1, the Supplier is also deemed to be the Receiving Party of Confidential Information generated by the Supplier itself in the course of the performance of its obligations under the Contract and relating to the businesses, finances, suppliers, employees, or other contacts of the Procuring Entity or the Procuring Entity's use of the System.

17.3 Notwithstanding GCC Clauses 17.1 and 17.2:

a) the Supplier may furnish to its Subcontractor Confidential Information of the Procuring Entity to the extent reasonably required for the Subcontractor to perform its work under the Contract; and

b) the Procuring Entity may furnish Confidential Information of the Supplier: (i) to its support service suppliers and their subcontractors to the extent reasonably required for them to perform their work under their support service contracts; and (ii) to its affiliates and subsidiaries, in which event the Receiving Party shall ensure that the person to whom it furnishes Confidential Information of the Disclosing Party is aware of and a tenderer by the Receiving Party's obligations under this GCC Clause 17 as if that person were party to the Contract in place of the Receiving Party.

17.4 The Procuring Entity shall not, without the Supplier's prior written consent, use any Confidential Information received from the Supplier for any purpose other than the operation, maintenance and further development of the System. Similarly, the Supplier shall not, without the Procuring Entity's prior written consent, use any Confidential Information received from the Procuring Entity for any purpose other than those that are required for the performance of the Contract.

17.5 The obligation of a party under GCC Clauses 17.1 through 17.4 above, however, shall not apply to that information which:

a) Now or hereafter enters the public domain through no fault of the Receiving Party.

b) can be proven to have been possessed by the Receiving Party at the time of disclosure and that was not previously obtained, directly or indirectly, from the Disclosing Party.

c) otherwise lawfully becomes available to the Receiving Party from a third party that has no obligation of confidentiality.

17.6 The above provisions of this GCC Clause 17 shall not in any way modify any undertaking of confidentiality given by either of the parties to this Contract prior to the date of the Contract in respect of the System or any part thereof.

17.7 **Unless otherwise specified in the SCC**, the provisions of this GCC Clause 17 shall survive the termination, for whatever reason, of the Contract for three (3) years.

C2: CBK - Official

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System

18 Representatives

18.1 Project Manager

If the Project Manager is not named in the Contract, then within fourteen (14) days of the Effective Date, theProcuring Entity shall appoint and notify the Supplier in writing of the name of the Project Manager. The Procuring Entity may from time to time appoint some other person as the Project Manager in place of the person previously so appointed and shall give a notice of the name of such other person to the Supplier without delay. No such appointment shall be made at such a time or in such a manner as to impede the progress of work on the System. Such appointment shall take effect only upon receipt of such notice by the Supplier. **Unless otherwise specified in the SCC** (if any), the Project Manager shall have the authority to represent the Procuring Entity on all day-to-day matters relating to the System or arising from the Contract and shall normally be the person giving or receiving notices on behalf of the Procuring Entity pursuant to GCC Clause4.

18.2 Supplier's Representative

18.2.1 If the Supplier's Representative is not named in the Contract, then with in fourteen (14) days of the EffectiveDate, the Supplier shall appoint the Supplier's Representative and shall request the Procuring Entity in writing to approve the person so appointed. The request must be accompanied by a detailed curriculum vitae for the nominee, as well as a description of any other System or non-System responsibilities the nominee would retain while performing the duties of the Supplier's Representative. If the Procuring Entity does not object tothe appointment within fourteen (14) days, the Supplier's Representative shall be deemed to have been approved. If the Procuring Entity objects to the appointment within fourteen (14) days giving the reason therefor, then the Supplier shall appoint a replacement within fourteen (14) days of such objection in accordance with this GCC Clause 18.2.1.

18.2.2 **Unless otherwise specified in the SCC** (if any), the Supplier's Representative shall have the authority to represent the Supplier on all day-to-day matters relating to the System or arising from the Contract and shallnormally be the person giving or receiving notices on behalf of the Supplier pursuant to GCC Clause 4.

18.2.3 The Supplier shall not revoke the appointment of the Supplier's Representative without the Procuring Entity'sprior written consent, which shall not be unreasonably withheld. If the Procuring Entity consents to such anaction, the Supplier shall appoint another person of equal or superior qualifications as the Supplier's Representative, pursuant to the procedure set out in GCC Clause 18.2.1.

18.2.4 The Supplier's Representative and staff are obliged to work closely with the Procuring Entity's Project Manager and staff, act within their own authority, and a tenderer by directives issued by the Procuring Entitythat are consistent with the terms of the Contract. The Supplier's Representative is responsible for managingthe activities of its personnel and any subcontracted personnel.

18.2.5 The Supplier's Representative may, subject to the approval of the Procuring Entity (which shall not be unreasonably withheld), at any time delegate to any person any of the powers, functions, and authorities vested in him or her. Any such delegation may be revoked at any time. Any such delegation or revocation shall be subject to a prior notice signed by the Supplier's Representative and shall specify the powers, functions, and authorities there by delegated or revoked. No such delegation or revocation shall take effect unless and until the notice of it has been delivered.

18.2.6 Any act or exercise by any person of powers, functions and authorities so delegated to him or her in accordance with GCC Clause18.2.5shall be deemed to be an act or exercise by the Supplier's Representative.

C2: CBK - Official

18.3 Objections and Removals

18.3.1 The Procuring Entity may by notice to the Supplier object to any representative or person employed by the Supplier in the execution of the Contract who, in the reasonable opinion of the Procuring Entity, may have behaved inappropriately, be incompetent, or be negligent. The Procuring Entity shall provide evidence of thesame, where upon the Supplier shall remove such person from work on the System.

18.3.2 If any representative or person employed by the Supplier is removed in accordance with GCC Clause18.3.1,the Supplier shall, where required, promptly appoint a replacement.

19 Project Plan

19.1 In close cooperation with the Procuring Entity and based on the Preliminary Project Plan included in the Supplier's tender, the Supplier shall develop a Project Plan encompassing the activities specified in the Contract. The contents of the Project Plan shall be as **specified in the SCC** and/ or Technical Requirements. **Unless otherwise specified in the SCC**, within thirty (30) days from the Effective Date of the Contract, the Supplier shall present a Project Plan to the Procuring Entity. The Procuring Entity shall, within fourteen (14) days of receipt of the Project Plan, notify the Supplier of any respects in which it considers that the Project Plan does not adequately ensure that the proposed program of work, proposed methods, and/or proposed Information Technologies will satisfy the Technical Requirements and/or the SCC (in this Clause 19.2 called"non-conformities" below). The Supplier shall, within five (5) days of receipt of such notification, correct theProject Plan and resubmit to the Procuring Entity. The Procuring Entity shall, within five (5) days of resubmission of the Project Plan, notify the Supplier of any remaining non-conformities. This procedure shallbe repeated as necessary until the Project Plan is free from non-conformities. When the Project Plan is free from non-conformities, the Procuring Entity shall provide confirmation in writing to the Supplier. This approved Project Plan ("the Agreed Project Plan") shall be contractually binding on the Procuring Entity andthe Supplier.

19.2 If required, the impact on the Implementation Schedule of modifications agreed during finalization of the Agreed Project Plan shall be incorporated in the Contract by amendment, in accordance with GCC Clauses 39and 40.

19.3 The Supplier shall undertake to supply, install, test, and commission the System in accordance with the AgreedProject Plan and the Contract.

19.4 **Unless otherwise specified in the SCC**, the Supplier shall submit to the Procuring Entity Monthly ProgressReports summarizing:

i) Results accomplished during the prior period.

ii) cumulative deviations to date from schedule of progress milestones as specified in the Agreed Project Plan.

iii) corrective actions to be taken to return to planned schedule of progress; proposed revisions to planned schedule.

iv) other issues and outstanding problems; proposed actions to be taken.

v) resources that the Supplier expects to be provided by the Procuring Entity and/ or actions to be takenby the Procuring Entity in the next reporting period.

vi) other issues or potential problems the Supplier foresees that could impact on project progress and/or effectiveness.

19.5 The Supplier shall submit to the Procuring Entity other (periodic) reports **as specified in the SCC**.

20 Sub-contracting

20.1 Appendix 3 (List of Approved Subcontractors) to the Contract Agreement specifies critical items of supply or services and a list of Subcontractors for each item that are considered acceptable by the

C2: CBK - Official

Procuring Entity. If no Subcontractors are listed for an item, the Supplier shall prepare a list of Subcontractors it considers qualified and wishes to be added to the list for such items. The Supplier may from time to time propose additions to or deletions from any such list. The Supplier shall submit any such list or any modification to the list to the Procuring Entity for its approval insufficient time so as not to impede the progress of work onthe System. The Procuring Entity shall not withhold such approval unreasonably. Such approval by the Procuring Entity of a Subcontractor (s) shall not relieve the Supplier from any of its obligations, duties, or responsibilities under the Contract.

20.2 The Supplier may, at its discretion, select and employ Subcontractors for such critical items from those Subcontractors listed pursuant to GCC Clause 20.1. If the Supplier wishes to employ a Subcontractor not solisted, or subcontract an item not so listed, it must seek the Procuring Entity's prior approval under GCC Clause 20.3.

20.3 For items for which pre-approved Subcontractor lists have not been specified in Appendix 3 to the ContractAgreement, the Supplier may employ such Subcontractors as it may select, provided:

(i) the Supplier notifies theProcuring Entity in writing at least twenty-eight (28) days prior to the proposed mobilization date for such Subcontractor; and

(ii) by the end of this period either the Procuring Entity has granted its approval in writing or fails to respond. The Supplier shall not engage any Subcontract to which the Procuring Entity has objected in writing prior to the end of the notice period. The absence of a written objection by the ProcuringEntity during the above specified period shall constitute formal acceptance of the proposed Subcontractor. Except to the extent that it permits the deemed approval of the Procuring Entity of Subcontractors not listedin the Contract Agreement, nothing in this Clause, however, shall limit the rights and obligations of either the Procuring Entity or Supplier as they are specified in GCC Clauses 20.1 and 20.2, or in Appendix3 of theContract Agreement.

21 Design and Engineering

21.1 Technical Specifications and Drawings

21.1.1 The Supplier shall execute the basic and detailed design and the implementation activities necessary for successful installation of the System in compliance with the provisions of the Contractor, where not so specified, in accordance with good industry practice.

The Supplier shall be responsible for any discrepancies, errors or omissions in the specifications, drawings, and other technical documents that it has prepared, whether such specifications, drawings, and other documents have been approved by the Project Manager or not, provided that such discrepancies, errors, or omissions are not because of in accurate information furnished in writing to the Supplier by or on behalf of the Procuring Entity.

21.1.2 The Supplier shall be entitled to disclaim responsibility for any design, data, drawing, specification, or other document, or any modification of such design, drawings, specification, or other documents provided or designated by or on behalf of the Procuring Entity, by giving a notice of such disclaimer to the Project Manager.

21.2 Codes and Standards

Wherever references are made in the Contract to codes and standards in accordance with which the Contractshall be executed, the edition or the revised version of such codes and standards current at the date twenty- eight (28) days prior to date of tender submission shall apply. During Contract execution, any changes in such codes and standards shall be applied after approval by the Procuring Entity and shall be treated in accordance with GCC Clause 39.3.

21.3.1 Approval/ Review of Controlling Technical Documents by the Project Manager

21.3.2 **Unless otherwise specified in the SCC**, there will NO Controlling Technical Documents required. However,**if the SCC specifies** Controlling Technical Documents, the Supplier shall prepare and furnish suchdocuments for the Project Manager's approval or review.

Any part of the System covered by or related to the documents to be approved by the Project Manager shallbe executed only after the Project Manager's approval of these documents.

GCC Clauses 21.3.2 through 21.3.7 shall apply to those documents requiring the Project Manager's

C2: CBK - Official

approval,but not to those furnished to the Project Manager for its review only.

21.3.3 Within fourteen (14) days after receipt by the Project Manager of any document requiring the Project Manager's approval in accordance with GCC Clause 21.3.1, the Project Manager shall either return one copyof the document to the Supplier with its approval endorsed on the document or shall notify the Supplier in writing of its disapproval of the document and the reasons for disapproval and the modifications that the Project Manager proposes. If the Project Manager fails to take such action within the fourteen (14) days, thenthe document shall be deemed to have been approved by the Project Manager.

21.3.4 The Project Manager shall not disapprove any document except on the grounds that the document does not comply with some specified provision of the Contract or that it is contrary to good industry practice.

21.3.5 If the Project Manager disapproves the document, the Supplier shall modify the document and resubmit it for the Project Manager's approval in accordance with GCC Clause 21.3.2. If the Project Manager approvesthe document subject to modification(s), the Supplier shall make the required modification(s), and the document shall then be deemed to have been approved, subject to GCC Clause 21.3.5. The procedure set outin GCC Clauses 21.3.2 through 21.3.4 shall be repeated, as appropriate, until the Project Manager approvessuch documents.

21.3.6 If any dispute occurs between the Procuring Entity and the Supplier in connection with or arising out of thedisapproval by the Project Manager of any document and/ or any modification (s) to a document that cannotbe settled between the parties within a reasonable period, then, in case the Contract Agreement includes andnames an Adjudicator, such dispute may be referred to the Adjudicator for determination in accordance withGCC Clause 43.1 (Adjudication). If such dispute is referred to an Adjudicator, the Project Manager shall give instructions as to whether and if so, how, performance of the Contract is to proceed. The Supplier shallproceed with the Contract in accordance with the Project Manager's instructions, provided that if the Adjudicator upholds the Supplier's view on the dispute and if the Procuring Entity has not given notice underGCC Clause 43.1.2, then the Supplier shall be reimbursed by the Procuring Entity for any additional costs incurred by reason of such instructions and shall be relieved of such responsibility or liability in connectionwith the dispute and the execution of the instructions as the Adjudicator shall decide, and the Time for Achieving Operational Acceptance shall be extended accordingly. The Project Manager's approval, with or without modification of the document furnished by the Supplier, shallnot relieve the Supplier of any responsibility or liability imposed upon it by any provisions of the Contract except to the extent that any subsequent failure results from modifications required by the Project Manager orinaccurate information furnished in writing to the Supplier by or on behalf of the Procuring Entity.

21.3.7 The Supplier shall not depart from any approved document unless the Supplier has first submitted to the ProjectManager an amended document and obtained the Project Manager's approval of the document, pursuant to theprovisions of this GCC Clause 21.3. If the Project Manager requests any change in any already approved document and/or in any document based on such an approved document, the provisions of GCC Clause 39 (Changes to the System) shall apply to such request.

22 Procurement, Delivery, and Transport

22.1 Subject to related Procuring Entity's responsibilities pursuant to GCC Clauses 10 and 14, the Supplier shall manufacture or procure and transport all the Information Technologies, Materials, and other Goods in an expeditious and orderly manner to the Project Site.

22.2 Delivery of the Information Technologies, Materials, and other Goods shall be made by the Supplier in accordance with the Technical Requirements.

22.3 Early or partial deliveries require the explicit written consent of the Procuring Entity, which consent shall notbe unreasonably withheld.

22.4 Packaging and Transportation

22.4.1 The Supplier shall provide such packing of the Goods as is required to prevent their damage or deterioration during shipment. The packing, marking, and documentation within and outside the packages shall comply strictly with the Procuring Entity's instructions to the Supplier.

22.4.2 The Supplier will bear responsibility for and cost of transport to the Project Sites in accordance with the termsand conditions used in the specification of prices in the Price Schedules, including the terms and conditions ofthe associated Inco terms.

22.4.3 **Unless otherwise specified in the SCC,** the Supplier shall be free to use transportation through carriers registered in any eligible country and to obtain insurance from any eligible source country.

C2: CBK - Official

Unless otherwise specified in the SCC, the Supplier will provide the Procuring Entity with shipping and otherdocuments, as specified below:

22.4.4 For Goods supplied from outside Kenya:
Upon shipment, the Supplier shall notify the Procuring Entity and the insurance company contracted by the Supplier to provide cargo insurance by cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Procuring Entity by mail or courier, as appropriate, with a copy to the cargo insurance company:

a Two copies of the Supplier's invoice showing the description of the Goods, quantity, unit price, and totalamount.

b usual transportation documents.

c insurance certificate.

d certificate (s) of origin; and

e estimated time and point of arrival in Kenya and at the site.

22.4.5 For Goods supplied locally (i.e., from within Kenya):

Upon shipment, the Supplier shall notify the Procuring Entity by cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Procuring Entity by mail or courier, as appropriate:

a Two copies of the Supplier's invoice showing the Goods' description, quantity, unit price, and total amount.

b. Delivery note, railway receipt, or truck receipt.

c. certificate of insurance.

d. certificate (s) of origin; and

e. estimated time of arrival at the site.

22.4.6 Customs Clearance

a) The Procuring Entity will bear responsibility for, and cost of, customs clearance into Kenya in accordance with the particular Incoterm(s) used for Goods supplied from outside Kenya in the Price Schedules referred to by Article2 of the Contract Agreement.

b) At the request of the Procuring Entity, the Supplier will make available a representative or agent during the process of customs clearance in Kenya for goods supplied from outside Kenya. In the event of delays in customs clearance that are not the fault of the Supplier:

i) the Supplier shall be entitled to an extension in the Time for Achieving Operational Acceptance, pursuant to GCC Clause40.

ii) the Contract Price shall be adjusted to compensate the Supplier for any additional storagecharges that the Supplier may incur as a result of the delay.

23 Product Upgrades

23.1 At any point during performance of the Contract, should technological advances be introduced by the Supplier for Information Technologies originally offered by the Supplier in its tender and still to be delivered, the Supplier shall be obligated to offer to the Procuring Entity the latest versions of the available InformationTechnologies having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC Clause39 (Changes to the System).

23.2 At any point during performance of the Contract, for Information Technologies still to be delivered, the Supplier will also pass on to the Procuring Entity any cost reductions and additional and/ or improved supportand facilities that it offers to other clients of the Supplier in Kenya, pursuant to GCC Clause39 (Changes to the System).

23.3 During performance of the Contract, the Supplier shall offer to the Procuring Entity all new versions, releases, and updates of Standard Software, as well as related documentation and technical support services,within thirty (30) days of their availability from the Supplier to other clients of the Supplier in Kenya, and no later than twelve (12) months after they are released in the country of origin. In no case will the prices for these Software exceed those quoted by the Supplier in the Recurrent Costs tables in

C2: CBK - Official

its tender.

23.4 **Unless otherwise specified in the SCC,** during the Warranty Period, the Supplier will provide at no additional cost to the Procuring Entity all new versions, releases, and updates for all Standard Software thatare used in the System, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in Kenya, and no later than twelve (12) months after they are released in the country of origin of the Software.

23.5 The Procuring Entity shall introduce all new versions, releases or updates of the Software within eighteen
(18) months of receipt of a production-ready copy of the new version, release, or update, provided that the new version, release, or update does not adversely affect System operation or performance or require extensive reworking of the System. In cases where the new version, release, or update adversely affects System operation or performance, or requires extensive reworking of the System, the Supplier shall continueto support and maintain the version or release previously in operation for as long as necessary to allow introduction of the new version, release, or update. In no case shall the Supplier stop supporting or maintaining a version or release of the Software less than twenty-four (24) months after the Procuring Entityreceives a production-ready copy of a subsequent version, release, or update. The Procuring Entity shall use all reasonable endeavors to implement any new version, release, or update as soon as practicable, subject tothe twenty-four-month-long stop date.

24 Implementation, Installation, and Other Services

24.1 The Supplier shall provide all Services specified in the Contract and Agreed Project Plan in accordance withthe highest standards of professional competence and integrity.

24.2 Prices charged by the Supplier for Services, if not included in the Contract, shall be agreed upon in advanceby the parties (including, but not restricted to, any prices submitted by the Supplier in the Recurrent Cost Schedules of its Tender) and shall not exceed the prevailing rates charged by the Supplier to other ProcuringEntity's in Kenya for similar services.

25 Inspections and Tests

25.1 The Procuring Entity or its representative shall have the right to inspect and/or test any components of the System, as specified in the Technical Requirements, to confirm their good working order and/ or conformityto the Contract at the point of delivery and/ or at the Project Site.

25.2 The Procuring Entity or its representative shall be entitled to attend any such inspections and/or tests of the components, provided that the Procuring Entity shall bear all costs and expenses incurred in connection withsuch attendance, including but not limited to all inspection agent fees, travel, and related expenses.

25.3 Should the inspected or tested components fail to conform to the Contract, the Procuring Entity may reject the component (s), and the Supplier shall either replace the rejected component (s) or make alterations as necessary so that it meets the Contract requirements free of cost to the Procuring Entity.

25.4 The Project Manager may require the Supplier to carry out any inspection and/or test not specified in the Contract, provided that the Supplier's reasonable costs and expenses incurred in the carrying out of such inspection and/ or test shall be added to the Contract Price. Further, if such inspection and/ or test impedes the progress of work on the System and/or the Supplier's performance of its other obligations under the Contract, due allowance will be made in respect of the Time for Achieving Operational Acceptance and theother obligations so affected.

25.5 If any dispute shall arise between the parties in connection with or caused by an inspection and/ or with regard to any component to be incorporated in the System that cannot be settled amicably between the partieswithin a reasonable period of time, either party may invoke the process pursuant to GCC Clause 43 (Settlement of Disputes), starting with referral of the matter to the Adjudicator in case an Adjudicator is included and named in the Contract Agreement.

C2: CBK - Official

26 Installation of the System

26.1 As soon as the System, or any Subsystem, has, in the opinion of the Supplier, been delivered, pre-commissioned, and made ready for Commissioning and Operational Acceptance Testing in accordance withthe Technical Requirements, the SCC and the Agreed Project Plan, the Supplier shall so notify the ProcuringEntity in writing.

26.2 The Project Manager shall, within fourteen (14) days after receipt of the Supplier's notice under GCC Clause26.1, either issue an Installation Certificate in the form specified in the Sample Contractual Forms Section inthe tendering documents, stating that the System, or major component or Subsystem (if Acceptance by majorcomponent or Sub system is specified pursuant to the SCC for GCC Clause27.2.1), has achieved Installationby the date of the Supplier's notice under GCC Clause 26.1, or notify the Supplier in writing of any defects and/or deficiencies, including, but not limited to, defects or deficiencies in the interoperability or integration of the various components and/or Subsystems making up the System. The Supplier shall use all reasonable endeavors to promptly remedy any defect and/ or deficiencies that the Project Manager has notified the Supplier of. The Supplier shall then promptly carryout retesting of the System or Sub system and, when in the Supplier's opinion the System or Sub system is ready for Commissioning and Operational Acceptance Testing, notify the Procuring Entity in writing, in accordance with GCC Clause 26.1. The procedure set outin this GCC Clause shall be repeated, as necessary, until an Installation Certificate is issued.

26.3 If the Project Manager fails to issue the Installation Certificate and fails to inform the Supplier of any defectsand/or deficiencies within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 26.1,orif the Procuring Entity puts the System or a Subsystem in to production operation, then the System (or Subsystem) shall be deemed to have achieved successful Installation as of the date of the Supplier's notice or repeated notice, or when the Procuring Entity put the System in to production operation, as the case maybe.

27 Commissioning and Operational Acceptance

27.1 Commissioning

27.1.1 Commissioning of the System (or Subsystem if specified pursuant to the SCC for GCC Clause 27.2.1) shallbe commenced by the Supplier:

a) immediately after the Installation Certificate is issued by the Project Manager, pursuant to GCC Clause 26.2; or

b) as otherwise specified in the Technical Requirement or the Agreed Project Plan; or

c) immediately after Installation is deemed to have occurred, under GCC Clause 26.3.

27.1.2 The Procuring Entity shall supply the operating and technical personnel and all materials and information reasonably required to enable the Supplier to carry out its obligations with respect to Commissioning. Production use of the System or Subsystem(s) shall not commence prior to the start of formal Operational Acceptance Testing.

27.2 Operational Acceptance Tests

27.2.1 The Operational Acceptance Tests (and repeats of such tests) shall be the primary responsibility of the Procuring Entity (in accordance with GCC Clause 10.9), but shall be conducted with the full cooperation of the Supplier during Commissioning of the System (or major components or Subsystem[s]), to ascertain whether the System (or major component or Subsystem[s]) conforms to the Technical Requirements and meetsthe standard of performance quoted in the Supplier's tender, including, but not restricted to, the functional andtechnical performance requirements. **Unless otherwise specified in the SCC**, the Operational Acceptance Tests during Commissioning will be conducted as specified in the Technical Requirements and/ or the Agreed Project Plan. At the Procuring Entity's discretion, Operational Acceptance Tests may also be performed on replacement Goods, upgrades and new version

C2: CBK - Official

releases, and Goods that are added or field-modified after Operational Acceptance of the System.

27.2.2 If for reasons attributable to the Procuring Entity, the Operational Acceptance Test of the System (or Subsystem[s] or major components, pursuant to the SCC for GCC Clause 27.2.1) cannot be successfully completed within ninety (90) days from the date of Installation or any other period agreed upon in writing bythe Procuring Entity and the Supplier, the Supplier shall be deemed to have fulfilled its obligations with respectto the technical and functional aspects of the Technical Specifications, SCC and/ or the Agreed Project Plan, and GCC Clause 28.2 and 28.3 shall not apply.

27.3 Operational Acceptance

27.3.1 Subject to GCC Clause 27.4 (Partial Acceptance) below, Operational Acceptance shall occur in respect of theSystem, when

a the Operational Acceptance Tests, as specified in the Technical Requirements, and/or SCC and/or the Agreed Project Plan have been successfully completed; or

b the Operational Acceptance Tests have not been successfully completed or have not been carried out for reasons that are attributable to the Procuring Entity within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause 27.2.2 above; or

c the Procuring Entity has put the System into production or use for sixty (60) consecutive days. If the System is put into production or use in this manner, the Supplier shall notify the Procuring Entity and document such use.

27.3.2 At any time after any of the events set out in GCC Clause 27.3.1 have occurred, the Supplier may give anotice to the Project Manager requesting the issue of an Operational Acceptance Certificate.

27.3.3 After consultation with the Procuring Entity, and within fourteen (14) days after receipt of the Supplier's notice, the Project Manager shall:

a Issue an Operational Acceptance Certificate; or

b Notify the Supplier in writing of any defect or deficiencies or other reason for the failure of the Operational Acceptance Tests; or

c Issue the Operational Acceptance Certificate if the situation covered by GCC Clause 27.3.1 (b) arises.

27.3.4 The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or otherreasons for the failure of the Operational Acceptance Test that the Project Manager has notified the Supplier of. Once such remedies have been made by the Supplier, the Supplier shall notify the Procuring Entity, and the Procuring Entity, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptlycarry out retesting of the System or Sub system. Upon the successful conclusion of the Operational AcceptanceTests, the Supplier shall notify the Procuring Entity of its request for Operational Acceptance Certification, in accordance with GCC Clause 27.3.3. The Procuring Entity shall then issue to the Supplier the Operational Acceptance Certification in accordance with GCC Clause 27.3.3 (a), or shall notify the Supplier of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set outin this GCC Clause27.3.4 shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.

27.3.5 If the System or Subsystem fails to pass the Operational Acceptance Test(s) in accordance with GCC Clause 27.2, the neither:

a The Procuring Entity may consider terminating the Contract, pursuant to GCC Clause41.2.2; or

b If the failure to achieve Operational Acceptance within the specified time period is a result of the failure of the Procuring Entity to fulfill its obligations under the Contract, then the Supplier shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract, and GCC Clauses 30.3 and 30.4 shall not apply.

27.3.6 If within fourteen (14) days after receipt of the Supplier's notice the Project Manager fails to issue the Operational Acceptance Certificate or fails to inform the Supplier in writing of the justifiable reasons why the Project Manager has not issued the Operational Acceptance Certificate, the System or Subsystem shall be deemed to have been accepted as of the date of the Supplier's said notice.

C2: CBK - Official

27.4 Partial Acceptance

27.4.1 If so specified in the SCC for GCC Clause 27.2.1, Installation and Commissioning shall be carried out individually for each identified major component or Subsystem (s) of the System. In this event, the provisions in the Contract relating to Installation and Commissioning, including the Operational Acceptance Test, shall apply to each such major component or Subsystem individually, and Operational Acceptance Certificate (s) shall be issued accordingly for each such major component or Subsystem of the System, subject to the limitations contained in GCC Clause 27.4.2.

27.4.2 The issuance of Operational Acceptance Certificates for individual major components or Subsystems pursuantto GCC Clause 27.4.1 shall not relieve the Supplier of its obligation to obtain an Operational Acceptance Certificate for the System as an integrated whole (if so specified in the SCC for GCC Clauses 12.1 and 27.2.1)once all major components and Subsystems have been supplied, installed, tested, and commissioned.

27.4.3 In the case of minor components for the System that by their nature do not require Commissioning or an Operational Acceptance Test (e.g., minor fittings, furnishings or site works, etc.), the Project Manager shall issue an Operational Acceptance Certificate within fourteen (14) days after the fittings and/or furnishings havebeen delivered and/or installed or the site works have been completed. The Supplier shall, however, use all reasonable endeavors to promptly remedy any defects or deficiencies in such minor components detected by the Procuring Entity or Supplier.

F. Guarantees and Liabilities

28 Operational Acceptance Time Guarantee

28.1 The Supplier guarantees that it shall complete the supply, Installation, Commissioning, and achieve Operational Acceptance of the System (or Subsystems, pursuant to the SCC for GCC Clause 27.2.1) within the time periods specified in the Implementation Schedule and/or the Agreed Project Plan pursuant to GCC Clause 8.2, or within such extended time to which the Supplier shall be entitled under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance).

28.2 **Unless otherwise specified in the SCC**, if the Supplier fails to supply, install, commission, and achieve Operational Acceptance of the System (or Subsystems pursuant to the SCC for GCC Clause 27.2.1) within the time for achieving Operational Acceptance specified in the Implementation Schedule or the Agreed Project Plan, or any extension of the time for achieving Operational Acceptance previously granted under GCC Clause 40 (Extension of Time for Achieving Operational Acceptance), the Supplier shall pay to the Procuring Entity liquidated damages at the rate of one half of one percent per week as a percentage of the Contract Price (exclusive of Recurrent Costs if any), or the relevant part of the Contract Price if a Subsystem has not achieved Operational Acceptance. The aggregate amount of such liquidated damages shall in no event exceed the amount often (10) percent of the Contract Price (exclusive of Recurrent Costs if any). Once the Maximum is reached, the Procuring Entity may consider termination of the Contract, pursuant to GCC Clause41.2.2.

28.3 **Unless otherwise specified in the SCC,** liquidated damages payable under GCC Clause 28.2 shall apply onlyto the failure to achieve Operational Acceptance of the System (and Subsystems) as specified in the Implementation Schedule and/or Agreed Project Plan. This Clause 28.3 shall not limit, however, any other rights or remedies the Procuring Entity may have under the Contract for other delays.

28.4 If liquidated damages are claimed by the Procuring Entity for the System (or Subsystem), the Supplier shall have no further liability whatsoever to the Procuring Entity in respect to the Operational Acceptance time guarantee for the System (or Subsystem). However, the payment of liquidated damages shall not in any way relieve the Supplier from any of its obligations to complete the System or from any other of its obligations andliabilities under the Contract.

C2: CBK - Official

29 Defect Liability

29.1 The Supplier warrants that the System, including all Information Technologies, Materials, and other Goods supplied and Services provided, shall be free from defects in the design, engineering, Materials, and workmanship that prevent the System and/or any of its components from fulfilling the Technical Requirementsor that limit in a material fashion the performance, reliability, or extensibility of the System and/or Subsystems. **Unless otherwise specified in the SCC**, there will be NO exceptions and/or limitations to this warranty withrespect to Software (or categories of Software). Commercial warranty provisions of products supplied under the Contract shall apply to the extent that they do not conflict with the provisions of this Contract.

29.2 The Supplier also warrants that the Information Technologies, Materials, and other Goods supplied under theContract are new, unused, and in corporate all recent improvements in design that materially affect the System'sor Subsystem's ability to fulfill the Technical Requirements.

29.3 **Unless otherwise specified in the SCC,** the Supplier warrants that :(i) all Goods components to be incorporated into the System form part of the Supplier's and/or Subcontractor's current product lines, and (ii) they have been previously released to the market.

29.4 **Unless otherwise specified in the SCC**, the Warranty Period shall commence from the date of Operational Acceptance of the System (or of any major component or Subsystem for which separate OperationalAcceptance is provided for in the Contract) and shall extend for thirty-six (36) months.

29.5 If during the Warranty Period any defect as described in GCC Clause 29.1 should be found in the design, engineering, Materials, and workmanship of the Information Technologies and other Goods supplied or of theServices provided by the Supplier, the Supplier shall promptly, in consultation and agreement with the Procuring Entity regarding appropriate remedying of the defects, and at its sole cost, repair, replace, or otherwise make good (as the Supplier shall, at its discretion, determine) such defect as well as any damage tothe System caused by such defect. Any defective Information Technologies or other Goods that have been replaced by the Supplier shall remain the property of the Supplier.

29.6 The Supplier shall not be responsible for the repair, replacement, or making good of any defect, or of anydamage to the System arising out of or resulting from any of the following causes:

a) Improper operation or maintenance of the System by the Procuring Entity.
b) Normal wear and tear.
c) use of the System with items not supplied by the Supplier, unless otherwise identified in the Technical Requirements, or approved by the Supplier; or
d) modifications made to the System by the Procuring Entity, or a third party, not approved by the Supplier.

29.7 The Supplier's obligations under this GCC Clause 29 shall not apply to:

a) any materials that are normally consumed in operation or have a normal life shorter than the Warranty Period; or any designs, specifications, or other data designed, supplied, or specified by or on behalf of the ProcuringEntity or any matters for which the Supplier has disclaimed responsibility, in accordance with GCC Clause 21.1.2.

29.8 The Procuring Entity shall give the Supplier a notice promptly following the discovery of such defect, statingthe nature of any such defect together with all available evidence. The Procuring Entity shall afford all reasonable opportunity for the Supplier to inspect any such defect. The Procuring Entity shall afford the Supplier all necessary access to the System and the site to enable the Supplier to perform its obligations under this GCC Clause 29.

29.9 The Supplier may, with the consent of the Procuring Entity, remove from the site any Information Technologies and other Goods that are defective, if the nature of the defect, and/or any damage to the Systemcaused by the defect, is such that repairs cannot be expeditiously carried out at the site. If the repair, replacement, or making good is of such a character that it may affect the efficiency of the System, the Procuring Entity may give the Supplier notice requiring that tests of the defective part be made by the Supplier immediately upon completion of such remedial work, where upon the Supplier shall carry out suchtests.

C2: CBK - Official

If such part fails the tests, the Supplier shall carry out further repair, replacement, or making good (as the case maybe) until that part of the System passes such tests. The tests shall be agreed upon by the Procuring Entity and the Supplier.

29.10 **Unless otherwise specified in the SCC**, the response times and repair/replacement times for Warranty Defect Repair are specified in the Technical Requirements. Nevertheless, if the Supplier fails to commence the work necessary to remedy such defect or any damage to the System caused by such defect within two weeks the Procuring Entity may, following notice to the Supplier, proceed to do such work or contract a third party (or parties) to do such work, and the reasonable costs incurred by the Procuring Entity in connection with such work shall be paid to the Procuring Entity by the Supplier or may be deducted by the Procuring Entity from any monies due the Supplier or claimed under the Performance Security.

29.11 If the System or Subsystem cannot be used by reason of such defect and/or making good of such defect, theWarranty Period for the System shall be extended by a period equal to the period during which the System or Subsystem could not be used by the Procuring Entity because of such defect and/or making good of suchdefect.

29.12 Items substituted for defective parts of the System during the Warranty Period shall be covered by the DefectLiability Warranty for the remainder of the Warranty Period applicable for the part replaced or three (3) months, whichever is greater. For reasons of information security, the Procuring Entity may choose to retainphysical possession of any replaced defective information storage devices.

29.13 At the request of the Procuring Entity and without prejudice to any other rights and remedies that the Procuring Entity may have against the Supplier under the Contract, the Supplier will offer all possible assistance to the Procuring Entity to seek warranty services or remedial action from any subcontracted third-party producers or licensor of Goods included in the System, including without limitation assignment or transfer in favor of the Procuring Entity of the benefit of any warranties given by such producers or licensorsto the Supplier.

30 Functional Guarantees

30.1 The Supplier guarantees that, once the Operational Acceptance Certificate(s) has been issued, the System represents a complete, integrated solution to the Procuring Entity's requirements set forth in the Technical Requirements and it conforms to all other aspects of the Contract. The Supplier acknowledges that GCC Clause 27 regarding Commissioning and Operational Acceptance govern show technical conformance of theSystem to the Contract requirements will be determined.

30.2 If, for reasons attributable to the Supplier, the System does not conform to the Technical Requirements or does not conform to all other aspects of the Contract, the Supplier shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Technical Requirements and meet all functional and performance standards. The Supplier shall notify the Procuring Entity upon completion of the necessary changes, modifications, and/or additions and shall request the Procuring Entity to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance. If the System (or Subsystem[s]) fails to achieve Operational Acceptance, the Procuring Entity may consider termination of the Contract, pursuant to GCC Clause 41.2.2, and forfeiture of the Supplier's Performance Security in accordance with GCC Clause 13.3 in compensation for the extra costs and delays likely to resultfrom this failure.

31 Intellectual Property Rights Warranty

31.1 The Supplier here by represents and warrants that:

a) The System as supplied, installed, tested, and accepted.

b) Use of the System in accordance with the Contract; and

c) Use of the Software and Materials provided to the Procuring Entity in accordance with the Contractdo not and will not infringe any Intellectual Property Rights held by any third party and that it has all

C2: CBK - Official

necessary rights or at its sole expense shall have secured in writing all transfer so frights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for the Procuring Entity to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the Supplier shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for development of the System.

32 Intellectual Property Rights Indemnity

32.1 The Supplier shall indemnify and hold harmless the Procuring Entity and its employees and officers from andagainst any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that the Procuring Entity or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of:

a) Installation of the System by the Supplier or the use of the System, including the Materials, in the country where the site is located.

b) copying of the Software and Materials provided by the Supplier in accordance with the Agreement; and

c) sale of the products produced by the System in any country, except to the extent that such losses, liabilities, and costs arise as a result of the Procuring Entity's breach of GCC Clause 32.2.

32.2 Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose indicated by or to be reasonably inferred from the Contract, any infringement resulting from the use of the System, or any products of the System produced there by in association or combination with any other goodsor services not supplied by the Supplier, where the infringement arises because of such association or combination and not because of use of the System in its own right.

32.3 Such indemnities shall also not apply if any claim of infringement:

a) Is asserted by a parent, subsidiary, or affiliate of the Procuring Entity's organization.

b) Is a direct result of a design mandated by the Procuring Entity's Technical Requirements and the possibility of such infringement was duly noted in the Supplier's Tender; or

c) Results from the alteration of the System, including the Materials, by the Procuring Entity or anypersons other than the Supplier or a person authorized by the Supplier.

32.4 If any proceedings are brought or any claim is made against the Procuring Entity arising out of the matters referred to in GCC Clause 32.1, the Procuring Entity shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Procuring Entity's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.

If the Supplier fails to notify the Procuring Entity within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Procuring Entity shall be free to conduct thesame on its own behalf. Unless the Supplier has so failed to notify the Procuring Entity within the twenty- eight (28) days, the Procuring Entity shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Procuring Entity shall, at the Supplier's request, afford all available assistanceto the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing.

32.5 The Procuring Entity shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from and against any and all losses, liabilities, and costs (including losses, liabilities, and costsincurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of any infringement or alleged infringement of any Intellectual PropertyRights arising out of or in connection with any design, data, drawing, specification, or other documents or materials provided to the Supplier in connection with this Contract by the Procuring Entity or any persons (other than the Supplier) contracted by the Procuring Entity, except to the extent that such losses, liabilities, and costs arise as a result of the Supplier's breach of GCC Clause 32.8.

C2: CBK - Official

32.6 Such indemnity shall not cover

a) any use of the design, data, drawing, specification, or other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract.

b) any infringement resulting from the use of the design, data, drawing, specification, or other documents or materials, or any products produced thereby, in association or combination with any other Goods or Services not provided by the Procuring Entity or any other person contracted by the Procuring Entity, where the infringement arises because of such association or combination and not because of the use of the design, data, drawing, specification, or other documents or materials in its own right.

32.7 Such indemnities shall also not apply:

a) If any claim of infringement is asserted by apparent, subsidiary, or affiliate of the Supplier's organization.

b) to the extent that any claim of infringement is caused by the alteration, by the Supplier, or any persons contracted by the Supplier, of the design, data, drawing, specification, or other documents or materials provided to the Supplier by the Procuring Entity, or any persons contracted by the Procuring Entity.

32.8 If any proceedings are brought or any claim is made against the Supplier arising out of the matters referred toin GCC Clause 32.5, the Supplier shall promptly give the Procuring Entity notice of such proceedings or claims, and the Procuring Entity may at its own expense and in the Supplier's, name conduct such proceedingsor claim and any negotiations for the settlement of any such proceedings or claim. If the Procuring Entity failsto notify the Supplier within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless the Procuring Entity has so failed to notify the Supplier within the twenty-eight (28) days, the Supplier shall makeno admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at the Procuring Entity's request, afford all available assistance to the Procuring Entity in conducting such proceedings or claim and shall be reimbursed by the Procuring Entity for all reasonable expenses incurred in so doing.

33 Limitation of Liability

33.1 Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

a) the Supplier shall not be liable to the Procuring Entity, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Procuring Entity; and

b) the aggregate liability of the Supplier to the Procuring Entity, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Procuring Entity with respect to intellectual property rights infringement.

G. Risk Distribution

34 Transfer of Ownership

34.1 With the exception of Software and Materials, the ownership of the Information Technologies and other Goodsshall be transferred to the Procuring Entity at the time of Delivery or otherwise under terms that may be agreedupon and specified in the Contract Agreement.

34.2 Ownership and the terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC Clause 15 (Copyright) and any elaboration in the Technical Requirements. Ownership of the Supplier's Equipment used by the Supplier and its Subcontractors in connection with the Contract shall remain with the Supplier or its Subcontractors.

C2: CBK - Official

35 Care of the System

35.1 The Procuring Entity shall be come responsible for the care and custody of the System or Subsystems upon their Delivery. The Procuring Entity shall make good at its own cost any loss or damage that may occur to theSystem or Subsystems from any cause from the date of Delivery until the date of Operational Acceptance of the System or Subsystems, pursuant to GCC Clause 27 (Commissioning and Operational Acceptance), exceptsuch loss or damage arising from acts or omissions of the Supplier, its employees, or subcontractors.

35.2 If any loss or damage occurs to the System or any part of the System by reason of:

a) (in so far as they relate to the country where the Project Site is located) nuclear reaction, nuclear radiation, radioactive contamination, a pressure wave caused by aircraft or other aerial objects, or any other occurrences that an experienced contractor could not reasonably foresee, or if reasonably foreseeable could not reasonably make provision for or insure against, in so far as such risks are not normally insurable on the insurance market and are mentioned in the general exclusions of the policy of insurance taken out under GCC Clause 37;

b) Any use not in accordance with the Contract, by the Procuring Entity or any third party.

c) Any use of or reliance upon any design, data, or specification provided or designated by or on behalf of the Procuring Entity, or any such matter for which the Supplier has disclaimed responsibility in accordance with GCC Clause 21.1.2, the Procuring Entity shall pay to the Supplier all sums payable in respect of the System or Subsystems that have achieved Operational Acceptance, notwithstanding that the same be lost, destroyed, or damaged. If the Procuring Entity requests the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Supplier shall make good the same at the cost of the Procuring Entity in accordance with GCC Clause 39. If the Procuring Entity does not request the Supplier in writing to make good any loss or damage to the System there by occasioned, the Procuring Entity shall either request a change in accordance with GCC Clause 39, excluding the performance of that part of the System there by lost, destroyed, or damaged, or, where the loss or damage affects a substantial part of the System, the Procuring Entity shall terminate the Contract pursuant to GCC Clause 41.1.

35.3 The Procuring Entity shall be liable for any loss of or damage to any Supplier's Equipment which the ProcuringEntity has authorized to locate within the Procuring Entity's premises for use in fulfillment of Supplier's obligations under the Contract, except where such loss or damage arises from acts or omissions of the Supplier,its employees, or subcontractors.

36 Loss of or Damage to Property; Accident or Injury to Workers; Indemnification

36.1 The Supplier and each and every Subcontractor shall abide by the job safety, insurance, customs, and immigration measures prevalent and laws in force in Kenya.

36.2 Subject to GCC Clause 36.3, the Supplier shall indemnify and hold harmless the Procuring Entity and its employees and officers from and against any and all losses, liabilities and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Procuring Entity or its employees orofficers may suffer as a result of the death or injury of any person or loss of or damage to any property (otherthan the System, whether accepted or not) arising in connection with the supply, installation, testing, and Commissioning of the System and by reason of the negligence of the Supplier or its Subcontractors, or their employees, officers or agents, except any injury, death, or property damage caused by the negligence of the Procuring Entity, its contractors, employees, officers, or agents.

36.3 If any proceedings are brought or any claim is made against the Procuring Entity that might subject the Supplierto liability under GCC Clause 36.2, the Procuring Entity shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Procuring Entity's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Supplier fails to notify the Procuring Entity within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Procuring Entity shall be free to conduct the sameon its own behalf. Unless the Supplier has so failed to notify the

C2: CBK - Official

Procuring Entity within the twenty-eight (28) day period, the Procuring Entity shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Procuring Entity shall, at the Supplier's request, afford all available assistance to the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonableexpenses incurred in so doing. The Procuring Entity shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred indefending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors maysuffer as a result of the death or personal injury of any person or loss of or damage to property of the ProcuringEntity, other than the System not yet achieving Operational Acceptance, that is caused by fire, explosion, or any other perils, in excess of the amount recoverable from insurances procured under GCC Clause 37 (Insurances), provided that such fire, explosion, or other perils were not caused by any act or failure of the Supplier.

36.4 If any proceedings are brought or any claim is made against the Supplier that might subject the Procuring Entity to liability under GCC Clause 36.4, the Supplier shall promptly give the Procuring Entity notice of such proceedings or claims, and the Procuring Entity may at its own expense and in the Supplier's, name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Procuring Entity fails to notify the Supplier within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless the Procuring Entity has so failed to notify the Supplier within the twenty-eight (28) days,the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim.The Supplier shall, at the Procuring Entity's request, provide all available assistance to the Procuring Entity inconducting such proceedings or claim and shall be reimbursed by the Procuring Entity for all reasonable expenses incurred in so doing.

36.5 The party entitled to the benefit of an indemnity under this GCC Clause 36 shall take all reasonable measuresto mitigate any loss or damage that has occurred. If the party fails to take such measures, the other party's liabilities shall be correspondingly reduced.

37 Insurances

37.1 The Supplier shall at its expense take out and maintain in effect or cause to be taken out and maintained in effect, during the performance of the Contract, the insurance set forth below. The identity of the insurers and the form of the policies shall be subject to the approval of the Procuring Entity, who should not unreasonablywith hold such approval.

a) Cargo Insurance During Transport

as applicable, 110 percent of the price of the Information Technologies and other Goods in a freely convertible currency, covering the Goods from physical loss or damage during shipment through receipt at the Project Site.

b) Installation "All Risks" Insurance

as applicable, 110 percent of the price of the Information Technologies and other Goods covering the Goods at the site from all risks of physical loss or damage (excluding only perils commonly excluded under "all risks" insurance policies of this type by reputable insurers) occurring prior to Operational Acceptance of the System.

c) Third-Party Liability Insurance

On terms as **specified in the SCC,** covering bodily injury or death suffered by third parties (including the Procuring Entity's personnel) and loss of or damage to property (including the Procuring Entity's property and any Subsystems that have been accepted by the Procuring Entity) occurring in connection with the supply and installation of the Information System.

d) Automobile Liability Insurance

In accordance with the statutory requirements prevailing in Kenya, covering use of all vehicles used by the Supplier or its Subcontractors (whether or not owned by them) in connection with the execution of the Contract.

C2: CBK - Official

e) Other Insurance (if any), as **specified in the SCC.**

37.2 The Procuring Entity shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause 37.1, except for the Third-Party Liability, and the Supplier's Subcontractors shall benamed as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause 37.1 exceptfor Cargo Insurance During Transport. All insurer's rights of subrogation against such co-insured for losses orclaims arising out of the performance of the Contract shall be waived under such policies.

37.3 The Supplier shall deliver to the Procuring Entity certificates of insurance (or copies of the insurance policies)as evidence that the required policies are in full force and effect. The Supplier shall ensure that, where applicable, its Subcontractor(s) shall take out and maintain in effect adequate insurance policies for their personnel and vehicles and for work executed by them under the Contract, unless such Subcontractors are covered by the policies taken out by the Supplier.

37.4 If the Supplier fails to take out and/or maintain in effect the insurance referred to in GCC Clause 37.1, the Procuring Entity may takeout and maintain in effect any such insurance and may from time to time deduct from any amount due to the Supplier under the Contract any premium that the Procuring Entity shall have paidto the insurer or may otherwise recover such amount as a debt due from the Supplier.

37.5 Unless otherwise provided in the Contract, the Supplier shall prepare and conduct all and any claims made under the policies affected by it pursuant to this GCC Clause 37, and all monies payable by any insurers shallbe paid to the Supplier. The Procuring Entity shall give to the Supplier all such reasonable assistance as may be required by the Supplier in connection with any claim under the relevant insurance policies. With respect to insurance claims in which the Procuring Entity's interest is involved, the Supplier shall not give any releaseor make any compromise with the insurer without the prior written consent of the Procuring Entity. With respect to insurance claims in which the Supplier's interest is involved, the Procuring Entity shall not give anyrelease or make any compromise with the insurer without the prior written consent of the Supplier.

38 Force Majeure

38.1 "Force Majeure" shall mean any event beyond the reasonable control of the Procuring Entity or of the Supplier,as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected and shall include, without limitation, the following:

a) war, hostilities, or war like operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war.

b) rebellion, revolution, insurrection, mutiny, usurpation of civil or military government, conspiracy, riot, civil commotion, and terrorist acts.

c) confiscation, nationalization, mobilization, commandeering or requisition by or under the order of any government or dejure or defacto authority or ruler, or any other act or failure to act of any local state or national government authority.

d) strike, sabotage, lockout, embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague.

e) earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster.

f) failure, by the Supplier, to obtain the necessary export permit (s) from the governments of the Country(s) of Origin of the Information Technologies or other Goods, or Supplier's Equipment provided that the Supplier has made all reasonable efforts to obtain the required export permit(s), including the exercise of due diligence in determining the eligibility of the System and all of its components for receipt of the necessary export permits.

38.2 If either party is prevented, hindered, or delayed from or in performing any of its obligations under the

C2: CBK - Official

Contractby an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen (14) days after the occurrence of such event.

38.3 The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The Time for Achieving Operational Acceptance shall be extended in accordance with GCC Clause 40 (Extension of Time for AchievingOperational Acceptance).

38.4 The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfill its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract under GCC Clause 38.6.

38.5 No delay or nonperformance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

a) Constitute a default or breach of the Contract.

b) (Subject to GCC Clauses 35.2, 38.3, and 38.4) give rise to any claim for damages or additional cost or expense occasioned by the delay or nonperformance, if, and to the extent that, such delay or non-performance is caused by the occurrence of an event of Force Majeure.

38.6 If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of morethan sixty (60) days or an aggregate period of more than one hundred and twenty (120) days on account of oneor more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

38.7 In the event of termination pursuant to GCC Clause 38.6, the rights and obligations of the Procuring Entity and the Supplier shall be as specified in GCC Clauses 41.1.2 and 41.1.3.

38.8 Notwithstanding GCC Clause 38.5, Force Majeure shall not apply to any obligation of the Procuring Entity tomake payments to the Supplier under this Contract.

H. Change in Contract Elements

39 Changes to the System

39.1 Introducing a Change

39.1.1 Subject to GCC Clauses 39.2.5 and 39.2.7, the Procuring Entity shall have the right to propose, and subsequently require, the Project Manager to order the Supplier from time to time during the performance of the Contract to make any change, modification, addition, or deletion to, in, or from the System (interchangeably called “Change”), provided that such Change falls within the general scope of the System, does not constitute unrelated work, and is technically practicable, taking into account both the state of advancement of the System and the technical compatibility of the Change envisaged with the nature of the System as originally specified in the Contract.

39.1.2 A Change may involve, but is not restricted to, the substitution of updated Information Technologies and related Services in accordance with GCC Clause 23 (Product Upgrades).

39.1.3 The Supplier may from time to time during its performance of the Contract propose to the Procuring Entity (with a copy to the Project Manager) any Change that the Supplier considers necessary or desirable to improvethe quality or efficiency of the System. The Procuring Entity may at its discretion approve or reject any Changeproposed by the Supplier.

C2: CBK - Official

39.1.4 Notwithstanding GCC Clauses 39.1.1 and 39.1.2, no change made necessary because of any default of the Supplier in the performance of its obligations under the Contract shall be deemed to be a Change, and such change shall not result in any adjustment of the Contract Price or the Time for Achieving Operational Acceptance.

39.1.5 The procedure on how to proceed with and execute Changes is specified in GCC Clauses 39.2 and 39.3, and further details and sample forms are provided in the Sample Contractual Forms Section in the tendering documents.

39.1.6 Moreover, the Procuring Entity and Supplier will agree, during development of the Project Plan, to a date priorto the scheduled date for Operational Acceptance, after which the Technical Requirements for the System shallbe "frozen." Any Change initiated after this time will be dealt with after Operational Acceptance.

39.2 Changes Originating from Procuring Entity

39.2.4 If the Procuring Entity proposes a Change pursuant to GCC Clauses 39.1.1, it shall send to the Supplier a "Request for Change Proposal," requiring the Supplier to prepare and furnish to the Project Manager as soon as reasonably practicable a "Change Proposal," which shall include the following:

a Brief description of the Change.

b Impact on the Time for Achieving Operational Acceptance.

c Detailed estimated cost of the Change.

d Effect on Functional Guarantees (if any)

e Effect on any other provisions of the Contract.

39.2.5 Prior to preparing and submitting the "Change Proposal," the Supplier shall submit to the Project Manager a "Change Estimate Proposal," which shall be an estimate of the cost of preparing the Change Proposal, plus a first approximation of the suggested approach and cost for implementing the changes. Upon receipt of the Supplier's Change Estimate Proposal, the Procuring Entity shall do one of the following:

a accept the Supplier's estimate with instructions to the Supplier to proceed with the preparation of theChange Proposal.

b advise the Supplier of any part of its Change Estimate Proposal that is unacceptable and request theSupplier to review its estimate.

c advise the Supplier that the Procuring Entity does not intend to proceed with the Change.

39.2.6 Upon receipt of the Procuring Entity's instruction to proceed under GCC Clause 39.2.2 (a), the Supplier shall,with proper expedition, proceed with the preparation of the Change Proposal, in accordance with GCC Clause
39.2.1. The Supplier, at its discretion, may specify a validity period for the Change Proposal, after which if the Procuring Entity and Supplier has not reached agreement in accordance with GCC Clause 39.2.6, then GCC Clause 39.2.7 shall apply.

39.2.7 The pricing of any Change shall, as far as practicable, be calculated in accordance with the rates and prices included in the Contract. If the nature of the Change is such that the Contract rates and prices are in equitable,the parties to the Contract shall agree on other specific rates to be used for valuing the Change.

39.2.8 If before or during the preparation of the Change Proposal it becomes apparent that the aggregate impact of compliance with the Request for Change Proposal and with all other Change Orders that have already becomebinding upon the Supplier under this GCC Clause 39 would be to increase or decrease the Contract Price as originally set forth in Article 2 (Contract Price) of the Contract Agreement by more than fifteen (15) percent, the Supplier may give a written notice of objection to this Request for Change Proposal prior to furnishing theChange Proposal. If the Procuring Entity accepts the Supplier's objection, the Procuring Entity shall withdrawthe proposed Change and shall notify the Supplier in writing of its

C2: CBK - Official

acceptance.

The Supplier's failure to so object to a Request for Change Proposal shall neither affect its right to object to any subsequent requested Changes or Change Orders, nor affect its right to take into account, when making such subsequent objection, the percentage increase or decrease in the Contract Price that any Change not objected to by the Supplier represents.

39.2.9 Upon receipt of the Change Proposal, the Procuring Entity and the Supplier shall mutually agree upon all matters contained in the Change Proposal. Within fourteen (14) days after such agreement, the Procuring Entity shall, if it intends to proceed with the Change, issue the Supplier a Change Order. If the Procuring Entityis unable to reach a decision within fourteen (14) days, it shall notify the Supplier with details of when the Supplier can expect a decision. If the Procuring Entity decides not to proceed with the Change for whatever reason, it shall, within the said period of fourteen (14) days, notify the Supplier accordingly. Under such circumstances, the Supplier shall be entitled to reimbursement of all costs reasonably incurred by it in the preparation of the Change Proposal, provided that these do not exceed the amount given by the Supplier in itsChange Estimate Proposal submitted in accordance with GCC Clause 39.2.2.

39.2.10 If the Procuring Entity and the Supplier cannot reach agreement on the price for the Change, an equitable adjustment to the Time for Achieving Operational Acceptance, or any other matters identified in the Change Proposal, the Change will not be implemented. However, this provision does not limit the rights of either partyunder GCC Clause 6 (Settlement of Disputes).

39.3 Changes Originating from Supplier

If the Supplier proposes a Change pursuant to GCC Clause 39.1.2, the Supplier shall submit to the Project Manager a written "Application for Change Proposal," giving reasons for the proposed Change and includingthe information specified in GCC Clause 39.2.1. Upon receipt of the Application for Change Proposal, the parties shall follow the procedures outlined in GCC Clauses 39.2.6 and 39.2.7. However, should the ProcuringEntity choose not to proceed, or the Procuring Entity and the Supplier cannot come to agreement on the change during any validity period that the Supplier may specify in its Application for Change Proposal, the Supplier shall not be entitled to recover the costs of preparing the Application for Change Proposal, unless subject to an agreement between the Procuring Entity and the Supplier to the contrary.

39.4 Value engineering. The Supplier may prepare, at its own cost, a value engineering proposal at any time duringthe performance of the Contract.

39.4.1 The value engineering proposal shall, at a minimum, include the following.

(a) The proposed change (s), and a description of the difference to the existing Contract requirements.

(b) a full cost/benefit analysis of the proposed change(s) including a description and estimate of costs (including life cycle costs) the Procuring Entity may incur in implementing the value engineering proposal; and

(c) a description of any effect(s) of the change on performance/ functionality.

39.4.2 The Procuring Entity may accept the value engineering proposal if the proposal demonstrates benefits that:

a) accelerates the delivery period; or

b) reduces the Contract Price or the life cycle costs to the Procuring Entity; or

c) improves the quality, efficiency, safety or sustainability of the systems; or

d) yields any other benefits to the Procuring Entity, without compromising the necessary functions of the systems.

39.4.3 If the value engineering proposal is approved by the Procuring Entity and results in:

C2: CBK - Official

a) a reduction of the Contract Price; the amount to be paid to the Supplier shall be the percentagespecified in the **SCC** of the reduction in the Contract Price; or

b) an increase in the Contract Price; but results in a reduction in life cycle costs due to any benefit described in
(a) to (d) above, the amount to be paid to the Supplier shall be the full increase in the Contract Price.

40 Extension of Time for Achieving Operational Acceptance

40.1 The time(s) for achieving Operational Acceptance specified in the Schedule of Implementation shall be extended if the Supplier is delayed or impeded in the performance of any of its obligations under the Contract by reason of any of the following:
a) Any Change in the System as provided in GCC Clause39 (Change in the Information System).
b) Any occurrence of Force Majeure as provided in GCC Clause 38 (Force Majeure).
c) Default of the Procuring Entity; or
d) Any other matter specifically mentioned in the Contract; by such period as shall be fair and reasonable in all the circumstances and as shall fairly reflect the delay or impediment sustained by the Supplier.

40.2 Except where otherwise specifically provided in the Contract, the Supplier shall submit to the Project Managera notice of a claim for an extension of the time for achieving Operational Acceptance, together with particularsof the event or circumstance justifying such extension as soon as reasonably practicable after the commencement of such event or circumstance. As soon as reasonably practicable after receipt of such notice and supporting particulars of the claim, the Procuring Entity and the Supplier shall agree upon the period of such extension. In the event that the Supplier does not accept the Procuring Entity's estimate of a fair and reasonable time extension, the Supplier shall be entitled to refer the matter to the provisions for the Settlementof Disputes pursuant to GCC Clause 43.

40.3 The Supplier shall at all times use its reasonable efforts to minimize any delay in the performance of its obligations under the Contract.

41 Termination

41.1 Termination for Procuring Entity's Convenience

41.1.1 The Procuring Entity may at any time and upon issuance of a Sixty (60) day notice terminate the Contract for any reason by giving the Supplier a noticeof termination that refers to this GCC Clause 41.1.

41.1.2 Upon receipt of the notice of termination under GCC Clause 41.1.1, the Supplier shall either as soon as reasonably practical or upon the date specified in the notice of termination

a) cease all further work, except for such work as the Procuring Entity may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition.

b) terminate all subcontracts, except those to be assigned to the Procuring Entity pursuant to GCC Clause (d)
(ii) below.

c) Remove all Supplier's Equipment from the site, repatriate the Supplier's and its Sub contractors' personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind.

d) In addition, the Supplier, subject to the payment specified in GCC Clause 41.1.3, shall

i) deliver to the Procuring Entity the parts of the System executed by the Supplier up to the date of termination.

ii) to the extent legally possible, assign to the Procuring Entity all right, title, and benefit of the Supplierto the System, or Subsystem, as at the date of termination, and, as may be required by the ProcuringEntity, in any subcontracts concluded between the Supplier and its Subcontractors.

C2: CBK - Official

iii) deliver to the Procuring Entity all nonproprietary drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.1.3 In the event of termination of the Contract under GCC Clause 41.1.1, the Procuring Entity shall pay to theSupplier the following amounts:

a) The Contract Price, properly attributable to the parts of the System executed by the Supplier as of the date of termination.

b) The costs reasonably incurred by the Supplier in the removal of the Supplier's Equipment from the site and in the repatriation of the Supplier's and its Subcontractors 'personnel.

c) any amount to be paid by the Supplier to its Subcontractors in connection with the termination of any subcontracts, including any cancellation charges.

d) costs incurred by the Supplier in protecting the System and leaving the site in a clean and safe condition pursuant to GCC Clause 41.1.2(a); and

e) the cost of satisfying all other obligations, commitments, and claims that the Supplier may in good faith have undertaken with third parties in connection with the Contract and that are not covered by GCC Clauses 41.1.3 (a) through (d) above.

41.2 Termination for Supplier's Default

41.2.1 The Procuring Entity, without prejudice to any other rights or remedies it may possess, may terminate the Contract forthwith in the following circumstances by giving a notice of termination and its reasons there forto the Supplier, referring to this GCC Clause41.2:

a) If the Supplier becomes bankrupt or in solvent, has a receiving order issued against it, compounds with its creditors, or, if the Supplier is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Supplier takes or suffers any other analogous action in consequence of debt;

b) If the Supplier assigns or transfers the Contractor any right or interest, there in in violation of the provision of GCC Clause 42 (Assignment); or

If the Supplier, in the judgment of the Procuring Entity has engaged in Fraud and Corruption, as defined in paragraph 2.2a. of the Appendix to the GCC, in competing for or in executing the Contract, including but not limited to willful misrepresentation of facts concerning ownership of Intellectual Property Rights in, or proper authorization and/or licenses from the owner to offer, the hardware, software, or materials provided under this Contract.

41.2.2 If the Supplier:

c) Has abandoned or repudiated the Contract.

d) Has without valid reason failed to commence work on the System promptly.

e) Persistently fails to execute the Contract in accordance with the Contract or persistently neglects to carry out its obligations under the Contract without just cause.

f) Refuses or is unable to provide sufficient Materials, Services, or labor to execute and complete the System in the manner specified in the Agreed Project Plan furnished under GCC Clause 19 at rates of progress that give reasonable assurance to the Procuring Entity that the Supplier can attain Operational Acceptance of the System by the Time for Achieving Operational Acceptance as extended; then the Procuring Entity may, without prejudice to any other rights it may possess under the Contract, give a notice to the Supplier stating the nature of the default and requiring the Supplier to remedy the same. If the Supplier fails to remedy or to take steps to remedy the same with in fourteen (14) days of its receipt of such notice, then the Procuring Entity may terminate the Contract forthwith by giving a notice of termination to the Supplier that refers to this GCC Clause 41.2.

41.2.3 Upon receipt of the notice of termination under GCC Clauses 41.2.1 or 41.2.2, the Supplier shall, either immediately or upon such date as is specified in the notice of termination:

C2: CBK - Official

g) cease all further work, except for such work as the Procuring Entity may specify in the notice of termination for the sole purpose of protecting that part of the System already executed or any work required to leave the site in a clean and safe condition.

h) terminate all subcontracts, except those to be assigned to the Procuring Entity pursuant to GCC Clause (d)below.

i) deliver to the Procuring Entity the parts of the System executed by the Supplier up to the date of termination.

j) to the extent legally possible, assign to the Procuring Entity all right, title and benefit of the Supplier to the System or Subsystems as at the date of termination, and, as may be required by the Procuring Entity, in any subcontracts concluded between the Supplier and its Subcontractors.

k) deliver to the Procuring Entity all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as at the date of termination in connection with the System.

41.2.4 The Procuring Entity may enter upon the site, expel the Supplier, and complete the System itself or by employing any third party. Upon completion of the System or at such earlier date as the Procuring Entity thinksappropriate, the Procuring Entity shall give notice to the Supplier that such Supplier's Equipment will be returned to the Supplier at or near the site and shall return such Supplier's Equipment to the Supplier in accordance with such notice. The Supplier shall thereafter without delay and at its cost remove or arrange removal of the same from the site.

41.2.5 Subject to GCC Clause 41.2.6, the Supplier shall be entitled to be paid the Contract Price attributable to the portion of the System executed as at the date of termination and the costs, if any, incurred in protecting the System and in leaving the site in a clean and safe condition pursuant to GCC Clause 41.2.3 (a). Any sums duethe Procuring Entity from the Supplier accruing prior to the date of termination shall be deducted from the amount to be paid to the Supplier under this Contract.

41.2.6 If the Procuring Entity completes the System, the cost of completing the System by the Procuring Entity shallbe determined. If the sum that the Supplier is entitled to be paid, pursuant to GCC Clause 41.2.5, plus the reasonable costs incurred by the Procuring Entity in completing the System, exceeds the Contract Price, the Supplier shall be liable for such excess. If such excess is greater than the sums due the Supplier under GCC Clause41.2.5, the Supplier shall pay the balance to the Procuring Entity, and if such excess is less than the sums due the Supplier under GCC Clause 41.2.5, the Procuring Entity shall pay the balance to the Supplier. The Procuring Entity and the Supplier shall agree, in writing, on the computation described above and the manner in which any sums shall be paid.

41.3 Termination by Supplier

41.3.1 If:

a) the Procuring Entity has failed to pay the Supplier any sum due under the Contract within the specified period, has failed to approve any invoice or supporting documents without just cause **pursuant to the SCC,** or commits a substantial breach of the Contract, the Supplier may give a notice to the Procuring Entity that requires payment of such sum, with interest on this sum as stipulated in GCC Clause 12.3, requires approval of such invoice or supporting documents, or specifies the breach and requires the Procuring Entity to remedy the same, as the case may be. If the Procuring Entity fails to pay such sum together with such interest, fails to approve such invoice or supporting documents or give its reasons for withholding such approval, fails to remedy the breach or take steps to remedy the breach within fourteen (14) days after receipt of the Supplier's notice; or

b) the Supplier is unable to carry out any of its obligations under the Contract for any reason attributable to the Procuring Entity, including but not limited to the Procuring Entity's failure to provide possession of or access to the site or other areas or failure to obtain any governmental permit necessary for the execution and/or completion of the System; then the Supplier may give a notice to the Procuring Entity of such events, and if the Procuring Entity has failed to pay the outstanding sum, to approve the invoice or supporting documents, to give its reasons for withholding such approval, or to remedy the breach within twenty-eight (28) days of such notice, or if the Supplier is still unable to carry out any of its

C2: CBK - Official

obligations under the Contract for any reason attributable to the Procuring Entity within twenty-eight (28) days of the said notice, the Supplier may by a further notice to the Procuring Entity referring to this GCC Clause 41.3.1, forth with terminate the Contract.

41.3.2 The Supplier may terminate the Contract immediately by giving a notice to the Procuring Entity to that effect, referring to this GCC Clause 41.3.2, if the Procuring Entity becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, being a corporation, if a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Procuring Entity takes or suffers any other analogous action in consequence of debt.

41.3.3 If the Contract is terminated under GCC Clauses 41.3.1 or 41.3.2, then the Supplier shall immediately:

a. Cease all further work, except for such work as may be necessary for the purpose of protecting that partof the System already executed, or any work required to leave the site in a clean and safe condition.
b. Terminate all subcontracts, except those to be assigned to the Procuring Entity pursuant to Clause 41.3.3 d(ii).
c. remove all Supplier's Equipment from the site and repatriate the Supplier's and its Subcontractor'spersonnel from the site.
d. In addition, the Supplier, subject to the payment specified in GCC Clause 41.3.4, shall:

i) deliver to the Procuring Entity the parts of the System executed by the Supplier up to the date of termination.

ii) to the extent legally possible, assign to the Procuring Entity all right, title, and benefit of the Supplier to the System, or Subsystems, as of the date of termination, and, as may be required bythe Procuring Entity, in any subcontracts concluded between the Supplier and its Subcontractors.

iii) to the extent legally possible, deliver to the Procuring Entity all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.3.4 If the Contract is terminated under GCC Clauses 41.3.1or 41.3.2, the Procuring Entity shall pay to the Supplierall payments specified in GCC Clause 41.1.3 and reasonable compensation for all loss, except for loss of profit, or damage sustained by the Supplier arising out of, in connection with, or in consequence of such termination.

41.3.5 Termination by the Supplier pursuant to this GCC Clause 41.3 is without prejudice to any other rights or remedies of the Supplier that may be exercised in lieu of or in addition to rights conferred by GCC Clause41.3.

41.4 In this GCC Clause 41, the expression “portion of the System executed” shall include all work executed, Services provided, and all Information Technologies, or other Goods acquired (or subject to a legally binding Obligation to purchase) by the Supplier and used or intended to be used for the purpose of the System, up to and including the date of termination.

41.5 In this GCC Clause 41, in calculating any monies due from the Procuring Entity to the Supplier, account shall be taken of any sum previously paid by the Procuring Entity to the Supplier under the Contract, including any advance payment paid **pursuant to the SCC.**

42 Assignment

42.1 Neither the Procuring Entity nor the Supplier shall, without the express prior written consent of the other, assign to any third party the Contractor any part thereof, or any right, benefit, obligation, or interest there inor there under, except that the Supplier shall be entitled to assign either absolutely or by way of charge any monies due and payable to it or that may become due and payable to it under the Contract.

I. Settlement of Disputes

C2: CBK - Official

43 Settlement of Disputes

43.1 Adjudication

43.1.1 If any dispute of any kind what so ever shall arise between the Procuring Entity and the Supplier in connectionwith or arising out of the Contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity, or termination, or the operation of the System (whether during the progress of implementation or after its achieving Operational Acceptance and whether before or after the termination, abandonment, or breach of the Contract), the parties shall seek to resolve any such dispute **by mutual consultation**. If the parties fail to resolve such a dispute by mutual consultation within fourteen (14)days after one party has notified the other in writing of the dispute, then, if the Contract Agreement in Appendix2 includes and names an Adjudicator, the dispute shall, within another fourteen (14) days, be referred in writing by either party to the Adjudicator, with a copy to the other party. If there is no Adjudicator specified in the Contract Agreement, the mutual consultation period stated above shall last twenty-eight (28)days (instead of fourteen), upon expiry of which either party may move to the notification of arbitration pursuant to GCC Clause43.2.1.

43.1.2 The Adjudicator shall give his or her decision in writing to both parties within twenty-eight (28) days of thedispute being referred to the Adjudicator. If the Adjudicator has done so, and no notice of intention to commence arbitration has been given by either the Procuring Entity or the Supplier within fifty-six (56) daysof such reference, the decision shall become final and binding upon the Procuring Entity and the Supplier. Any decision that has become final and binding shall be implemented by the parties forth with.

43.1.3 The Adjudicator shall be paid an hourly fee at the rate specified in the Contract Agreement plus reasonable expenditures incurred in the execution of duties as Adjudicator, and these costs shall be divided equally between the Procuring Entity and the Supplier.

43.1.4 Should the Adjudicator resign or die, or should the Procuring Entity and the Supplier agree that the Adjudicator is not fulfilling his or her functions in accordance with the provisions of the Contract, a new Adjudicator shall be jointly appointed by the Procuring Entity and the Supplier. Failing agreement between the two within twenty-eight (28) days, the new Adjudicator shall be appointed at the request of either party by the Appointing Authority **specified in the SCC,** or, if no Appointing Authority is **specified in SCC,** the Contract shall, from this point onward and until the parties may otherwise agree on an Adjudicator or an Appointing Authority, be implemented as if there is no Adjudicator.

43.2 Arbitration

43.2.1 If

a) the Procuring Entity or the Supplier is dissatisfied with the Adjudicator's decision and acts before this decision has become final and binding pursuant to GCC Clause 43.1.2, or

b) the Adjudicator fails to give a decision within the allotted time from referral of the dispute pursuant to GCC Clause 43.1.2, and the Procuring Entity or the Supplier acts within the following fourteen (14) days, or

c) in the absence of an Adjudicator from the Contract Agreement, the mutual consultation pursuant to GCC Clause 43.1.1 expires without resolution of the dispute and the Procuring Entity or the Supplier acts within the following fourteen (14) days, then either the Procuring Entity or the Supplier may act to give notice to the other party, with a copy for information to the Adjudicator incase an Adjudicator had been involved, of its intention to commence arbitration, as provided below, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

43.2.2 Any dispute in respect of which a notice of intention to commence arbitration has been given, in accordance with GCC Clause 43.2.1, shall be finally settled by arbitration. Arbitration may be commenced prior to or after Installation of the Information System.

43.2.3 Arbitration proceedings shall be conducted in accordance with the rules of procedure **specified in the SCC.**

43.3 Notwithstanding any reference to the Adjudicator or arbitration in this clause,

a) The parties shall continue to perform their respective obligations under the Contract unless they otherwise agree.

b) The Procuring Entity shall pay the Supplier any monies due the Supplier.

C2: CBK - Official

B. SPECIAL CONDITIONS OF CONTRACT

SECTION VII - SPECIAL CONDITIONS OF CONTRACT

Special Conditions of Contract

The following Special Conditions of Contract (SCC) shall supplement or amend the General Conditions of Contract(GCC). Whenever there is a conflict, the provisions of the SCC shall prevail over those in the General Conditions ofContract. For the purposes of clarity, any referenced GCC clause numbers are indicated in the left column of the SCC.

A. *Contract and Interpretation*

1. Definitions (GCC Clause1)

GCC 1.1(c)(xiv)	"**Business Continuity**" refers to Provider's documented plans and Procedures to maintain essential business functions and minimize service disruptions during and after a significant business disruption.
GCC 1.1 (b) (i)	The Procuring Entity is: **Central Bank of Kenya**
GCC 1.1 (b) (ii)	The Project Manager is **Security Service Division, Central Bank of Kenya**
GCC 1.1(d)(vii)	User Acceptance Testing" refers to the test and validation of the system by the end user or business representative confirming that the system meets the business requirements functional specifications and user needs before achieving the full operational acceptance of the system
GCC 1.1(d)(viii)	"Maintenance period" refers to the period after the end of the defect liability period
GCC 1.1 (e) (ix)	***There are no Special Conditions associated with GCC 1.1 (e) (ix).*** ***vi) "Technical Requirements" means the Technical Requirements in Section V of the tendering documents.*** ***vii) "Implementation Schedule" means the Implementation Schedule in Section V of the tendering documents.***
GCC 1.1 (e) (xii)	The Post-Warranty Services Period is ***[Please insert the number of months here]*** starting with the completionof the Warranty Period.
GCC 2.1	a) The Tender Documents for the tender shall form part of this Agreement constituting the following priority in the event of a conflict. i. Contract agreement form; ii. Tender Form; iii. Price Schedule or bill of quantities submitted by Contractor iv. Schedule of Requirements v. Technical Specifications vi. General and special Conditions of contract vii. Notification of intention to enter into a contract dated …. viii. Acceptance letter dated …. ix. Notification of award dated ……
3.5	As updated from time to time

2. Joint Venture (GCC Clause 3.9)

GCC 3.9	----------shall be the leader of the JV

4.0 Notices (GCC Clause 4)

GCC 4.3	Security Service Division, Central Bank of Kenya, Haile Selassie Avenue, P.O. Box 60000-00200 Nairobi. For Electronic Data Interchange (EDI) the Procuring Entity and Supplier will use the following standards, protocols, addresses, and procedures: ***NA***

B. Subject Matter of Contract

3. Scope of the System (GCC Clause 7)

GCC 7.1	No limitation
GCC 7.3	The Supplier's obligations under the Contract will include the following recurrent cost items, as identified in the Recurrent Cost tables in the Supplier's Tender: as per **appendix 8.** The summary list of services/deliverables are defined in **appendix 9** three years comprehensive maintenance service shall commence upon Full operational acceptance and sign off-Post Migration support shall commence upon project implementation signoff.

4. Time for Commencement and Operational Acceptance (GCC Clause 8)

GCC 8.1	The Supplier shall commence work on ----------

5. Supplier's Responsibilities (GCC Clause 9)

GCC 9.5 — In addition to the responsibilities of the supplier. He shall perform the following obligations

Gap Area	Proposed Clause Addition
Cybersecurity and Data Protection	"The Supplier shall ensure compliance with applicable data protection laws and maintain security controls aligned with recognized cybersecurity frameworks (e.g., ISO 27001). Any data breaches must be reported to the Procuring Entity within 24 hours."
Subcontractor Oversight	"The Supplier shall conduct periodic audits of its subcontractors and submit compliance reports to the Procuring Entity."
Business Continuity and Resilience	"The Supplier shall develop, test, and maintain a Business Continuity Plan (BCP to ensure continuity of services during disruptions."
Performance Monitoring and Reporting	"The Supplier shall submit monthly performance reports detailing progress, risk and mitigations. Critical delays must be escalated immediately to the Procuring Entity."
Training and Knowledge Transfer	"The Supplier shall provide comprehensive training sessions for the Procuring Entity's personnel on the operation, maintenance, and administration of the System."
Sustainable Procurement	"The Supplier shall adhere to sustainable procurement guidelines, including reporting on environmental, social, and governance (ESG) compliance quarterly."
Risk Management Responsibilities	"The Supplier shall maintain a Risk Register throughout the contract duration and update the Procuring Entity monthly on risk mitigation actions."

GCC 9.8	The referenced clause 9.8 Pursuant to paragraph 2.2e. of Appendix B to the General Conditions; is hereby amended to read; Pursuant to section 1.1 (a) vi & vii of the General Conditions to the Contract; the Supplier shall permit and shall cause Its subcontractors and sub-consultants to permit, the PPRA and/or persons appointed by the PPRA to inspect the Site and/or the accounts and records relating to the procurement process, selection and/or contract execution, and to have such accounts and records audited by auditors appointed by the PPRA if requested by the PPRA. The Supplier's and its Sub contractors' and sub-consultants' attention is drawn to Sub-Clause 6.1 which provides, inter alia, that acts intended to

	materially impede the exercise of the PPRA's inspection and audit rights constitute a prohibited practice subject to contract termination (as well as to a determination of ineligibility pursuant to the PPRA's prevailing sanctions procedures).
GCC 9.9	Conformity to sustainable procurement contractual provisions ICT to provide during tendering
GCC 9.10	Supplier Responsibility: a) Maintain a current Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) designed to ensure the continued performance of its obligations under this Agreement. b) Review and update the BCP/DRP annually or more frequently as needed. c) Test the BCP/DRP on a regular basis (at least annually) and document the test results. d) Through mutual agreement provide the Procuring Entity with a summary copy of the documented test results upon request. These results should detail the scope of the testing, any identified weaknesses, and the planned corrective actions. e) In addition (or "Furthermore"), the supplier shall participate in mutually agreed-upon Business Continuity/Disaster Recovery test exercises conducted by the Procuring Entity at least [frequency] (e.g., annually). f) Communication During Disruptions: Provider shall promptly within (8hours) notify the Procuring Entity of any material service disruption, communicate the estimated restoration timeframe, and keep the Procuring Entity updated on the recovery process. g) Service Level Credits and Compensation for Downtime Beyond SLA: In the event of a service disruption exceeding agreed-upon RTOs or RPOs due to a non-Force Majeure event, Procuring Entity shall be entitled to Service Level Credits as defined in of this Agreement.
GCC 10.12	Procuring Entity's responsibility, IT to advise during tendering

C. PAYMENT

6. Contract Price (GCC Clause 11)

GCC 11.2	Adjustments to the Contract Price shall be as follows***: "This is not applicable.***

7. Terms of Payment (GCC Clause 12)

GCC 12.1	Subject to the provisions of GCC Clause 12 (Terms of Payment), the Procuring Entity shall pay the Contract Price to the Supplier according to the categories and in the manner specified below. Only the categories Advance Payment and Complete System Integration relate to the entire Contract Price. In other payment categories, the term "total Contract Price" means the total cost of goods or services under the specific payment category. Within each such category, the Contract Implementation Schedule may trigger pro-rata payments for the portion of the total Contract Price for the category corresponding to the goods or services actually Delivered, Installed, or
	Operationally Accepted, at unit prices and in the currencies specified in the Price Schedules of the Contract Agreement. (a) Advance Payment A maximum of twenty percent (20%) of the Contract Price for supply, delivery, installation, testing and commission, exclusive of all Recurrent Costs,may be paid against receipt of a claim accompanied by the Advance Payment Security specified in GCC Clause 13.2. (b) Information Technologies, Materials, and other Goods, with the exception of CustomSoftware and Custom Materials: sixty percent (60%) of the total or pro-rata Contract Price for this category againstDelivery ten percent (10%) of the same price against Installation

	ten percent (10%) of the same price against Operational Acceptance. (c) Custom Software and Custom Materials: sixty percent (60%) of the total or pro-rata Contract Price for this category againstInstallation twenty percent (20%) of the same price against Operational Acceptance. (d) Services other than Training: eighty percent (80%) of the pro-rata Contract Price for services performed will be paidmonthly in arrears, on submission and Procuring Entity's approval of invoices: **(see appendix 8 attached)**
	(e) Training - **(see appendix 8 attached)** thirty percent (30%) of the total Contract Price for training services at the start of the full training program fifty percent (50%) of the pro-rata Contract Price for training services performed will be paid monthly in arrears, on submission and approval of appropriate invoices. (f) Complete System Integration ten percent (10%) of the entire Contract Price, exclusive of all Recurrent Costs, as final payment against Operational Acceptance of the System as an integrated whole. (g) Recurrent Costs one hundred percent (100%) of the price of the services actually delivered will be paid quarterly in arrears, on submission and Procuring Entity's approval of invoices. ***[Note:** If a separate Operational Acceptance for the System as an integrated whole is not required, increase by 10% points the final payment percentages of all other goods and services above.]*
GCC 12.3	The Procuring Entity shall pay to the Supplier interest on the delayed payments for the certified invoice at a rate of:[***insert: "3%" above the prevailing Central Bank rate per annum].***
GCC 12.4	The Supplier will invoice promptly to the procurement division for the Procuring Entity in Kenya Shilling and payment for goods and services will be made in Kenya Shilling
GCC 12.5	Not Applicable

8. Securities (GCC Clause 13)

GCC 13.2	Advance Payment allowed for up to 20 percent (20%)
GCC 13.3.1	Within twenty-one (21) days of the receipt of the Form of Acceptance from the Procuring Entity, the successful Tenderer shall furnish the Bank with a performance security of 5% of the value of the tender sum provided by a Commercial Bank operating in Kenya and supervised by the Central Bank of Kenya
GCC 13.3.4	During the Warranty Period (i.e., after Operational Acceptance of the System), the Performance Security shall be reduced to 2 Percent ***[2%]*** percent of the Contract Price, excluding any Recurrent Costs.

D. INTELLECTUAL PROPERTY

9. Copyright (GCC Clause 15)

GCC 15.1	***Provided that the intellectual property for the system or materials developed by the Procuring Entity including value engineering in the course of implementation remains with the procuring entity***
GCC 15.2	***Within 15 days***
GCC 15.3	***the Procuring Entity may assign to entities under the governance structure of the Procuring Entity***

GCC 15.4	***There are no Special Conditions of Contract applicable to GCC Clause 15.4***

GCC 15.5	***CBK shall have full rights to the system /source code of the integration flows/ APIs which will be developed by the vendor. Working and latest copy of the Source Code shall be delivered to CBK for safe custody as part of the go-live sign-off and any subsequent updates.***

10. Software License Agreements (GCC Clause 16)

GCC 16.1 (a) (iv)	***Special Conditions of Contract applicable to GCC Clause 16.1 (a) (iv)*** *Except to the extent that the Intellectual Property Rights in the Software vest in the Procuring Entity, the Supplier here by, subject to the terms, conditions and limitations issued by the manufacturer of the software, grants to the Procuring Entity license to access and use the Software, including all inventions, designs, and marks embodied in the Software.*
GCC 16.1 (b) (vi)	***There are no Special Conditions of Contract applicable to GCC Clause 16.1 (b) (vi)***
GCC 16.1 (b) (vii)	***There are no Special Conditions of Contract applicable to GCC Clause 16.1 (b) (vii)***
GCC 16.1(vii)	***may be disclosed or reproduced for use by other affiliates of the bank***
GCC 16.2	***within 14 days***

11. Confidential Information (GCC Clause 17)

GCC 17.1	***There are no Special Conditions of Contract applicable to GCC Clause 17.1***
GCC 17.7	The provisions of this GCC Clause17 shall survive the termination, for whatever reason, of the Contract.

12. Representatives (GCC Clause 18)

GCC 18.3	***Upon the decision by the Procuring Entity to remove a representative, the Supplier shall provide a replacement immediately but no longer than Fourteen (14) days***

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System

13. Project Plan (GCC Clause 19)

GCC 19.1	Chapters in the Project Plan shall address the following subject**:** ***(a) Project Organization and Management Sub-Plan, including management authorities, responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format);*** ***(b) Implementation Sub-Plan;*** ***(c) Training Sub-Plan;*** ***(d) Testing and Quality Assurance Sub-Plan;*** ***(e) Warranty Defect Repair and Technical Support Service Sub-Plan*** ***Further details regarding the required contents of each of the above chapters are contained in the Technical Requirements, (insert: reference)].***
GCC 19.5	***The Supplier shall submit to the Procuring Entity:*** ***(i) monthly inspection and quality assurance reports*** ***(ii) monthly training participants test results*** ***(iii) monthly log of service calls and problem resolutions*** ***In addition to the above-mentioned reports, the supplier should submit reports on:***

Report Name	Purpose:
1	Project Progress
2	Risk Management
3	System Performance and Uptime
4	Cybersecurity and Data Protection
5	Compliance and SLA Monitoring
6	Financial and Invoicing
7	Training and Knowledge Transfer
8	Change Management

14. Design and Engineering (GCC Clause 21)

GCC 21.3.2	***There are no Special Conditions of Contract applicable to GCC Clause 21.3.2. "none":***

15. Product Upgrades (GCC Clause 23)

GCC 23.4	***There are no Special Conditions of Contract applicable to GCC Clause 23.4.***

16. Inspections and Tests (GCC Clause 25)

GCC 25.6	***26.6.1 Rights to Audit*** ***The Procuring Entity (or its authorized representatives, including external auditors) shall have the right to audit, inspect, and review all books, records, accounts, systems, documents, and operations maintained by the Supplier, its subcontractors, and agents, that relate to the performance of the Contract.*** ***25.6.2 Scope of Audit*** ***The audit may cover the following areas:*** ***a) Compliance with the terms and conditions of the Contract.*** ***b) Financial records, including invoices, payments, expenses, and cost breakdowns.*** ***c) Operational performance, including adherence to agreed timelines, milestones, and service levels.*** ***d) Data protection, cybersecurity practices, and information security controls.*** ***e) Subcontractor and third-party compliance with contractual obligations.*** ***f) Environmental, Social, and Governance (ESG) requirements, where applicable.*** ***25.6.3 Frequency and Notice*** ***a) Audits may be conducted upon reasonable notice of at least [7 to 14 days] to the Supplier.*** ***b) The Procuring Entity may conduct audits annually or at any time in response to reasonable concerns, disputes, or regulatory obligations.*** ***c) Audits may be conducted during normal business hours unless otherwise agreed or in cases of suspected fraud or breaches of contract.*** ***25.6.4 Access to Records and Facilities*** ***The Supplier shall grant full and unrestricted access to:*** ***a) All relevant documents, systems, and financial records related to the Contract.*** ***b) Facilities, sites, or data centres used to perform obligations under the Contract.*** ***c) Subcontractor operations and records where applicable.*** ***The Supplier shall cooperate fully during the audit process and provide reasonable assistance as required.*** ***25.6.5 Audit Costs*** ***a) The cost of any routine audit shall be borne by the Procuring Entity.*** ***b) If an audit reveals material non-compliance, misrepresentation, or overbilling, the Supplier shall reimburse the Procuring Entity for:*** ***a. The full cost of the audit.*** ***b. Any overpaid amounts, along with applicable interest or penalties, as determined in the Contract.*** ***25.6.6 Retention of Records*** ***The Supplier shall:*** ***a) Retain all records, documents, and data related to the Contract for a period of [3 to 7 years] after the Contract's expiration or termination.*** ***b) Ensure that records remain accessible and legible during this retention period, including electronic records.*** ***25.6.7 Confidentiality of Audit Information*** ***a) All information obtained during the audit shall be treated as confidential and used solely for the purpose of verifying compliance with the Contract.*** ***b) The Procuring Entity and its auditors shall not disclose such information to third parties except where required by law, regulation, or court order.*** ***25.6.8 Corrective Actions*** ***a) If an audit identifies non-compliance, breaches, or deficiencies, the Supplier shall:*** ***a. Remedy the identified issues within [30 days] or an agreed timeframe.*** ***b. Implement corrective and preventive measures to avoid recurrence.*** ***b) The Procuring Entity reserves the right to impose penalties, withhold payments, or***

	terminate the Contract if non-compliance is not rectified within the agreed period. ***25.6.9 Subcontractor Audits*** ***a) The Supplier shall ensure that all subcontractors engaged in the Contract provide the Procuring Entity with equivalent audit rights as outlined in this clause.*** ***b) The Supplier remains fully responsible for ensuring subcontractor compliance.*** ***25.6.10 Regulatory Compliance Audits*** ***If required by law, regulation, or government authorities, the Procuring Entity may conduct audits to ensure compliance with:*** ***c) Applicable laws and regulations, including data protection and cybersecurity laws.*** ***d) Financial reporting standards.*** ***e) Industry best practices or certifications (e.g., ISO 27001, NIST, SOC 2 compliance).*** ***25.6.11 Human Resources Security*** ***Purpose*** ***This clause mitigates risks of insider threats, unauthorized access, and data breaches by ensuring personnel are properly vetted, trained, and monitored.*** ***25.6.12 Pre-Employment Screening*** ***The Supplier shall conduct background checks, including identity verification, employment history, and criminal records, for all personnel accessing the Procuring Entity's systems, data, or facilities. Evidence of screening shall be maintained and shared upon request.*** ***25.6.13 Confidentiality and Training*** ***a) All personnel and subcontractors shall sign Non-Disclosure Agreements (NDAs) before deployment.*** ***b) The Supplier shall provide security awareness training on data protection, cybersecurity practices, and system handling, with annual refresher sessions.*** ***25.6.14 Access Management*** ***The Supplier shall:*** ***a) Grant system or facility access based on the principle of least privilege.*** ***b) Immediately revoke access upon termination, reassignment, or project completion.*** ***c) Maintain access logs and provide them upon request.*** ***25.6.15 Termination and Asset Return*** ***Upon personnel termination or role change, the Supplier shall:*** ***a) Revoke all access rights.*** ***b) Ensure prompt return of assets, credentials, and documentation provided by the Procuring Entity.*** ***25.6.15 Subcontractors and Incident Reporting*** ***a) The Supplier shall ensure subcontractors comply with all HR security provisions.*** ***Any personnel-related security incidents must be reported immediately to the Procuring Entity, with a root cause analysis provided within 5 business***

17. Commissioning and Operational Acceptance (GCC Clause 27)

GCC 27.2.1	***. The Operational Acceptance Tests to include System Integration Test as outlined in the Technical Specification***

F. Guarantees and Liabilities

18. Operational Acceptance Time Guarantee (GCC Clause 28)

GCC 28.2	***There are no Special Conditions of Contract applicable to GCC Clause*** ***28.2.***

GCC 28.3	***There are no Special Conditions of Contract applicable to GCC Clause 28.3.***

19. Defect Liability (GCC Clause 29)

GCC 29.1	***There are no Special Conditions of Contract applicable to GCC Clause 29.1.***
GCC 29.4	***The Defect liability period shall be …….***
GCC 29.10	***There are no Special Conditions of Contract applicable to GCC Clause 29.10***

20. Functional Guarantees (GCC Clause 30)

GCC 30	***There are no Special Conditions of Contract applicable to GCC Clause 30.***
GCC 30.3	***The period for achieving operational acceptance shall defined in the agreed Service Level Agreement signed by both parties***

21. Limitation of Liability (GCC Clause 33)

GCC 33.1	

22. Care of the System (GCC Clause 35)

GCC 35.1	The Procuring Entity shall avail a secure place for the storage of the system upon delivery and shall not take responsibility until the system has been operationalized and commissioned.

G. Risk Distribution

23. Insurances (GCC Clause 37)

GCC 37.1 (c)	***Third party insurance shall include*** ***a) cyber liability insurance*** ***b) WIBA***
	The insured Parties shall be ***[list insured parties].*** The Insurance shall cover the period from ***[insert beginning date, relative to the Effective Date of the Contract]***until ***[insert: expiration date, relative to the Effective Date of the Contract or its completion]. As per tender document***
GCC 37.1 (e)	***There are no Special Conditions of Contract applicable to GCC Clause 37.1 (e).*** ***[Note: Many countries have statutory requirements for various insurances. These should be reviewed with the Procuring Entity's legal department. - As per tender document***

H. Change in Contract Elements

24. Changes to the System (GCC Clause 39)

GCC 39.4.3	**Value Engineering N/A** If the value engineering proposal is approved by the Procuring Entity the amount to be paid tothe Supplier shall be 50 % (insert appropriate percentage. The percentage is normally up to 50%) of the reduction in the Contract Price.

25. Extension of Time for achieving Operational acceptance (GCC Clause 40)

GCC 40.2	The request for extension shall be made by the supplier promptly but not more than Fourteen (14) days from the commencement of such event or circumstance. In the event the supplier does not issue a notice of extension after the 14 days, then they are deemed ineligible for an extension

26. Termination (GCC Clause 41)

GCC 41.2.1 (c	Add the following clause to 41.2.1(c)

)	If the Procuring Entity has documented evidence that the supplier has engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for or executing the Contract, the Procuring Entity shall: a) Notify the supplier in writing, providing details of the alleged malpractice and evidence supporting the claim. b) Allow the supplier 14 calendar days to respond in writing and, where feasible, rectify the alleged malpractice. If, after reviewing the supplier's response, the Procuring Entity concludes that malpractice has occurred, it may terminate the Contract by issuing a written notice specifying the effective date of termination. The supplier shall retain the right to receive payment for services satisfactorily performed up to the date of termination unless such payments are directly linked to the malpractice.
41.2.2(h)	If the supplier fails to achieve the Operational Acceptance Test within the specified period

I. Settlement of Disputes

27. Settlement of Disputes (GCC Clause 43)

41.1.1	*The Procuring Entity may at any time and upon issuance of a thirty (30) day notice terminate the Contract for any reason by giving the Supplier a notice of termination that refers to this GCC Clause 41.1.*
41.2.2	Acceptance of the System by the Time for Achieving Operational Acceptance as extended; then the Procuring Entity may, without prejudice to any other rights it may possess under the Contract, give a notice to the Supplier stating the nature of the default and requiring the Supplier to remedy the same. If the Supplier fails to remedy or to take steps to remedy the same within Twenty One (21) days of its receipt of such notice, then the Procuring Entity may terminate the Contract forthwith by giving a notice of termination to the Supplier that refers to this GCC Clause 41.2.
GCC 43.1& 43.2	***"not applicable.".***
GCC 43.4	*a. The parties shall negotiate in good faith with a view to settling any dispute or claim arising out of or relating to this Agreement and may not initiate any further proceedings until either party has, by written notice to the other, declared that such negotiations have failed.* *b. Any disputes between the parties arising out of or in connection with this Agree, which cannot be settled amicably shall proceed to the Courts of Law in Kenya. The Courts of Law in Kenya shall have exclusive jurisdiction to resolve all disputes arising herein.*

28. Data Protection (GCC Clause 44)

GCC 44	**Data Protection** a. The supplier acknowledges that this Agreement may involve the processing of personal data. The Parties shall handle such personal data in accordance with the Data Protection Act (No. 4 of 2019 Laws of Kenya) and any applicable laws, regulations, and other legal requirements relating to; i. privacy and data security; and ii. the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any personal data.

	b. The Parties shall process personal data in accordance with the Data Processing Agreement between the Parties as provided in Annex xxxxxx["Data Processing Agreement"]. c. The Parties agree to be bound by the terms of the Data Processing Agreement in connection with the processing of personal data under this Agreement. d. Without prejudice to any clauses in this Agreement, this Clause shall survive termination of this Agreement.

SECTION VIII - CONTRACT FORMS

Notes to the Procuring Entity on preparing the Contract Forms.

Performance Security: Pursuant to GCC Clause 13.3, the successful Tenderer is required to provide the Performance Security within twenty-eight (28) days of notification of Contract award.

Advance Payment Security: Pursuant to Clause13.2, the successful Tenderer is required to provide a bank guarantee securing the Advance Payment, if the SCC related to GCC Clause 12.1 provides for an Advance Payment.

Installation and Operational Acceptance Certificates: Recommended formats for these certificates are included in this SPD. Unless the Procuring Entity has good reason to require procedures that differ from those recommended, or to require different wording in the certificates, the procedures and forms shall be included unchanged. If the Procuring Entity wishes to amend the recommended procedures and/ or certificates, it may do so before release of the tendering document to potential Tenderers.

Change Order Procedures and Forms: Similar to the Installation and Operational Acceptance Certificates, the Change Estimate Proposal, Estimate Acceptance, Change Proposal, Change Order, and related Forms should be included in the tendering document unaltered. If the Procuring Entity wishes to amend the recommended procedures and/ or certificates, it may do so before release of the tendering document.

Notes to Tenderers on working with the Sample Contractual Forms

The following forms are to be completed and submitted by the successful Tenderer following notification of award: (i) Contract Agreement, with all Appendices; (ii) Performance Security; and (iii) Advance Payment Security.

Contract Agreement: In addition to specifying the parties and the Contract Price, the Contract Agreement is where the: (i) Supplier Representative; (ii) if applicable, agreed Adjudicator and his/her compensation; and (iii) the List of Approved Subcontractors are specified. In addition, modifications to the successful Tenderer's Tender Price Schedules are attached to the Agreement. These contain corrections and adjustments to the Supplier's tender prices to correct errors, adjust the Contract Price to reflect - if applicable - any extensions to tender validity beyond the last day of original tender validity plus 56 days, etc.

Performance Security: Pursuant to GCC Clause 13.3, the successful Tenderer is required to provide the Performance Security in the form contained in this section of these tendering documents and in the amount specified in accordance with the SCC.

Advance Payment Security: Pursuant to GCC Clause 13.2, the successful Tenderer is required to provide a bank guaranteeforthefullamountoftheAdvancePayment-ifanAdvancePaymentisspecifiedintheSCCforGCCClause 12.1- in the form contained in this section of these tendering documents or another form acceptable to the Procuring Entity. If a Tenderer wishes to propose a different Advance Payment Security form, it should submit a copy to the Procuring Entity promptly for review and confirmation of acceptability before the tender submission deadline.

The Procuring Entity and Supplier will use the following additional forms during Contract implementation to formalize or certify important Contract events: (i) the Installation and Operational Acceptance Certificates; and (ii) the various Change Order forms. These and the procedures for their use during performance of the Contract are included in the tendering documents for the information of Tenderers.

1. Notification of Intention to Award

[*This Notification of Intention to Award shall be sent to each Tenderer that submitted a Tender.*]
[*Send this Notification to the Tenderer's Authorized Representative named in the Tenderer Information Form*]

1) For the attention of Tenderer's Authorized Representative Name: ..... [insert Authorized Representative's name]
Address: ..... *[insert Authorized Representative's Address]*
Telephone/Fax numbers: ..... *[insert Authorized Representative's telephone/fax numbers]*
Email Address: ..... *[insert Authorized Representative's email address]*

[IMPORTANT: insert the date that this Notification is transmitted to all participating Tenderers. The Notification must be sent to all Tenderers simultaneously. This means on the same date and as close to the same time as possible.]

DATE OF TRANSMISSION: .....This Notification is sent by: [*email/fax*] on[*date*](local time)
Notification of Intention to Award
[Procuring Entity]: ..... *[insert the name of the Procuring Entity]*
Project: .....*[insert name of project]*
Contract title: ..... *[insert the name of the contract]*
Country: .....*[insert country where ITT is issued]*
ITT No: ..... *[insert ITT reference number from Procurement Plan]*

This Notification of Intention to Award (Notification) notifies you of our decision to award the above contract. The transmission of this Notification begins the Standstill Period. During the Standstill Period you may:

a) Request a debriefing inrelation to the evaluation of your Tender, and/ or

b) Submit a Procurement-related Complaint in relation to the decision to award the contract.

i) The successful Tenderer

Name:	[*insert name of successful Tenderer*]
Address:	[*insert address of the successful Tenderer*]
Contract price:	[*insert contract price of the successful Tenderer*]
Total combined score:	[*insert the total combined score of the successful Tenderer*]

2) Other Tenderers ***[INSTRUCTIONS: insert names of all Tenderers that submitted a Tender. If the Tender's price was evaluated include the evaluated price as well as the Tender price as read out.]***

Name of Tenderer	Technical Score (If applicable)	Tender price	Evaluated Tender Cost	Combined Score (if applicable)
[*insert name*]	[*insert Technical score*]	[*insert Tender price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Tender price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Tender price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Tender price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Tender price*]	[*insert evaluated cost*]	[*insert combined score*]

3) ***Reason/s why your Tender was unsuccessful [Delete if the combined score already reveals the reason]***

[INSTRUCTIONS; State the reason/s why this Tenderer's Tender was unsuccessful. Do NOT include: (a) a point by point comparison with another Tenderer's Tender or (b) information that is marked confidential by the Tenderer in its Tender.]

4) ***How to request a debriefing***

DEADLINE: The deadline to request a debriefing expires at midnight on [*insert date*] (local time).

You may request a debriefing in relation to the results of the evaluation of your Tender. If you decide to request a debriefing your written request must be made within three (3) Business Days of receipt of this Notification of Intention to Award.

Provide the contract name, reference number, name of the Tenderer, contact details; and address the request for debriefing as follows:

Attention: [*insert full name of person, if applicable*] **Title/position**:___[*insert title/position*]

Agency: [*insert name of Procuring Entity*] **Email address**:_____[*insert email address*] **Fax**

number:_____[*insert fax number*] ***delete if not used***

If your request for a debriefing is received within the 3 Business Days deadline, we will provide the debriefing within five (5) Business Days of receipt of your request. If we are unable to provide the debriefing within this period, the Standstill Period shall be extended by five (5) Business Days after the date that the debriefing is provided. If this happens, we will notify you and confirm the date that the extended Standstill Period will end.

The debriefing may be in writing, by phone, video conference call or in person. We shall promptly advise you in writing how the debriefing will take place and confirm the date and time.
If the deadline to request a debriefing has expired, you may still request a debriefing. In this case, we will provide the debriefing as soon as practicable, and normally no later than fifteen (15) Business Days from the date of publication of the Contract Award Notice.

5) How to make a complaint

DEADLINE: The deadline for submitting a Procurement-related Complaint challenging the decision to award the contract expires on midnight, [*insert date*] (local time).

Provide the contract name, reference number, name of the Tenderer, contact details; and address the Procurement-related Complaint as follows:

Attention: [*insert full name of person, if applicable*] **Title/position**:___[*insert title/position*]

Agency: [*insert name of Procuring Entity*] **Email address**:_____[*insert email address*]

At this point in the procurement process, you may submit a Procurement-related Complaint challenging the decision to award the contract. You do not need to have requested, or received, a debriefing before making this complaint. Your complaint must be submitted within the Standstill Period and received by us before the Standstill Period ends. Further information:

For more information refer to the Public Procurement and Disposals Act 2015 and its Regulations available from the Website info@ppra.go.ke or complaints@ppra.go.ke.

In summary, there are four essential requirements:

1. You must be an' interested party'. In this case, that means a Tenderer who submitted a Tender in this procurement and is the recipient of a Notification of Intention to Award.
2. The complaint can only challenge the decision to award the contract.
3. You must submit the complaint within the deadline stated above.
4. You must include, in your complaint, all of the information required by the Procurement Regulations (as described in Annex III).

6) Standstill Period

DEADLINE: The Standstill Period is due to end at midnight on [*insert date*] (local time).

The Standstill Period lasts ten (10) Business Days after the date of transmission of this Notification of Intention to Award.

The Standstill Period may be extended. This may happen where we are unable to provide a debriefing within the five (5) Business Day deadline. If this happens, we will notify you of the extension.

If you have any questions regarding this Notification please do not hesitate to contact us. On behalf of the Procuring Entity:

Signature: _____

Name: _____

Title/position:

_____

Telephone: _____

Email: _____

2. REQUEST FOR REVIEW

FORM FOR REVIEW(r.203(1))

PUBLIC PROCUREMENT ADMINISTRATIVE REVIEW BOARD

APPLICATION NO…….OF…….20……...

BETWEEN

……...…….APPLICANT

AND

……RESPONDENT (Procuring Entity)

Request for review of the decision of the…… (Name of the Procuring Entity of ……dated the…day of …….20…….in the matter of Tender No……..…of ……..20….. for .....(Tender description).

REQUEST FOR REVIEW

I/We……,the above named Applicant(s), of address: Physical address…….P. O. Box No……. Tel. No……..Email ……, hereby request the Public Procurement Administrative Review Board to review the whole/part of the above mentioned decision on the following grounds , namely:

1.

2.

By this memorandum, the Applicant requests the Board for an order/orders that:

1.

2.

SIGNED …….(Applicant) Dated on…….day of ……/…20……

FOR OFFICIAL USE ONLY Lodged with the Secretary Public Procurement Administrative Review Board on……day of ……....20….……

SIGNED

Board Secretary

3. Letter of Award

_____)_____

To: _____

This is to notify you that your Tender dated_____for execution of the_____ for the Contract Price in the aggregate of_____, as corrected and modified in accordance with the Instructions to Tenderers is here by accepted by our Agency.

You are requested to furnish the Performance Security within 28 days in accordance with the Conditions of Contract, using for that purpose one of the Performance Security Form*s* included in Section X, - Contract Forms, of the Tendering Document.

Authorized Signature:_____

Name and Title of Signatory:_____

Name of Agency:_____

Attachment: Contract Agreement

4. Contract Agreement

THE CENTRAL BANK OF KENYA established under Article 231 of the Constitution of Kenya 2010 and of Post Office Box Number 60000 – 00200, Nairobi, situate, Haile Selassie Avenue Nairobi (hereinafter referred to as the "Procuring Entity") which expression shall where the context so admits include its successors in title and permitted assigns) on the one part;

-AND-

The Supplier……

WHEREAS the Procuring Entity desires to engage the Supplier to supply, install, achieve Operational Acceptance of, and support the following Information System XXXXX ("the Systems"), and the Supplier (JV) has agreed to such engagement upon and subject to the terms and conditions appearing below in this Contract Agreement.

NOW IT IS HERE BY AGREED as follows:

1.0 Article 1. Contract Documents

Contract Documents (Reference GCC Clause1.1(a) (ii))

The following documents shall constitute the Contract between the Procuring Entity and the Supplier, and each shall be read and construed as an integral part of the Contract:

a) This Contract Agreement and the Appendices attached to the Contract Agreement

b) Special Conditions of Contract

c) General Conditions of Contract

d) Technical Requirements (including Implementation Schedule)

e) The Supplier's tender and original Price Schedules

f) Scope of Works document detailing the work to be done and deliverables

g) Joint Venture Agreement

1**.2 Order of Precedence (Reference GCC Clause 2)**

In the event of any ambiguity or conflict between the Contract Documents listed above, the order of precedence shall be the order in which the Contract Documents are listed in Article 1.1 (Contract Documents) above, if Appendix 7 shall prevail over all provisions of the Contract Agreement and the other Appendices attached to the Contract Agreement and all the other Contract Documents listed in Article 1.1 above.

1.3 Definitions (Reference GCC Clause1)

Capitalized words and phrases used in this Contract Agreement shall have the same meanings as prescribed to them in the General Conditions of Contract.

2.0 Article 2. Contract Price and Terms of Payment

2.1 Contract Price (Reference GCC Clause 1.1(a) (viii) and GCC Clause 11) The Procuring Entity here by agrees to pay to the Supplier the Contract Price in consideration of the performance by the Supplier of its obligations under the Contract. The Contract Price shall be the aggregate shown below and more particularly as specified in the Grand Summary Price Schedule.

1. Provision of XXXXX at a total cost of Kenya Shillings Kes. AMOUNT. The breakdown of the cost and services is as per appendix 7 and schedule 2

The Contract Price shall be understood to reflect the terms and conditions used in the specification of prices in the detailed price schedules, including the terms and conditions of the associated incoterms, and the taxes, duties and related levies if and as identified.

3.0 Article 3. Effective Date for Determining Time for Operational Acceptance

3.1 Effective Date (Reference GCC Clause 1.1(e) (ix))

The time allowed for supply, installation, and achieving Operational Acceptance of the System shall be determined from the date when all of the following conditions have been fulfilled:

a) This Contract Agreement has been duly executed for and on behalf of the Procuring Entity and the Supplier.

b) The Supplier has submitted to the Procuring Entity the performance security and the advance payment security, in accordance with GCC Clause 13.2 and GCC Clause13.3.

c) The Procuring Entity has paid the Supplier the advance payment, in accordance with GCC Clause 12; Each party shall use its best efforts to fulfill the above conditions for which it is responsible as soon as practicable.

3.2 If the conditions listed under 3.1 are not fulfilled within two (2) months from the date of this Contract Agreement because of reasons not attributable to the Supplier, the parties shall discuss and agree on an equitable adjustment to the Contract Price and the Time for Achieving Operational Acceptance and/or other relevant conditions of the Contract.

4.0 Article4. Appendixes.

4.1 The Appendixes listed below shall be deemed to form an integral part of this Contract Agreement.

4.2 Reference in the Contract to any Appendix shall mean the Appendixes listed below and attached to this Contract Agreement, and the Contract shall be read and construed accordingly.

IN WITNESS WHERE OF, the Parties here to have caused this Contract to be signed in their respective names as of the day and year first above written.

For and on behalf of **CENTRAL BANK OF KENYA** *[Authorized Representative]*

_____ _____

Name: Designation

_____ _____

Signature Date

Witnessed By:

_____ _____

Name Designation

_____

Signature

For and on behalf of **SUPPLIER** *[Authorized Representative]*

_____ _____

Name: Designation

_____

Signature

Witnessed By:

_____ _____

Name Designation

_____

Signature

5. Appendices

a) Appendix 1. Supplier's Representative

In accordance with GCC Clause 1.1 (b) (iv), the Supplier's Representative is:

Name: .....*[insert: name and provide title and address further below, or state "to be nominated within fourteen (14) days of the Effective Date"]*

Title: .....*[if appropriate, insert: title]*

In accordance with GCC Clause 4.3, the Supplier's addresses for notices under the Contract are:

Address of the Supplier's Representative: .....[***as appropriate, insert: personal delivery, postal, cable, facsimile, electronic mail, and/or EDI addresses.]***

Fallback address of the Supplier: .....[***as appropriate, insert: personal delivery, postal, cable, facsimile, electronic mail, and/or EDI addresses.]***

b) Appendix 2. Adjudicator (Not Applicable)

c) Appendix 3. List of Approved Subcontractors – Not Applicable

d) Appendix 9: Deliverables/Services

e) Appendix 10: Service Level Agreement

Service Level Agreement (SLA)

1. **Online Issue Logging System**
   The supplier shall provide an online support mechanism, preferably a web portal where the Procuring Entity shall log all issues. The online system shall provide tracking and dashboard capabilities including:
   - Date and time of issue logging
   - Issue Description
   - Attachments capability
   - Issue priority
   - User reports – aging analysis, issue categorization
   - Integrations and email notifications- any updates on the ticket should be viewable online and email notifications should be generated upon update
   - User account creation and profiles
   - The procuring entity should have the capability to mark issues as closed; the supplier should never close any logged ticket

   The supplier to also provide a corporate support email address with ability to receive large content

2. **Issue Categorization and Prioritization**
   The priority assigned to an issue by the Procuring entity shall not be changed; however, in exceptional circumstances, the two parties might review and downgrade/re-prioritize the issue

   Reported faults will be prioritized into three categories:-

Priority 1	Critical faults requiring an immediate response
Priority 2	Faults requiring an urgent, though not necessarily an immediate response
Priority 3	Other faults

3. **Issue Resolution time Targets**
   he targets for resolving faults reported are as follows: -

Priority	**Response**	**Resolution (Temporary solution)**	**Target for Correction of fault**
1	Immediate	1 hours	Within the business day
2	Within 1 working day	3 hours	By the next day
3	Within 2 – 5 days	By agreement	By agreement

4. **Help Desk Service and 24/7 On-Call Services Requirements**

The supplier shall provide support on 24/7/365 hour basis and maintain local support office at all times during the duration of the contract

The supplier shall maintain a Help Desk facility. The Help Desk facility shall be staffed with qualified personnel who will take problem reports, answer technical questions and attempt to resolve problems and non-conformities over the telephone. Help Desk problem resolution time limits and penalty amounts are like that of

'On-Call Service Requirements' and are given in the below tables.

The Help Desk should initiate remote problem diagnostic routines and attempt to correct the problems or guide. The procuring entity's personnel through problem resolution.

5. **System Upgrade & Documentation**

The supplier shall ensure it provides the Procuring Entity with Regular Solution software updates & an up-to-date system documentation(s) as will relate to system functionality operations as specified in the contract.

6. **Security Vulnerabilities and Patches**

The supplier shall provide the necessary fixes to ensure the continued working of the provided solution if any security and product fixes/patches released to address security and product vulnerabilities. These shall also be logged as priority 1 issues

C. FORMS

SECTION VIII -CONTRACT FORMS

FORM NO. 1 - PERFORMANCE SECURITY – (Unconditional Demand Bank Guarantee)

[Guarantor letterhead or SWIFT identifier code]

Beneficiary:_____*[insert name and Address of* Procuring Entity*]*

Date:_____*[Insert date of issue]*

PERFORMANCE GUARANTEE No.:_____

Guarantor:..... *[Insert name and address of place of issue, unless indicated in the letterhead]*

1. We have been informed that_____(hereinafter called "the Applicant") has entered into Contract No._____*dated*_____with the Beneficiary, for the execution of_____ (herein after called "the Contract").

2. Furthermore, we understand that, according to the conditions of the Contract, a performance guarantee is required.

3. At the request of the Applicant, we as Guarantor, hereby irrevocably under take to pay the Beneficiary any sum or sums not exceeding in total an amount of_____(),[1] such sum being payable in the types and proportions ofcurrenciesinwhichtheContractPriceispayable,uponreceiptbyusoftheBeneficiary'scomplyingdemand supported by the Beneficiary's statement, whether in the demand itself or in a separate signed document accompanying or identifying the demand, stating that the Applicant is in breach of its obligation(s) under the Contract, without the Beneficiary needing to prove or to show grounds for your demand or the sum specified therein.

4. This guarantee shall expire, no later than the….Day of……, 2…[2], and any demand for payment under it must be received by us at this office indicated above on or before that date.

5. The Guarantor agrees to a one-time extension of this guarantee for a period not to exceed *[six months] [one year],* in response to the Beneficiary's written request for such extension, such request to be presented to the Guarantor before the expiry of the guarantee."_____

_____

[Name of Authorized Official, signature(s) and seals/stamps]

Note: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.

_____

[1] *The Guarantor shall insert an amount representing the percentage of the Accepted Contract Amount specified in the Letter o Acceptance, less provisional sums, if any, and denominated either in the currency(ies) of the Contract or a freely convertible currency acceptable to the Beneficiary.*

[2] *Insert the date twenty-eight days after the expected completion date as described in GC Clause 11.9. The Procuring Entity should note that in the event of an extension of this date for completion of the Contract, the Procuring Entity would need to request an extension of this guarantee from the Guarantor. Such request must be in writing and must be made prior to the expiration date established in the guarantee. In preparing this guarantee, the Procuring Entity might consider adding the following text to the form, at the end of the pen ultimate paragraph: "The Guarantor agrees to a one-time extension of this guarantee for a period not to exceed [six months] [one year], in response to the Beneficiary's written request for such extension, such request to be presented to the Guarantor before the expiry of the guarantee."*

FORM No. 2 - PERFORMANCE SECURITY OPTION 2 – (Performance Bond) NOT APPLICABLE

[Note: Procuring Entities are advised to use Performance Security–Unconditional Demand Bank Guarantee instead of Performance Bond due to difficulties involved in calling Bond holder to action]
[Guarantor letterhead or SWIFT identifier code] **Beneficiary:**
[insert name and Address of Procuring Entity*]* **Date:**
_____*[Insert date of issue]*

PERFORMANCE BOND No.:_____

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*

1. By this Bond_____ as Principal (hereinafter called "the Contractor") and _____] as Surety (herein after called "the Surety"), are held and firmly bound unto_____] as Obligee (herein after called "the Procuring Entity")in the amount of _____for the payment of which sum well and truly to be made in the types and proportions of currencies in which the Contract Price is payable, the Contractor and the Surety bind themselves, their heirs, executors, administrators, successors and assigns, jointly and severally, firmly by these presents.

2. WHEREAS the Contractor has entered into a written Agreement with the Procuring Entity dated the_____ day of _____, 20_____, for_____in accordance with the documents, plans, specifications, and amendments thereto, which to the extent herein provided for, are by reference made part hereof and are herein after referred to as the Contract.

3. NOW, THEREFORE, the Condition of this Obligation is such that, if the Contractor shall promptly and faithfully perform the said Contract (including any amendments thereto), then this obligation shall be null and void; otherwise, it shall remain in full force and effect. Whenever the Contractor shall be, and declared by the Procuring Entity to be, in default under the Contract, the Procuring Entity having performed the Procuring Entity's obligations there under, the Surety may promptly remedy the default, or shall promptly:

    1) Complete the Contract in accordance with its terms and conditions; or
    2) Obtain a tender or tenders from qualified tenderers for submission to the Procuring Entity for completing the Contract in accordance with its terms and conditions, and upon determination by the Procuring Entity and the Surety of the lowest responsive Tenderers, arrange for a Contract between such Tenderer, and Procuring Entity and make available as work progresses (even though there should be a default or a succession of defaults under the Contract or Contracts of completion arranged under this paragraph) sufficient funds to pay the cost of completion less the Balance of the Contract Price; but not exceeding, including other costs and damages for which the Surety may be liable here under, the amount set forth in the first paragraph hereof. The term "Balance of the Contract Price," as used in this paragraph, shall mean the total amount payable by Procuring Entity to Contractor under the Contract, less the amount properly paid by Procuring Entity to Contractor; or
    3) pay the Procuring Entity the amount required by Procuring Entity to complete the Contract in accordance with its terms and conditions up to a total not exceeding the amount of this Bond.

4. The Surety shall not be liable for a greater sum than the specified penalty of this Bond.

5. Any suit under this Bond must be instituted before the expiration of one year from the date of the issuing of the Taking-Over Certificate. No right of action shall accrue on this Bond to or for the use of any person or corporation other than the Procuring Entity named herein or the heirs, executors, administrators, successors, and assigns of the Procuring Entity.

6. In testimony whereof, the Contractor has hereunto set his hand and affixed his seal, and the Surety has caused these presents to be sealed with his corporate seal duly attested by the signature of his legal representative, this day___of _____20_____.SIGNED ON_____ behalf of by___in the capacity of In the presence of

    SIGNED ON behalf of By_____in the capacity of In the

    presence of

FORM NO. 3 - ADVANCE PAYMENT SECURITY [Demand Bank Guarantee]

[Guarantor letter head or SWIFT identifier code] [Guarantor letter head or SWIFT identifier code]

Beneficiary: _____*[Insert name and Address of* Procuring Entity*]*

Date:_____*[Insert date of issue]*

ADVANCE PAYMENTGUARANTEE No.:_____*[Insert guarantee reference number]*
Guarantor:*[Insert name and address of place of issue, unless indicated in the letterhead]*

1. We have been informed that_____(hereinafter called "the Applicant") has entered into Contract No._*dated* _with the Beneficiary, for the execution of (herein after called "the Contract").

2. Furthermore, we understand that, according to the conditions of the Contract, an advance payment in the sum is to be made against an advance payment guarantee.

3. At the request of the Applicant, we as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of_____()[1] upon receipt by us of the Beneficiary's complying demand supported by the Beneficiary's statement, whether in the demand itself or in a separate signed document ac companying or identifying the demand, stating either that the Applicant:

a. Has used the advance payment for purposes other than the costs of mobilization in respect of the Works; or

b. has failed to repay the advance payment in accordance with the Contract conditions, specifying the amount which the Applicant has failed to repay.

4. A demand under this guarantee may be presented as from the presentation to the Guarantor of a certificate from the Beneficiary's bank stating that the advance payment referred to above has been credited to the Applicant on its account number _at_____

5. The maximum amount of this guarantee shall be progressively reduced by the amount of the advance payment repaid by the Applicant as specified in copies of interim statements or payment certificates which shall be presented to us. This guarantee shall expire, at the latest, upon our receipt of a copy of the interim payment certificate indicating that ninety (90)percent of the Accepted Contract Amount, less provisional sums, has been certified for payment, or on the day of , 2,[2] whichever is earlier. Consequently, any demand for payment under this guarantee must be received by us at this office on or before that date.

6. The Guarantor agrees to a one-time extension of this guarantee for a period not to exceed *[six months] [one year],* in response to the Beneficiary' s written request for such extension, such request to be presented to the Guarantor before the expiry of the guarantee.

.....

[Name of Authorized Official, signature(s) and seals/stamps]

[1]*The Guarantor shall insert an amount representing the amount of the advance payment and denominated either in the currency(ies) of the advance payment as specified in the Contract, or in a freely convertible currency acceptable to the Procuring Entity.*

[2]*Insert the expected expiration date of the Time for Completion. The Procuring Entity should note that in the event of an extension of the time for completion of the Contract, the Procuring Entity would need to request an extension of this guarantee from the Guarantor. Such request must be in writing and must be made prior to the expiration date established in the guarantee. In preparing this guarantee, the Procuring Entity might consider adding the following ext. to the form, at the end of the penultimate paragraph: "The Guarantor agrees to a one-time extension of this guarantee for a period not to exceed [six months] [one year], in response to the Beneficiary's written request for such extension, such request to be presented to the Guarantor before the expiry of the guarantee."*

1. Installation and Acceptance Certificates *(insert format)*

Installation Certificate

Date:..... ***[insert: date]***

ITT ..... ***[insert title and number of ITT]***

Contract ..... ***[insert name and number of Contract]***

To:..... ***[insert: name and address of Supplier]***

Dear Sir or Madam:

Pursuant to GCC Clause 26 (Installation of the System) of the Contract entered into between yourselves and the..... ***[insert: name of Procuring Entity]*** (hereinafter the "Procuring Entity") dated..... ***[insert: date of Contract],*** relating to the..... ***[insert brief description of the Information System],*** we hereby notify you that the System (or a Subsystem or major component thereof) was deemed to have been correctly installed on the date specified below.

1. Description of the System (or relevant Subsystem or major component..... ***[insert description]***

2. Date of Installation ..... ***[insert date]***

Notwithstanding the above, you are required to complete the outstanding items listed in the attachment to this certificate as soon as practicable. This Form shall not relieve you of your obligation to achieve Operational Acceptance of the System in accordance with the Contract nor of your obligations during the Warranty Period.

For and on behalf of the Procuring Entity

Signed: .....

Date: .....

in the capacity of:..... [***state: "Project Manager" or state the title of a higher-level authority in the Procuring Entity's organization]***

1.1 Operational Acceptance Certificate

Date: ..... *[insert date]*

ITT ..... *[insert title and number of ITT]*

Contract .....*[insert name of System or Subsystem and number of Contract]*

To:..... *[insert: name and address of Supplier]*

Dear Sir or Madam:

Pursuant to GCC Clause 27 (Commissioning and Operational Acceptance) of the Contract entered into between yourselves and the.....***[insert: name of Procuring Entity]*** (hereinafter the "Procuring Entity") dated..... ***[insert: date of Contract],*** relating to the.....***[insert brief description of the Information System],*** we hereby notify you the System (or the Subsystem or major component identified below) successfully completed the Operational Acceptance Tests specified in the Contract. In accordance with the terms of the Contract, the Procuring Entity here by takes over the System (or the Subsystem or major component identified below), together with the responsibility for care and custody and the risk of loss thereof on the date mentioned below.

1. Description of the System (or Subsystem or major component).....[***insert description]***

2. Date of Operational Acceptance .....[***insert date]***

This Form shall not relieve you of your remaining performance obligations under the Contract nor of your obligations during the Warranty Period.

For and on behalf of the Procuring Entity

Signed: .....

Date: .....

in the capacity of:..... ***[state: "Project Manager" or higher-level authority in the Procuring Entity's organization]***

7. Change Order Procedures and Forms

Date:..... *[insert date]*

ITT ..... *[insert title and number of ITT]*

Contract .....*[insert name or System or Subsystem and number of Contract]*

General

This section provides samples of procedures and forms for carrying out changes to the System during the performance of the Contract in accordance with GCC Clause 39 (Changes to the System) of the Contract.

Change Order Log

The Supplier shall keep an up-to-date Change Order Log to show the current status of Requests for Change and Change Orders authorized or pending. Changes shall be entered regularly in the Change Order Log to ensure that the log is kept up to date. The Supplier shall attach a copy of the current Change Order Log in the monthly progress report to be submitted to the Procuring Entity.

References to Changes

1) Request for Change Proposals (including Application for Change Proposals) shall be serially numbered CR-nnn.
2) Change Estimate Proposals shall be numbered CN-nnn.
3) Estimate Acceptances shall be numbered CA-nnn.
4) Change Proposals shall be numbered CP-nnn.
5) Change Orders shall be numbered CO-nnn. On all forms, the numbering shall be determined by the original CR-nnn.

Annexes

7.1 Request for Change Proposal Form

7.2 Change Estimate Proposal Form

7.3 Estimate Acceptance Form

7.4 Change Proposal Form

7.5 Change Order Form

7.6 Application for Change Proposal Form

7.1 Request for Change Proposal Form

(Procuring Entity's Form head)

Date: ..... *[insert date]*
ITT ..... *[insert title and number of ITT]*
Contract ..... *[insert name of System or Subsystem or number of Contract]*
To:..... *[insert: name of Supplier and address]*
Attention: ..... *[insert name and title]*

Dear Sir or Madam:

With reference to the above-referenced Contract, you are requested to prepare and submit a Change Proposal for the Change noted below in accordance with the following instructions within ***[insert number]*** days of the date of this Form.

1. Title of Change: [***insert title]***
2. Request for Change No./Rev.: [***insert number]***
3. Originator of Change: ***[select Procuring Entity / Supplier (by Application for Change Proposal), and add name of originator]***
4. Brief Description of Change: ***[insert description]***
5. System (or Subsystem or major component affected by requested Change): [***insert description]***
6. Technical documents and/ or drawings for the request of

   Change: Document or Drawing No. Description
7. Detailed conditions or special requirements of the requested Change: [***insert description]***
8. Procedures to be followed:
   a) Your Change Proposal will have to show what effect the requested Change will have on the Contract Price.
   b) Your Change Proposal shall explain the time it will take to complete the requested Change and the impact, if any, it will have on the date when Operational Acceptance of the entire System agreed in the Contract.
   c) If you believe implementation of the requested Change will have a negative impact on the quality, operability, or integrity of the System, please provide a detailed explanation, including other approaches that might achieve the same impact as the requested Change.
   d) You should also indicate what impact the Change will have on the number and mix of staff needed by the Supplier to perform the Contract.
   e) You shall not proceed with the execution of work related to the requested Change until we have accepted and confirmed the impact it will have on the Contract Price and the Implementation Schedule in writing.
9. As next step, please respond using the Change Estimate Proposal form, indicating how much it will cost you to prepare a concrete Change Proposal that will describe the proposed approach for implementing the Change, all it's elements, and will also address the points in paragraph 8 above pursuant to GCC Clause 39.2.1. Your Change Estimate Proposal should contain a first approximation of the proposed approach, and implications for schedule and cost, of the Change.

For and on behalf of the Procuring Entity

Signed: .....

Date: .....

in the capacity of:.....[***state: "Project Manager" or higher-level authority in the Procuring Entity's organization]***

7.2 Change Estimate Proposal Form
(Supplier's Form head)

Date: .....*[insert date]*

ITT.....*[insert title and number of ITT]*

Contract .....*[insert name of System or Subsystem and number of Contract]*

To: ..... *[insert: name of Procuring Entity and address]*

Attention: ..... *[insert: name and title]*

Dear Sir or Madam:

With reference to your Request for Change Proposal, we are pleased to notify you of the approximate cost of preparing the below-referenced Change in accordance with GCC Clause 39.2.1 of the Contract. We acknowledge that your agreement to the cost of preparing the Change Proposal, in accordance with GCC Clause 39.2.2, is required before we proceed to prepare the actual Change Proposal including a detailed estimate of the cost of implementing the Change itself.

1. Title of Change:.....*[insert: title]*

2. Request for Change No./Rev.:.....*[insert: number]*

3. Brief Description of Change (including proposed implementation approach) ..... *[insert description]*

4. Schedule Impact of Change (initial estimate)..... *[insert description]*

5. Initial Cost Estimate for Implementing the Change: .....*[insert initial cost estimate]*

6. Cost for Preparation of Change Proposal .....*[insert cost in the currencies of the Contract],* as detailed below in the breakdown of prices, rates, and quantities.

For and on behalf of the Supplier Signed:

.....

Date: .....

in the capacity of: .....*[state: "Supplier's Representative" or other higher-level authority in the Supplier's organization]*

7.3 Estimate Acceptance Form

(Procuring Entity's Form head) Date ..... *[insert date]*

ITT ..... *[insert title and number of ITT]*

Contract ..... *[insert name of System or Subsystem and number of Contract]*

To:..... *[insert: name of Supplier and address]*

Attention: ..... *[insert: name and title]*

Dear Sir or Madam:

We hereby accept your Change Estimate and agree that you should proceed with the preparation of a formal Change Proposal.

1. Title of Change: *[insert title]*

2. Request for Change No./ Rev.: *[insert request number /revision]*

3. Change Estimate Proposal No./ Rev.: *[insert proposal number/ revision]*

4. Estimate Acceptance No./ Rev.: *[insert estimate number/ revision]*

5. Brief Description of Change: *[insert description]*

6. Other Terms and Conditions:

In the event that we decide not to order the Change referenced above, you shall be entitled to compensation for the cost of preparing the Change Proposal up to the amount estimated for this purpose in the Change Estimate Proposal, in accordance with GCC Clause 39 of the General Conditions of Contract.

For and on behalf of the Procuring Entity

Signed: .....

Date: .....

in the capacity of: ..... *[state: "Project Manager" or higher-level authority in the Procuring Entity's organization]*

7.4 Change Proposal Form

(Supplier's Form head)

Date: .....*[insert date]*
ITT..... *[insert title and number of ITT]*
Contract .....*[insert name of System or Subsystem and number of Contract]*

To: ..... *[insert: name of Procuring Entity and address]*

Attention:..... ***[insert name and title]***

Dear Sir or Madam:

In response to your Request for Change Proposal No. *[insert number],* we here by submit our proposal as follows:

1. Title of Change: *[insert name]*

2. Change Proposal No./ Rev.: *[insert proposal number /revision]*

3. Origin at or of Change: *[select: Procuring Entity /Supplier; and add name]*

4. Brief Description of Change: *[insert description]*

5. Reasons for Change: *[insert reason]*

6. The System Subsystem, major component, or equipment that will be affected by the requested Change: *[insert description]*

7. Technical documents and/ or drawings for the requested Change: Document or Drawing No. Description

8. Estimate of the increase/ decrease to the Contract Price resulting from the proposed Change: *[insert amount in currencies of Contract],* as detailed below in the breakdown of prices, rates, and quantities. Total lump sum cost of the Change:

   Cost to prepare this Change Proposal (i. e., the amount payable if the Change is not accepted, limited as provided by GCC Clause 39.2.6):

9. Additional Time for Achieving Operational Acceptance required due to the Change: *[insert amount in days/ weeks]*

10. Effect on the Functional Guarantees: *[insert description]*

11. Effect on the other terms and conditions of the Contract: ***[insert description]***

12. Validity of this Proposal: for a period of .....*[insert number]* days after receipt of this Proposal by the Procuring Entity

13. Procedures to be followed:
    a) You are requested to notify us of your acceptance, comments, or rejection of this detailed Change Proposal within. ....*[insert number]* days from your receipt of this Proposal.
    b) The amount of any increase and / or decrease shall be taken into account in the adjustment of the Contract Price.

For and on behalf of the Supplier

Signed: .....

Date: .....

in the capacity of: …… *[state: "Supplier's Representative" or other higher-level authority in the Supplier's organization]*

7.5 Change Order Form

(Procuring Entity's Form head)

Date: ..... ***[insert date]***

ITT ..... ***[insert title and number of ITT]***

Contract .....***[insert name of System or Subsystem and number of Contract]***

To:..... ***[insert: name of Supplier and address]***

Attention: ..... ***[insert name and title]***

Dear Sir or Madam:

We hereby approve the Change Order for the work specified in Change Proposal No. ***[insert number***], and agree to adjust the Contract Price, Time for Completion, and/ or other conditions of the Contract in accordance with GCC Clause 39 of the Contract.

1. Title of Change: [***insert name]***

2. Request for Change No./ Rev.: [***insert request number/ revision]***

3. Change Order No./ Rev.: [***insert order number/ revision]***

4. Origin at or of Change: [***select: Procuring Entity / Supplier; and add name]***

5. Authorized Price for the Change: Ref. No.: ***[insert number]*** Date: ***[insert date]***

[insert: amount in foreign currency A] plus ***[insert amount in foreign currency B]*** plus ***[insert amount in foreign currency C]*** plus ***[insert amount in local currency]***

6. Adjustment of Time for Achieving Operational Acceptance: ***[insert amount and description of adjustment]***

7. Other effects, if any: ***[state: "none" or insert description]***

For and on behalf of the Procuring Entity

Signed: .....

Date: .....

in the capacity of: .....***[state: "Project Manager" or higher-level authority in the Procuring Entity's organization]***

For and on behalf of the Supplier

Signed: .....

Date: .....

in the capacity of.....[***state "Supplier's Representative" or higher-level authority in the Supplier's organization]***

7.6 Application for Change Proposal Form

(Supplier's Form head)

Date:..... *[insert date]*

ITT .....*[insert title and number of ITT]*

Contract..... *[insert name of System or Subsystem and number of Contract]*

To:..... *[insert: name of Procuring Entity and address]*

Attention: .....*[insert name and title]*

Dear Sir or Madam:

We hereby propose that the below-mentioned work be

treated as a Change to theSystem.

1. Title of Change: .....*[insert name]*

2. Application for Change Proposal No./ Rev.: .....*[insert number/ revision]* dated: [*insert date]*

3. Brief Description of Change: ..... *[insert description]*

4. Reasons for Change: .....*[insert description]*

5. Order of Magnitude Estimation .....*[insert amount in currencies of the Contract]*

6. Schedule Impact of Change .....*[insert description]*

7. Effect on Functional Guarantees, if any: .....*[insert description]*

8. Appendix..... *[insert titles (if any); otherwise, state "none"]*

For and on behalf of the Supplier

Signed: .....

Date: .....

in the capacity of:..... *[state: "Supplier's Representative" or higher-level authority in the*
Supplier's organization

C2: CBK - Official

1. SERVICES

Services	Deliverables/Outputs
Solution Technical Design/Architecture	Design/architecture proposals based on reference or industry architectures for review and acceptance and sign off
OEM Services	Bidder MUST include technical expertise/consultancy service of the Original Equipment Manufacturers (OEM) from the onset of deployment to signoff (design workshops, installation/deployment, execution and signoff).
Implementation (Installation + Configuration + Feature Enablement) Services	The contractor Full deployment and activation of the required and standard the Products and components/Features and security controls for all instances in each of the 2 sites. The contractor is required to set up two (2) distinct RPD environments
Integrations Set Up and Implementation	The contractor shall implement the required integrations viz- - AD Integrations - Integrations with Enterprise soutions for Monitoring, security, offline backup, emails, sms etc
Security Requirements/Controls Compliance	The Contractor shall apply required security patches/fixes to comply with Organizational hardening and compliance requirements
Migration Scope	The contract to Migrate the applications from the C@C Environment to the set up On-Prem Environments - The high level details are: o About 200 OACs reports o About 20 ODI load plans comprising different scenarios o Conversion of about 100 OIC Restful API Integrations to run on SOA o About 3 Datawarehouse databases and related schemas
Documentation	The contractor shall provide documentation as part of deliverable i.e. Low level and High Level designs, Standard

C2: CBK - Official

	Operating Procedures (SOP), Installation & Technical Configuration Documents, Project design/plan, User acceptance test plan etc
Post implementation Support	During the post implementation period, the contractor shall Support activities such as patching, upgrades, respond and fix incidents,
Warranty Period Support	The contractor to support the environment for 12 months after successful deployment and sign off
Service Levels (SLAs)	Delightful and satisfactory service levels. The SLA Terms are as follows *(refer to the table below)*

Service Levels, Rankings, and Priority **Severity Level**	**Description**	**Target Response**
1. Outage	services down	Immediate
2. Critical	High risk of application downtime	Within 10 minutes
3. Urgent	End-user impact initiated	Within 20 minutes
4. Important	Potential for performance impact if not addressed	Within 30 minutes
5. Monitor	Issue addressed but potentially impactful in the future	Within one business day
6.Informational	Inquiry for information	Within 48 hours

FORM NO. 4 BENEFICIAL OWNERSHIP DISCLOSURE FORM

INSTRUCTIONS TO TENDERERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE FORM

This Beneficial Ownership Disclosure Form ("Form") is to be completed by the successful tenderer. In case of joint venture, the tenderer must submit a separate Form for each member. The beneficial ownership information to be submitted in this Form shall be current as of the date of its submission.

For the purposes of this Form, a Beneficial Owner of a Tenderer is any natural person who ultimately owns or controls the Tenderer by meeting one or more of the following conditions:

- *Directly or indirectly holding 25% or more of the shares.*
- *Directly or in directly holding 25% or more of the voting rights.*
- *Directly or indirectly having the right to appoint a majority of the board of directors or equivalent governing body of the Tenderer.*

Tender Reference No.:_____[*insert identification no*] Name of the Assignment:_____*[insert name of the assignment]* to:_____*[insert complete name of Procuring Entity]*

In response to your notification of award dated_____*[insert date of notification of award]* to furnish additional information on beneficial ownership:_____*[select one option as applicable and delete the options that are not applicable]*

I) We here by provide the following beneficial ownership information.

Details of beneficial ownership

Identity of Beneficial Owner	**Directly or indirectly holding 25% or more of the shares** **(Yes / No)**	**Directly or indirectly holding 25 % or more of the Voting Rights** **(Yes / No)**	**Directly or indirectly having the right to appoint a majority of the board of the directors or an equivalent governing body of the Tenderer** **(Yes / No)**
[include full name (last, middle, first), nationality, country of residence]			

OR

ii) We declare that there is no Beneficial Owner meeting one or more of the following conditions: directly or indirectly holding 25% or more of the shares. Directly or indirectly holding 25% or

more of the voting rights. Directly or indirectly having the right to appoint a majority of the board of directors or equivalent governing body of the Tenderer.

OR

We declare that we are unable to identify any Beneficial Owner meeting one or more of the following conditions. [If this option is selected, the Tenderer shall provide explanation on why it is unable to identify any Beneficial Owner]

Directly or indirectly holding 25% or more of the shares. Directly or indirectly holding25% or more of the voting rights.

Directly or indirectly having the right to appoint a majority of the board of directors or equivalent governing body of the Tenderer]"

Name of the Tenderer: .....[insert complete name of the Tenderer]*_____

*Name of the person duly authorized to sign the Tender on behalf of the Tenderer: ** [insert complete name of person duly authorized to sign the Tender]*

Title of the person signing the Tender: ..... [insert complete title of the person signing the Tender]

Signature of the person named above: ..... [insert signature of person whose name and capacity are shown above]

Date signed ..... [insert date of signing] day of..... [Insert month], [insert year]

TECHNICAL SPECIFICATIONS

CONTENTS

1 ABBREVIATIONS & TERMS 217

2 INTRODUCTION 221

2.1 General 221

2.2 The project sites 221

3 PRELIMINARIES 222

3.1 Preambles and Notes 222

3.2 Preliminaries 229

4 ISS GENERAL DESCRIPTION 245

4.1 General 245

4.2 PSIM 248

4.3 Electric fences 249

4.4 CCTV system 250

4.5 Video Management System (VMS) 250

4.6 AI analytics solution 253

4.7 Access Control System (ACS) 253

4.8 Intrusion Detection System (IDS) 256

4.9 License Plate Recognition (LPR) system 256

4.10 Under Vehicle Screening System (UVSS) 256

4.11 Intercom system 257

4.12 Public address (PA) system 257

4.13 Anti-ram arm barriers 257

4.14 Local Control Rooms (LCR's) 257

4.15 Main Security Center (MSC) 258

4.16 Secondary Main Security Center (SMSC) 258

4.17 Dedicated Data Communication Network (DDCN) 258

4.18 Cyber security 259

4.19 Existing equipment 261

4.20 Integration phases 261

4.21 Equipment compliance and brand authenticity requirements 261

4.22 Local sites - high-level network architecture 263

5 SCOPE OF WORKS 264

5.1 General 264

5.2 Detailed design 264

5.3 Design review meetings 265

5.4 Project schedule and the Contractor work plan 268

C2: CBK - Official

5.5 Project management 269
5.6 Installation works 269
5.7 Works at the Client premises 271
5.8 Safety and safety plan 272
5.9 Sites drawings 272
5.10 Protection of design materials 273
5.11 Design according to human factors principles 273
5.12 Quality of work & equipment 274
5.13 Manufacturing of "Non-Standard" equipment 274
5.14 Replacements of specified equipment 275
5.15 Commissioning 275
5.16 Acceptance tests 275
5.17 Technical documentation 277
5.18 Training 279
5.19 System hand – over 280
5.20 Supervision 280
5.21 Warranty period 281
5.22 Repair of faults 282
5.23 Supplementary warranty 282
5.24 Licenses and passwords 282
6 PSIM 284
6.1 General 284
6.2 General requirements 285
6.3 PSIM architecture 287
6.4 Redundancy 289
6.5 High - Availability 289
6.6 Capacity 290
6.7 PSIM core modules 290
6.8 Events management module 291
6.9 Video management module 293
6.10 GIS and map module 296
6.11 Mobile application 298
6.12 Mass notifications module 299
6.13 Reports generation module 300
6.14 Rules engine module 303
6.15 KPI's and dashboards module 303
6.16 Standard Operating Procedures (SOP's) module 304
6.17 Integration with subsystems 305
6.18 Events management workflow 309

C2: CBK - Official

6.19 System configuration and management 311
6.20 Tasks management module 312
6.21 Health monitoring capabilities 312
6.22 Cyber security 313
6.23 Audit logging 314
6.24 PSIM server 315
6.25 PSIM workstation 316
6.26 24” monitor 317
6.27 NTP server 319
7 HIGH AVAILABILITY 320
7.1 General 320
7.2 HA Environment Architecture 321
8 CCTV SYSTEM 323
8.1 General 323
8.2 Integration with PSIM 323
8.3 5 MP AI Dome camera 324
8.4 5 MP AI Bullet camera 326
8.5 8 MP AI Dome camera 328
8.6 8 MP AI Bullet camera 330
8.7 PTZ IR camera 4 MP 331
8.8 Thermal camera 334
8.9 Camera pole 335
8.10 Wall/fence mounted pole 337
9 VIDEO MANAGEMENT SYSTEM 338
9.1 General 338
9.2 System architecture 338
9.3 Edge intelligence and forensic search integration 340
9.4 Live viewing 342
9.5 Virtual Matrix 342
9.6 VMS software features 343
9.7 VMS server 348
9.8 Recording server 349
9.9 VMS client workstation 351
9.10 24’ monitor 352
10 VIDEO WALL 353
10.1 Functional requirements 353
10.2 Video wall management console 354
10.3 Audio management functional requirements 355
10.4 Cyber security 356

C2: CBK - Official

10.5 55’ screen 356
10.6 Video Wall Mounting Structure and Brackets 357
11 INTELLIGENT VIDEO ANALYTICS 358
11.1 General 358
11.2 System architecture 359
11.3 Cyber security 360
11.4 Performance requirements 360
11.5 Detection and classification 361
11.6 Behaviour analytics 361
11.7 Image-based search (Forensic Search) 361
11.8 Human attribute search 362
11.9 Bookmarking and export 362
11.10 Privacy masking 362
11.11 Analytics Management Requirements 362
12 ACCESS CONTROL SYSTEM 362
12.1 General 362
12.2 System architecture 363
12.3 System main features 364
12.4 Integration with the PSIM 365
12.5 ACS software 366
12.6 ACS server 373
12.7 ACS client workstation 374
12.8 Controller, 2 readers 376
12.9 Controller, 4 readers 378
12.10 Face recognition / Finger / RFID reader 378
12.11 Finger / RFID reader 380
12.12 RFID reader 381
12.13 Electromagnetic lock, single leaf door, 600 Lbs 383
12.14 Electromagnetic lock, double leaf door, 600 Lbs 383
12.15 Electromagnetic lock, single leaf door, 300 Lbs 383
12.16 Electric strike lock 383
12.17 Request To Exit (REX) - Contactless 384
12.18 Emergency door release 385
12.19 High security magnetic door position switch 385
12.20 Hydraulic door closer 385
12.21 Enrolment workstation 386
12.22 Enrolment RFID reader 389
12.23 Contactless smart card 389
12.24 Door alarm 390

C2: CBK - Official

13 INTRUSION DETECTION SYSTEM 391
13.1 General ... 391
13.2 Integration with the PSIM ... 392
13.3 Control panel ... 394
13.4 Internal 8 zones expansion module ... 402
13.5 External 32 zones expansion module ... 402
13.6 Keypad ... 402
13.7 External alarm strobe & siren ... 404
13.8 DT Wall mounted detector ... 405
13.9 Ceiling detector, up to 4 meters ... 406
13.10 Ceiling detector, up to 8 meters ... 407
13.11 Seismic detector ... 408
13.12 Panic alarm switch, wired ... 410
13.13 Magnetic door position switch ... 410
13.14 Heavy duty magnet ... 411
13.15 Active IR beam, 15 / 50 / 100 meter, Outdoor ... 411
13.16 Dual technologies detector, Outdoor ... 413
13.17 Curtain detector ... 414
13.18 Laser detector, Grade 3 ... 415
14 PUBLIC ADDRESS SYSTEM 415
14.1 General ... 415
14.2 Integration with the PSIM ... 416
14.3 PA master station console ... 417
14.4 Network horn speaker ... 418
14.5 Network ceiling speaker ... 419
15 INTERCOM SYSTEM 420
15.1 General ... 420
15.2 Performance ... 420
15.3 Integration with the PSIM ... 420
15.4 Intercom master station console ... 420
15.5 Video intercom door unit ... 422
15.6 Intercom pole ... 423
16 LICENSE PLATE RECOGNITION SYSTEM 424
16.1 General ... 424
16.2 System architecture ... 424
16.3 Functional requirements ... 425
16.4 System main components ... 427
16.5 Integration with the PSIM ... 428
16.6 Cyber security ... 428

C2: CBK - Official

16.7 LPR software 429
16.8 LPR server 432
16.9 LPR client workstation 433
16.10 LPR camera 434
16.11 LPR camera pole 435
17 UNDER VEHICLE SCANNING SYSTEM 436
17.1 General 436
17.2 Functional requirements 436
17.3 Technical specifications 437
17.4 Detection performance 440
17.5 Cyber security 441
17.6 Server / workstation 442
18 RADAR 443
18.1 General 443
18.2 Performance requirements 443
18.3 Technical requirements 445
18.4 Radar management software 446
18.5 Integration and cybersecurity 447
19 LIDAR RADAR 448
19.1 LiDAR system performance parameters 448
19.2 Zone configuration requirements 448
19.3 Laser characteristics 448
19.4 Coverage geometry 448
19.5 GIS Interface 448
19.6 AI capabilities 449
19.7 CCTV Cameras integration 449
19.8 Scalability 449
19.9 Display and management 449
19.10 Cyber security 451
20 DATA COMMUNICATION SYSTEM 451
20.1 Industrial 8 RJ45 ports + 2G SFP Managed PoE Switch 451
20.2 Industrial 16 RJ45 ports + 4G SFP Managed PoE Switch 451
20.3 Access switch, Managed layer 2/3, 24 ports 452
20.4 Layer 3, Managed core switch 453
20.5 Optical patch panel 455
20.6 Copper patch panel 456
20.7 Single mode fiber optic cable – 12 cores 456
20.8 Single mode fiber optic cable – 24 cores 457
20.9 CAT 7 data cable 458

C2: CBK - Official

20.10 CAT 6A data cable 458
20.11 44U Equipment rack 459
20.12 22U Equipment cabinet 461
20.13 15U Equipment cabinet 461
20.14 6U Equipment cabinet 462
20.15 Outdoor communication cabinet 462
20.16 DIN rail UPS for outdoor communication cabinet 464
20.17 UPS for indoor communication cabinet 465
20.18 UPS 10 kVA 465
20.19 KVM extender 466
20.20 Industrial controller (Data acquisition and control module) 467
20.21 Rodent repellent system 468
20.22 Environmental monitoring system 468
21 COMMUNICATION & ELECTRICITY INFRASTRUCTURE 469
21.1 General 469
21.2 Metal cable tray 60×120 mm 469
21.3 HDPE communication conduit, 50 / 75 mm 470
21.4 Flexible corrugated (flexible) conduit – 32 / 50 / 75 mm 470
21.5 PVC duct, 60 / 120 mm 471
21.6 Rigid PVC Conduit, 16 / 20 / 25 mm 472
21.7 Pliable conduit 16 / 20 / 25 mm 473
21.8 Manhole, 60cm 473
22 MAIN SECURITY CENTER 474
22.1 General 474
22.2 MSC components 474
22.3 Operation centre (OC) 474
22.4 Crisis Management Room (CMR). 476
22.5 Supervisor / Duty officer room 477
22.6 Technical equipment room 478
22.7 Operators' rest area 478
22.8 MSC construction 478
22.9 Control console module (control desk) 481
23 SCANNING DEVICES 485
23.1 Walk- Through metal detector 485
23.2 Hand-held metal detector 487
23.3 Luggage screening system 488
24 GATES & CONTROLLED PASSAGES 489
24.1 Full height turnstile 489
24.2 Speed gate 491

C2: CBK - Official

24.3 Wide speed gate 493
24.4 Accessible swing gate 494
24.5 Anti-ram raising arm barrier - DOD K 4 495
24.6 Retractable, hydro-electric bollards, K4 497
24.7 Arm barrier 498
24.8 Cantilever sliding gate 500
24.9 Gate control panel 501
24.10 Anti-vehicle spikes 501
24.11 Forced entry rated door, 5 minutes 502
24.12 Forced entry rated grille, 5 minutes 503
25 ELECTRONIC KEY MANAGEMENT SYSTEMS 504
25.1 Electronic physical keys management cabinet 504
26 CYBER SECURITY 506
26.1 Introduction 506
26.2 Cyber security concept 506
26.3 Procurement processes (Supply Chain Management - SCM) 507
26.4 Laboratory environment, test field, and integration 507
26.5 Service – Active Directory (AD) 507
26.6 NOC system (Monitoring) 508
26.7 Maintenance, security updates and license renewal – SLA 508
26.8 Data communication protection 509
26.9 Network separation principles 509
26.10 System hardening principles 510
26.11 Principles of switches hardening and network settings 511
26.12 Principles of computer stations and endpoints hardening 511
26.13 Central Cyber Incident Management System 511
26.14 Lifecycle vulnerability management (CVE) for IoT/OT assets 512
26.15 Compliance and reporting 512
26.16 Sanitization station 512
26.17 Endpoint security system 513
26.18 Intrusion Detection Systems (IDS) 513
26.19 NAC System (Network Access Control) 514
26.20 Hardened technician computers 514
26.21 Technical specification – EDR 514
26.22 Content Disarm and Reconstruction 515
26.23 Technical specification – Firewall 516
26.24 Training and documentation 518
27 GENERAL TECHNICAL SPECIFICATIONS 518
27.1 General 518

C2: CBK - Official

27.2 Installation of equipment & systems 519
27.3 Future expansion 520
27.4 Software and licenses 520
27.5 General environmental compliance requirements 520
27.6 Electricity 521
27.7 Protection 521
27.8 Grounding (Earthing) 521
27.9 Reliability and maintainability 521
27.10 General mechanical requirements 522
27.11 Marking and labelling 522
27.12 Galvanization 522
27.13 Conduits / Piping 522
28 MAINTENANCE SERVICE 523
28.1 General 523
28.2 Preventive maintenance 524
28.3 Fault and malfunctions repair 524
28.4 Software maintenance 525
28.5 Response time for service calls 525
28.6 Penalty mechanism 526
28.7 Service centre 526
28.8 Equipment and materials for maintenance 526
28.9 Inventory levels of equipment and components 526
28.10 Maintenance technical team 527
28.11 Computerized monitoring system 527
28.12 System documentation updates 527
29 MEASUREMENT OF QUANTITIES 527
29.1 General 527
29.2 Unit prices 527
29.3 Changes and additions to Bill of Quantities 528

C2: CBK - Official

ABBREVIATIONS & TERMS

A	
ACS	Access Control System
ADC	Access Door Controller
AIU	Access Identification Unit
AOI	Area of Interest
ARO	After Receipt of Order
ATP	Acceptance Test Procedures
B	
Bidder	A firm/s that will choose to reply to this RFP
C	
CBK	Central bank of Kenya
CCTV	Closed Circuit Television
CDR	Critical Design Review
Contractor	The awarded Tenderer
Consultant	J. Gordon Consulting Engineers Ltd.
D	
DDCN	Dedicated Data Communication Network
DLP	Defect Liability Period/Warranty Period
DVR	Digital Video Recording System
E	

EDR	Endpoint Detection and Response
F	
FAT	Factory Acceptance Tests
FAR	False Alarm Rate
FOC	Fiber Optic Cable
FPS	Frame Per Second
G	
GOS	Grade of Service
GUI	Graphical User Interface
I	
IDS	Intrusion Detection System
ILS	Integrated Logistic Support
IR	Infra-Red
ISS	Integrated Security System
J	
JV	Joint Venture
K	
KC	Keys Cabinet
L	
LAC	Local Alarm Controller
LAN	Local Area Network
LCR	Local Control Room

LPR	License Plate Recognition
LSS	Luggage Screening System
M	
MCBF	Mean Cycle Between Failure
MMI	Men Machine Interface
MSC	Main Security Center
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
N	
NAC	Network Access Control
NAS	Network Attached Storage
NVR	Network Video Recording
O	
ONVIF	Open Network Video Interface Forum
OSD	On - Screen Display
OTDR	Optical Time Domain Reflectometer
P	
PA	Public Address
PDR	Preliminary Design Review
PIDS	Perimeter Intrusion Detection System
PLC	Programmable Local Controller
PM	Project Manager

POD	Probability Of Detection
POE	Power Over Ethernet
PSIM	Physical Security Information Management
PTZ	Pan Tilt Zoom
R	
RAID	Redundant Array of Independent Disks
RFI	Request For Information
RFP	Request For Proposal
S	
SAT	Site acceptance tests
SMSC	Secondary Main Security Center
SNMP	Simple Network Management Protocol
SOW	Scope Of Work
T	
TBD	To Be Decided
Q	
QAP	Quality Assurance Plan
V	
VCS	Visitors Control System
VLAN	Virtual Local Area Network
VMS	Video Management System
VMD	Video Motion Detection
WAN	Wide Area Network

C2: CBK - Official

INTRODUCTION

General

The Central Bank of Kenya (hereinafter: CBK) is the monetary authority of Kenya. CBK promotes financial stability; ensures effectiveness and efficiency of the payment, clearing and settlement systems; formulates and implements foreign exchange policies; holds and manages foreign exchange reserves; issues currency; and serves as the banker, adviser, and fiscal agent of the Kenyan government.

As part of its efforts to enhance the organization's overall security posture, CBK management has decided to implement a modern Integrated Security System (hereinafter: "ISS"), intended to mitigate current and emerging security threats.

This document details the Scope of Work (hereinafter referred to as the "SOW"), general conditions for implementation, and technical specifications of the security subsystems that comprise the required ISS and are to be implemented by the winning Bidder (hereinafter referred to as the "Contractor").

The ISS described in this document has been designed by the Consultant at a "system engineering" level. The Contractor shall carry out the detailed design of each ISS subsystem, as well as the ISS system as a whole, producing a fully detailed and accurate design and work plans for the complete implementation of the Project.

Relevant drawings will be provided by the Client to the winning Bidder only.

The project sites

The project shall be implemented at the following CBK sites:

a) CBK HQ building – Nairobi County.
b) Institute of Momentary Studies (IMS) – Nairobi County.
c) ExTelecoms house – Nairobi County.
d) Kisumu branch - Kisumu County.
e) Mombasa branch – Mombasa County.
f) Eldoret branch - Uasin Gishu County.
g) Nakuru currency center – Nakuru County.
h) Nyeri currency center – Nyeri County.
i) Meru currency center – Meru County.
j) Kisii currency center - Kisii County.

Some of the project sites are large multi-story office buildings, ranging from six (6) to eleven (11) floors. These sites include: CBK Headquarters, ExTelecom Building, Mombasa Branch, Kisumu Branch, and Eldoret Branch.

Other project sites are smaller, consisting of two (2) to three (3) floor buildings. These include the Nakuru, Kisii, Meru, and Nyeri currency centers.

C2: CBK - Official

All of the above sites share common characteristics, including strong rooms, service yards, banking halls, and office areas.

The Institute of Momentary Studies (IMS) is a large complex that occupies an area of approx. 50 hectares. Within the complex there are various buildings, including: the main administrative building, academic and conference complex, a library building, staff residences compound, a police station, police officers' housing compound, rental housing units, hotel, football field and other facilities.

PRELIMINARIES

Preambles and Notes

Parties and project responsibility matrix

Project Management Team

CBK Project Team shall be responsible for overall management of the project and shall remain overall approver and decision-making organ of the project.

The Consultant

CBK have appointed consultants in the project who shall have delegated authority and shall be responsible for contract administration and supervision of the project, herein be referred to as 'The Consultant'.

Contractor

The contractor shall mean the entity contracted to execute the works, personnel, agents and subcontractors engaged for the works and shall be responsible for execution of works in accordance with the contract conditions and shall herein be referred to as 'The Contractor'.

Definitions and abbreviations

Abbreviations used in these Bills of Quantities shall be interpreted as follows: -

- "Approved" shall mean approved by the Consultant and CBK
- "As Directed" shall mean directed by the Consultant
- "Architect/Engineer" shall mean the Consultant
- "B.S. " shall mean the current British Standard BMS shall mean Building Management System
- "C. M" or "M3" shall mean Cubic metres
- "CCTV" shall mean Closed Circuit Television
- "CV" shall mean Curriculum Vitae
- "Ditto" shall mean the whole of the preceding description except as qualified in the section in which it occurs. Where it occurs in brackets it shall mean the whole of the preceding description which is contained within the approximate brackets.
- "GIFA" shall mean Gross Internal Floor Area
- "GBA" shall mean Gross Building Area as measured in accordance with RICS and IPMS guidelines.
- "Kg" shall mean Kilograms
- "KPC" shall mean Kenya Power Company
- "L.M" or "M" shall mean Linear Metre

C2: CBK - Official

- “M.S” shall mean Measured separately
- "No" or "N" shall mean Number
- “S.M” or "M²" shall mean Square Metres
- "VAT" shall mean Value Added Tax
- “CBK" shall mean Central Bank of Kenya Office
- “UPS” shall mean Uninterrupted Power Supply
- “PV” shall mean Photovoltaic
- “LPG” shall mean Liquified Petroleum Gas

Notes:

a) Bidders are required to study general and particular conditions of contract and price under particular preliminaries section.
b) Bidders are referred to the Definitions and Abbreviations section contained in the General Preliminaries section for the abbreviations stated in the Bills of Quantities.
c) The Contractor may be required to share during the course of the contract or hand-over at completion of the contract the site offices, stores and hoarding to other Contractor's at no cost.
d) Items not priced shall be deemed to have been included in rates for other priced items.
e) This is a fixed unit-rate re-measurable contract. (The unit-rates shall remain fixed for the duration of the contract and no fluctuations of prices shall be allowable. However, some quantities may be remeasured particularly where indicated as 'provisional' or following changes on site)

Description of site

The site of the works is as indicated in item 2.2 of this document

Deliveries & removal

The project is within an active site, fully operational Facility which operates in normal working hours with various conferences, operations and meetings going on. Deliveries of goods, materials, tools and equipment shall therefore be done in a manner that does not cause any hindrances or inconvenience to the normal operations. For start-up it may be done prior to the day of the initial start of the first workday or it can be done on Saturdays, during the work day it should at least be done outside of the peak period of CBK staff arriving at work in the mornings, preferably early morning hours, mid-day deliveries at 1300 hours and last delivery 1 hour before close of day which can be either 1500 hours if work ends at 1600 and 1600 hours if work ends at 1700hours. Advance permission has to be obtained from CBK Security. Deliveries are to be made through the designated gates approved by security team. The Contractor is to notify CBK at least 48 hours in advance of deliveries in order that relevant clearance is obtained. Heavy materials deliveries: Delivery of heavy materials to site shall be governed to comply with delivery times in accordance with the Local Authority requirements.

Sufficiency of bid

The Contractor shall be deemed to have satisfied themselves before bidding as to the correctness and sufficiency of their bid for the works and of the rates and prices used in arriving at the fixed unit-rate(s) stated in the priced bills of quantities which rates and prices shall cover all the obligations under the Contract and all matters and things necessary for the proper completion and maintenance of the works.

DRAWINGS

C2: CBK - Official

Before submitting the bid, bidders may examine all the drawings and satisfy themselves regarding all details as no claim by reason of ignorance to this connection will be allowed.

The bidder shall satisfy themselves as to the correctness of all drawings and measurements. If the bidder finds any discrepancy on the drawing or between the drawings and the bills of quantities, they shall immediately refer the same to CBK who shall decide which direction shall be followed.

Figured dimensions will be used in preference to scales mentioned on or attached to any drawing.

The Contractor is to take the necessary particulars for ordering materials and work from the drawings and the work in progress on the building and not use the Bills of Quantities for that purpose.

Request for information

All requests from the Contractor shall be in writing in the form of a RFI pro- forma containing the following basic information:

- Contractor's Name
- Project Name
- Author of RFI
- RFI Number
- RFI Date
- Subject Title
- Subject Matter RFI"€™s shall be issued in numerical order and if multiple pro forma booklets are produced they shall be in consecutive series.

Works to be executed in a highly sensitive environment

Operating within the CBK facility requires exceptional attention to detail, careful planning, and strict adherence to operational, safety, and security standards. The Contractor shall plan, review, and execute all activities so as to safeguard business continuity and avoid disruption to CBK operations. Key obligations include minimizing nuisance and disruption to site operations and personnel; maintaining safety and security through coordinated and approved movements and activities; monitoring site conditions continuously and adapting promptly to unforeseen issues; ensuring business continuity during construction; and maintaining civil and respectful conduct when communicating or interacting with CBK staff. The Bidder shall adhere to these principles and commit to a collaborative, detail-oriented approach subject to CBK approval.

Cooperation with stakeholders and other contractors on site

Collaboration with CBK team is mandatory to ensure smooth integration of contractor activities with ongoing site management tasks. Bidders' attention is drawn to the fact that other works by other vendors will be running concurrently. Cooperation by all parties, including syncing deliveries and use of any CBK designated areas for storage of materials, waste etc shall be required. The contractor must ensure open and constant communication with these teams, addressing any potential impacts to operations well in advance.

C2: CBK - Official

Prohibition of publicity

CBK is a highly guarded organization where security and operation of activities remain highly confidential. The Contractor shall not, without the prior written consent of CBK, use the Central Bank of Kenya"€™s name, logo, or any information related to the Project for any advertising, marketing, or publicity purposes. The Contractor shall not issue any press releases, public announcements, or engage in any form of media communication regarding the project without the prior written approval of the Central Bank of Kenya.

Bidders conference & site visit

Bidders shall be required to visit the site at a date to be advised by CBK, to acquaint themselves with the nature of the site, access to site, delivery logistics, source of various materials and all matters relating site and its operations. Bidders shall be required to liaise with CBK for additional information on site visit arrangement including clarity on date and time of visit and security clearance procedures. The bidder and any of their personnel or agents shall be required to request for conditional permission to enter the site upon complying with all security procedures as shall be required. The permission shall be deemed to be based upon the bidder, their personnel and agents indemnifying CBK and their personnel and agents from and against all liability and upon the bidder being responsible for personal injury (whether fatal or otherwise), loss of or damage to property and any other loss, damage, costs and expenses (however caused) which would not have arisen other than due to the exercise of such permission. The bidder is required to visit the site and shall be deemed to have acquainted themselves therewith as to the nature of the site, position and means of access etc and no claim in this connection will be allowed before or after award of the contract. No claims will be allowed for travelling expenses which may be incurred by the bidder in visiting the site or preparing the bid for the works.

Supervision

The Works shall be executed under the direction and to the entire satisfaction of the Consultant, who shall have CBK's specifically delegated authority and shall always have access to the Works and to the yards and workshops of the Contractor or other places where work is being prepared for the building works.

Proprietary materials and alternatives

Identified proprietary items:

Identification of a proprietary item, product or system does not necessarily imply exclusive preference for the item so identified, but indicates the necessary properties, performance and/or appearance of the item, and available warranties. Where items are identified as a proprietary item or product they have generally been selected for their appearance and performance. Substitutions will only be considered if the substitutions are identical in appearance, and equal and greater in performance. Artificial and fake substitutions such as pattern printed board products must not be deemed to be identical appearance to specified natural products. If substitutions to the documented proprietary items, products, methods or systems are proposed, submit sufficient information shall be required to permit evaluation of the proposed substitution including the following: Evidence of conformity to a cited standard Samples Essential technical information, in English Reasons for the proposed substitutions Advantages to the Central Bank of Kenya Statement of the extent of revisions to the contract documents Statement of the extent of revisions to the construction program Statement of cost implications including costs outside the contract Statement of consequent alterations to other parts of the Works Documentary evidence demonstrating that the proposed substitution of materials and products meet the technical and design intent aspects of the design in the contract Documentary evidence demonstrating the proprietary item or product's equal or better compliance with relevant standards Documentary evidence demonstrating that the substitution is consistent with the contract documents and is as effectual as the identified proprietary item Proprietary materials, products and items are specifically noted as the preferred selection. Substitutions will only be considered under the following conditions: Substitutions are submitted for

C2: CBK - Official

approval insufficient time to permit proper evaluation Evidence is provided that the documented proprietary items, products or systems are unavailable within the time constraints of the construction program Once substitutions have been submitted and approved, they shall not be varied nor shall further substitutions be offered or proposed without specific written permission. Substitutions offered by reason of the specified item or product not being ordered in sufficient time will not be considered a valid reason for substitution demonstrate that the proposed substitutions to proprietary items or products meet the technical and design intent aspects of the current design Performance based specifications: Where items are specified by performance the Contractor shall submit evidence to show compliance with the performance criteria provided in the specification and drawings.

Value engineering

The bidder may propose alternatives only after award of the contract and shall be required to demonstrate how the alternatives give value to the project (cost saving or time). Bid submission shall however strictly comply to prescribed standards and specifications. Alternatives shall meet or exceed the performance requirements specified in the bid document and shall be approved by the Consultant and CBK.

Blasting

Unless otherwise agreed with the relevant authorities no blasting shall be allowed to be carried out on site. Any rock that is encountered with must be removed by use of sledgehammers, heavy-duty rippers mounted to tractors or by compressor.

Provisional work

All "Provisional" and other work liable to adjustment or remeasurement under this Contract shall be left uncovered for a reasonable time to allow all measurements needed for such adjustment to be taken by the Consultant. Immediately the work is ready for measurement, the Contractor shall give notice to the Consultant. If the Contractor makes default in these respects, they shall, if the Consultant so directs, uncover the work at their own expense to enable the measurements to be taken.

Existing works and protection of completed works

The Tenderer is hereby advised that main builders and infrastructure works have already been executed by the Main Works Contractor and/or other contractors within the project area. The Tenderer shall be deemed to have inspected and familiarized himself with the nature, extent, condition, and location of such existing and completed works prior to submission of tender.

The Tenderer shall take all necessary precautions to protect existing structures, finishes, installations, services, equipment, and completed works from damage during the execution of his works. Any damage caused directly or indirectly by the Tenderer, his employees, subcontractors, or suppliers shall be made good by the Tenderer at his own cost and to the satisfaction of the Engineer/Project Manager.

No additional payment shall be made for compliance with this requirement, and all costs associated with inspection, protection, temporary coverings, safeguarding measures, and reinstatement of damaged works shall be deemed to be included in the Tender Sum.

General and special attendance

The Contractor shall be deemed to have allowed for providing all general attendance and special attendance necessary for the proper execution, completion, testing, commissioning, and maintenance of his works.

General attendance shall include, but not be limited to, site management, supervision, labour, access to work areas, coordination with other contractors, unloading, handling, storage of materials, attendance at meetings,

C2: CBK - Official

setting out, cleaning, waste disposal, and all other routine support services required for the execution of the works.

Special attendance shall include, but not be limited to, the provision of scaffolding, lifting equipment, hoisting facilities, temporary supports, temporary weather protection, plant, tools, testing equipment, power, water, security measures, protection of completed works, and any other specialist services or facilities necessary for the proper execution of the works.

The Contractor shall make his own arrangements for all such attendance and no separate or additional payment shall be made in respect thereof. All costs associated with the provision of general attendance and special attendance shall be deemed to be included in the Contract Sum.

Domestic sub-contractors & specialists

The Contractor will be expected to employ approved specialist domestic subcontractors. The contractor shall be expected to provide for the works and services listed above with attendance to specialist subcontractor and undertake the necessary builders work in connection therewith. Where such builders work is not separately and identified under the measured section of these bills of quantities; this shall be deemed considered included in the Contractor's overall building works rates

Implementation options & Central Bank of Kenya’s direct contracts

The Central Bank of Kenya shall have the right to employ other Contractors (hereinafter referred to as "Direct Contractors") to execute any special or other works whether contained in this Contract or not, concurrently with the work being executed under this Contract. In addition, the Central Bank of Kenya shall have the right to send on to the Works any furniture, furnishings, curtaining, carpeting and fittings and have same installed by their own employees or by Direct Contractors. The Contractor shall not be entitled to any percentage, profit or discount on the value of any work executed by "Direct Contractors but shall nevertheless allow these Direct Contractors and the Central Bank of Kenya's employees to have access to the Works, allocate reasonable space in the building for the storage of their materials, tools and equipment, and co-ordinate the work of and "attend upon" such Direct Contractors as necessary all to the satisfaction of the Consultant and CBK. Any such costs associated with such direct contracts shall be deemed included in the Bid. The Contractor shall have the duty to undertake all such works as measured in the required quality and hence must ensure adequate rates are provided.

Note:

The Contractor shall allow such Direct Contractors to work on site without encumbrances and shall ensure that all direct contractors are inducted into the safety regime of the Contractor.

Accommodation and labour camps on site

No accommodation on site will be permitted for the Contractors staff or work people including those of sub-contractors other than the security staff. The Contractor shall NOT be permitted to house any other workers on site. The Contractor should make their own arrangements to house the workers elsewhere and/or organize for their transportation to and from site. Any application for exemption from this requirement shall be at CBK's discretion.

Area to be occupied by contractor to be approved & authorized by CBK

The area of the site which may be occupied by the Contractor for use as storage and for the purpose of erecting workshops, etc., shall be defined on the site by the Consultant and CBK. All operations of the contractor, including without limitation, storage of equipment, materials, supplies and parts, within CBK premises or property, shall be confined to areas authorized or approved by CBK. The Contractor's personnel shall not enter or pass through and shall not store or dispose off any of its equipment or materials in any areas within CBK's premises or property without appropriate authorization from CBK.

C2: CBK - Official

Transport to and from the site

The Contractor shall include in their fixed unit-rates, for the transport of materials, workmen, etc., to and from the site of the proposed Works, at such hours and by such routes as are permitted by the authorities.

Prime cost sums and rates

a) The words "Prime Cost" (or the initials "PC") wherever appearing in the Contract Documents shall mean net cost exclusive of any trade, cash or other discount whatsoever but inclusive of the cost of packing. Such cost shall be the sums due to the Sub-Contractor or Supplier after adjustment where applicable in respect of measurements or rates.

b) Any increases or decreases in these Prime Cost Sums and Rates resulting from the adjustments and properly paid by the Contractor shall be added to or deducted from the Contract Sum in the final account. In substantiation the Contractor will be required to produce to the Consultant all quotations, invoices and receipted accounts as shall be necessary to show the details of the sums actually paid.

c) Prime Cost Rates shall be deemed to be exclusive of VAT, delivery to site and fixing. Any sum added by the Contractor in these Bills of Quantities in respect of profit upon any Prime Cost will be deducted at the final settlement of accounts and a sum will be added the amount of which will bear the same proportion to the sum added as the net amount properly expended bears to the original PC sum.

Fair wages

The Contractor shall pay rates of wages and observe hours and conditions of labor not less favorable than the minimum rates of remuneration and minimum conditions of employment applicable. The Contractor is to comply with the Regulation of Wages and Conditions of Employment Act, Building and Construction Industry Wages Council and is to be responsible for compliance by sub-contractors employed in the execution of the Contract. If required, the Contractor is to notify the Consultant and CBK of the name and addresses of all such sub-contractors. Any Contractor or sub- contractor not so complying will not be permitted to bid for other work for such period as CBK may determine. Should a claim be made to the Consultants alleging the Contractor's default in payment of fair wages of any workman employed on the Contract and if proof thereof satisfactory to the Consultant is furnished in accordance with the Contract, the Consultant may, failing payment by the contractor, recommend payment of the claim by CBK and offset from any monies due or which may become due to the Contractor under this contract. The Contractor shall furnish to the Consultant, where so required, such particulars of the rates of wages, hours and conditions of Contract referred above, as the Consultant may direct.

Standards levy

The Contractor is required to ascertain at their own cost of any legal notices, regulations or laws which require payment by the Contractor of a Standard levy to the Kenya Bureau of Standards.

Training levy

The Contractor is required to ascertain at their own cost of any legal notices, regulations or laws which require payment by the Contractor of a Training levy for any Contract.

Withholding tax

The Contractor shall ensure that they have full knowledge of the workings of withholding tax in a tax, particularly VAT, exempt project.

C2: CBK - Official

Value added tax (vat)

The contractor shall include VAT at the current rate.

Copyright

The copyright of this document is vested in CBK and they may not be reproduced in whole or in part without CBK's written permission.

Preliminaries

Contractor's investigation for service infrastructure & other utilities

No work may commence without a full and detailed validation of existing service infrastructure. The Contractor is expected to use available documentation to plan for the Works particularly where tapping and connection to established system.

The contractor shall be expected to employ skill and carefully identify, protect and avoid cutting, damaging or disrupting the active existing site services during the execution of the Works. If the Contractor has any doubt to services encountered, then the contractor shall immediately notify the Consultant and CBK for instructions and guidance on how to proceed.

The contractor must assess where and when services will need to be disconnected and work closely with CBK to schedule these disruptions with minimal impact. Any interruptions to power, water, communications, or other utilities must be planned well in advance and communicated clearly to all affected parties. The contractor shall provide temporary measures where there are interruption of services (power, water, UPS etc) including provision of consumables and leasing of temporary equipment)

Detailed Review and Run-Through: A preliminary run-through of the planned activities must be conducted with the project management and CBK. This ensures all parties understand the sequence of works, potential risks, and mitigation strategies. Note: Mock scenarios or simulations may be required to validate the contractor’s readiness and coordination efforts.

Security of works (within allocated site area)

The Contractor shall be entirely responsible for the security of all the works, stores, materials, plant, personnel, etc., both owned by the Contractor and sub-contractors and shall provide all necessary watching, lighting, site hoarding and other precautions as necessary to ensure the security and the protection of the public. The contractor shall liaise with CBK Security on access control and clearance protocols to CBKs approval. The bidder shall obtain the list of security companies from CBK and MUST deploy approved security personnel to man the site. Maximum precautions must be exercised to uphold existing security in the vicinity of the Works. The Contractor shall comply with all security requirements in accordance with the Central Bank of Kenya’ security regulations currently in force and all instructions issued by the Central Bank of Kenya with regard to upholding of security arrangements and will be held responsible for any breach of security by their employees. The Contractor shall be held responsible for any breach of security by any of their agents, employees, personnel etc. The movement of the Contractor’s staff/labour must be confined strictly to the Works and the Contractor’s working and storage areas. At no time shall the contractor and his agents, be allowed to gain access to non-designated/restricted areas within the compound and must always stick operations within the allocated site. The contractor's staff shall not engage in horseplay and loitering on site. All areas on site outside the temporary hoarding are designated as "out of Bounds’ areas for the Contractor’s employees and the Contractor will be required to comply strictly with this rule. Contractors, site staff and vehicles entering the compound on a daily basis will require prior clearance and to be issued with Ground Passes to the CBK compound. Any additional staff or vehicles requiring entry during the course of the project will require similar clearance. Contractors must anticipate regular badge checks, equipment inspections, and vehicle reauthorization processes. Any lapse in clearance will result in denied access to the

C2: CBK - Official

site. Ground passes must be worn and visible at all times. Vendors may be required to provide clearance certificate as part of security vetting exercise.

Phased implementation and sectional completion

The Contractor shall abide by the proposed phased implementation of the works as shall be directed by the Consultant to suit the requirements of CBK and achieve milestones if any. Where required, the bidder shall submit a methodology, with alternative phasing proposals for approval; if any. Bidders are also notified that no contractual claims or increase in prices will be allowed due to any Phased implementation of the works. If the contractor fails to complete any section by the specified date, liquidated damages for the relevant portion shall apply proportionately. The last date of the contract works is however to be completed within the overall Contract Completion Period; and shall be the substantive date for commencement of defects liability period. No claim associated with phasing of works shall be entertained.

Working hours and overtime

The Contractor's working hours shall be in tandem with CBK's working hours as follows:

- Mon to Friday - 8am to 5pm, Nairobi time
- Saturdays - 8am to 1pm, Nairobi time
- Sundays - No Work

The Contractor shall liaise with the Consultant and CBK for approval of any other working hours. The Contractor shall be responsible for any extra costs for overtime working that they consider necessary in order to complete the work within the contract period or recover delays. If overtime is worked in accordance with a written instruction issued by the Consultant, the Contractor will be reimbursed in respect of such overtime to the extent only of the additional net cost in line with Construction Industry Wages Council and excluding any bonuses, profits and overheads.

Insurances

The Contractor shall obtain and shall, for the term of the contract and any extension thereof, maintain policies of insurance, with reputable insurance companies approved by CBK.

Minimum policy requirements

All insurance policies providing the minimum insurance coverage shall

a) Name the Central Bank of Kenya as an additional insured except worker compensation. In addition, the general liability policy shall contain cross liability clause.
b) Include waiver of subrogation of the contractor's insurers rights against the Central Bank of Kenya.
c) Provide that CBK shall receive sixty (60) days' written notice from the insurance carrier, underwriter or provider prior to any cancellation or change of insurance coverage provided under the insurance policy or policies concerned.
d) Include the provision for primary and non-contributing basis with respect to any other insurance that may be available to CBK.
e) Name the CBK as loss payee for any claims resulting from this contract.
f) The Contractor shall be responsible to fund all amounts within any policy deductible or retention.

C2: CBK - Official

Performance bond

The contractor shall provide to the Central Bank of Kenya, performance security in the form of appended bank guarantee (first demand guarantee) in accordance with prescribed form specimen. The performance security shall remain valid and in force until the end of defects liability period.

Waste management

The provision of waste disposal at the waste storage area shall be separated into the following materials as a minimum:

- Cardboard
- Timber
- Ferrous metals
- Non-ferrous metals
- Soft Plastic
- Polystyrene
- Insulation
- Concrete
- Glass
- Bricks and masonry blocks

Each bin must be color coded and clearly labelled on all four of its sides specifying which materials are to be placed in the bin. All bins must be emptied or changed on a regular basis to ensure that the bins never reach more than 99% of maximum capacity. This will ensure that recyclable waste is not inadvertently placed in the incorrect bin due to the correct bin being full. Records must be kept of materials used including data sheets and quantities for future compliance records

Hazardous substances

The Contractor is responsible for the safe removal of all hazardous substances during demolition and excavation that may include contaminated soil, asbestos, lead, lead paint, polychlorinated biphenyls (PCBs) and the like to approved standards of removal and handling of hazardous substances.

Environmental Management Plan (EMP)

The Contractor shall develop, review, update where necessary, and implement the Environmental Management Plan (EMP) prepared by the Consultant. The Environmental Management Plan shall, on a bare minimum, include:

a) Details of the proposed management structure and responsibilities of the persons responsible for environmental protection and monitoring
b) Details of the induction, training, and awareness programs, aimed at the total workforce, proposed to be implemented.
c) Details of auditing procedures proposed to be implemented to ensure adherence to environmental policies.
d) Specific project environmental constraints
e) Environmental correspondence, reporting and record keeping procedures

C2: CBK - Official

f) Risks and responsibilities (including risk assessments and method statements as well as organizational responsibilities)
g) Environmental audit procedures
h) Environmental incident and emergency response (non- conformance management)
i) Environmental training procedures
j) Solid waste management
k) Toxic waste management
l) Chemical product management
m) Temporary drainage management
n) Water quality monitoring
o) Dust and air quality management
p) Ecological protection
q) Archaeological protection
r) Excavated materials management
s) Reinstatement management
t) Borrow pits (Internal and external from CBK compound)
u) Construction Methods (Plants, machinery and equipment)
v) Access roads during construction
w) Pollution monitoring and control (spillage, refueling locations, emergency spillage kits, etc.)
x) Any special requirements in the EIA guideline (appended).

The EMP will also incorporate a construction emissions reduction plan, demolition waste management plan, an indoor air quality plan, Construction waste management plan, erosion and sedimentation control, soil management, site protection as well as observing world's best construction safety standards. Possible emissions reduction initiatives include:

a) Use energy efficient lighting (e.g. fluorescent, LED or HID)
b) Control light pollution.
c) Meter water

Hoarding, security fence and approvals

Where required, the contractor shall provide temporary hoarding around the site of the works. Bidders are required to erect the hoarding immediately on commencement of the contract works. The Contractor shall install hoarding around the site and secure the perimeter fence. Hoarding to have guarded entry points to secure the site. The hoarding shall be in painted fabricated mild steel framing, including adopting, replacing and amending as may be necessary and redecorating on commencement of works and maintaining the same throughout the construction period; hoarding may be left in place upon completion of works in this scope. All hoarding shall be painted in color approved by the Consultant and no advertisements whatsoever shall be put on the hoarding without the approval of the Consultant. The Contractor shall allow CBK to use hoarding face for any sign writing or advertising as required. All statutory charges in connection with hoarding shall be paid by the Contractor. Hoarding shall be constructed in phases and relocated and re-constructing as shall be required, all as per the Consultant's hoarding plan (appended). Bidders are therefore required to consider in their pricing, the cost of relocating and re-constructed of the hoarding to Consultant's approval.

C2: CBK - Official

Dust screens

Temporary 1.5m high solid metal hoarding The Contractor shall provide dust screen over the hoarding extending the overall hoarding height to approximately 6m high: comprising: Heavy duty dust netting fixed on and including 100 x 100 x 3mm mild steel RHS posts at 3 .0 meters centers : all to NEMA requirements and regulations: Contractor to allow for paying of all statutory charges etc. and compliance with all requirements and regulations : Allow for cleaning and maintenance of the dust netting throughout the construction period: The Contractor shall pay for all permits and approval fees related to erection and maintenance. Length of dust screen - 1500m

Occupational health & safety

All bidders shall be expected to have operational knowledge and strictly comply to the Occupational Health & Safety Act, 2007. The site shall have a competent Health & Safety Officer who shall enforce compliance of the Act. Safety officers shall be required to prepare the safety policy specific to the construction site. The 'golden rules' of the site safety shall be summarized and pinned on the notice board. As part of safety policy, visitors (and any new person to site) shall be taken through a safety moment and induction session with a view to ensure the understanding of site safety. In addition to complying with the requirements of the Occupational Safety & Health Act 2007 and the Factories Act, the Contractor and Sub-Contractors shall be required to comply in all respects with the Factories (Building Operations and Work of Architectural Construction) rules together with the Construction Safety Plan in compliance with International Labor Organizations (ILO) Regulations. All contractors staff together with visitors to site shall be expected to have safety helmet (to specific color codes), reflector jackets and safety boots (at the bare minimum) together with all other PPE safety gear necessary for their areas of operation. NOTE: The Contractor will be held responsible and shall give written Notice not later than Seven (7) days after the beginning of the building operations included in this Contract stating the particulars included in this Contract. The Contractor will further be required to identify a Site Safety Officer in accordance with the above Rules who will be responsible for the health and safety of workers on the site. A log of all incidences, accidents and near misses shall be entered into incidence logbook by competent personnel. The Contractor, subcontractors and their agents are required to study, understand and comply with the health safety strategic management plan and Health and Safety specification appended to the bid document.

Site levels

Before commencing work the Contractor must arrange for and agree with the Consultant the existing site levels and similarly establish and agree on a benchmark.

Setting out

The Contractor shall set out the Works in accordance with the dimensions and levels shown on the drawings and shall be responsible for the correctness of all dimensions and levels so set out and will be required to amend all errors arising from inaccurate setting out at their own cost and expense. Setting out will be done using survey equipment that is able to use Global Positioning System (GPS) signals to minimize errors as much as possible. In the event of any error or discrepancy in the dimensions or levels marked on the drawings being discovered, such errors or discrepancies must be corrected and reported by the Contractor to the Consultant and CBK. The setting out of works shall include setting out of all subcontractor’s work. The survey plan established shall be submitted to the Consultant and CBK for approval, use and retention. The Land Surveyor shall establish at least six (6) additional benchmarks which shall be handed over to CBK on completion of works for future reference.

C2: CBK - Official

Contractor working area, access and movements

The Contractor’s working storage and dumping area, and all their activities will be confined to locations to be as indicated in bid site layout drawings and agreed with the Consultant and CBK at the commencement of the works. The movement of the Contractor’s vehicles and workmen will be restricted to areas and routes to be agreed with the Consultant before commencing the Contract Works and these should strictly be adhered to throughout the course of the Contract unless otherwise agreed.

Temporary roads

Site access roads Upon the completion of the Works the Contractor shall remove such temporary roads, temporary culverts, bridges etc., and make good and reinstate all works and services disturbed to the satisfaction of the Consultant.

Contract samples & prototypes

Samples and Prototypes listed in the Trade Sections of the Specification shall be obtained and submitted in sufficient time to permit proper evaluation, approval and where necessary modification and re-submission prior to any requirement to commence fabrication or stockpile materials for work for which the Sample or Prototype is required as a Control. Delays caused by or arising from the late submission of Samples or Prototypes shall not be, nor deemed to be, a justification for any claim for an extension of time for completion of the Works or cost variation to the contract. Inspections off site: Where appropriate, allow for inspection of samples and prototypes in the factory or in the case of stone from the quarry. Where the factories are located in areas outside Nairobi and other countries, the contractor shall allow for all costs including travel and accommodation for consultant's staff travel for inspection and assessment of samples, equipment, materials and any other prototypes as required or directed by the Consultant and CBK.

Submission Procedure:

All samples submitted for review shall be identified by an attached label showing the project name, Contractor's name, the word "Sample", the sample number and numbered consecutively in order of submission. Acceptance: Samples shall be accompanied by the Contractor's Sample Submission and Acceptance Form' containing the following information:

a) Project name
b) Contractor's names
c) sample number
d) Date of samples
e) Sample generic name
f) Sample description
g) Building location
h) Specification Section name
i) Space for Consultants' review notes and acceptance
j) Space for CBK review Notes and remarks
k) Acceptance

Large Samples: Samples of a bulky nature may be kept on site for review with a request for review made to the appropriate reviewer.

Sample Room: The Contractor shall provide on the site a designated Sample Room

C2: CBK - Official

Sample display and store

The Contractor shall allow under this item for construction of a lockable space for storage of approved samples.

As built drawings

The Contractor including all the sub- contractors shall engage competent drafting staff to prepare "As-built drawings" in AutoCAD, Revit by Autodesk, or any other approved specialist design software to consultants' approval: copies shall be shared electronically in both editable and non-editable format for the Consultant's interim approval prior to final submission. As-built drawings shall show all work above and below ground, with any corresponding identification, where applicable. Drawings shall be to scale of 1:100 for general layout drawings, 1:250 for Site Plans and 1:10, 1:20, 1:50 for details or any other scale as directed. As-built drawings shall indicate all services installations as executed on site. All drawings shall be accurately dimensioned and clearly detailed including all relative inverts and levels, valves, stopcocks, changes in direction, points of access, junction fittings, sizes, flow capacity and other relevant information. Submission of these As-built drawings" is a condition precedent to achieving substantial completion and issuance of respective certificate and shall be provided together with Operation and Maintenance Manuals. The as-built drawings shall form the basis for recording the locations of all services including but not limited to the following: Ring main for power reticulation Water supply (including cocks, ties, branches, valves etc.) Stormwater (including pits, inverts, etc.) Sewerage (including pits, I.O's inverts, etc.) Fire Service (including control valves, etc.) Underground Electrical Supply Cables Conduits cast into slabs Lightning protection ICT Installations Any other services installed by the Contractor and subcontractors.

Shop drawings

The Contractor shall prepare for review and approval by the Consultant and CBK detailed shop drawings generated in AutoCAD and Revit by Autodesk, or any other approved software including shop drawings for all specialist works by domestic sub-contractors. Following the Consultant's review of the shop drawings the Contractor shall immediately make the necessary amendments and resubmit for approval. The Contractor shall issue to the Consultant a soft copy and four printed copies of the approved shop drawings for use and transmission to CBK. The scrutiny of shop drawings by the Consultant shall be for general conformity, including conformity with the work of others and to co-ordinate the contract work in space. Such approval shall not imply any further indication of correctness. The Contractor shall obtain and check the manufacturer's shop drawings, certified prints, and other pertinent data for conformance with all requirements of the Drawings and Specifications in ample time to permit satisfactory progress of the work. After completion of such checking and verification by the Contractor, the Contractor shall sign and stamp such drawings, which stamp shall state as follows:

Specification Section/Drawing Number: …….

Checked By: (Contractor Name) ……..

Signed by: (Consultant's Name) ……

Enough shop drawings and review data shall be submitted to the Consultant and CBK. Sufficient time for the review of all shop drawing submittal shall be allowed in Contractor's schedule. The Contractor and Sub-Contractor shall provide As-Built drawings in all the specialist services on practical completion of works

C2: CBK - Official

Warranties

The Contractor including all the sub-contractors shall allow for warranties to commence from date of certificate of substantial completion in accordance with the manufacturer's specifications

Operation and maintenance manuals

General: Submit operation and maintenance manuals for installations where requested in the Contract Documents, including but not limited to the items listed below: Maintenance manuals for corrosion protection - Structural steel finishes: Information: Submit Operating & Maintenance Manuals that contain the following details:

a) Scope of work carried out- Application methods
b) An inventory of installed components listing type and manufacturer
c) An inspection, testing and maintenance program in tabular form showing the frequency and the level of routing attentions required throughout the life of each component
d) Manufacturer's literature on all component provided
e) A list of relevant applicators giving addresses and contact telephone numbers
f) Maintenance manuals
g) An inspection, testing and maintenance program in tabular form showing the frequency and the level of routing attentions required throughout the life of each component

Procedures for operation and emergency conditions, where applicable Safety features and controls, where applicable

An inspection, testing and maintenance program in tabular form showing the frequency

Maintenance spares & tools

Spares shall be supplied as additional material and/or equipment for use by the CBK after the 12 months Operation and Maintenance period and shall not be used during this period for replacement of faulty materials or equipment except on approval by CBK and installed or replaced free of charge and a replacement stock procured. Spare components and materials required to be provided shall be procured, securely packaged and/or boxed, identified with suitable labelling and any cross reference to relevant drawings and delivered to CBK prior to and as a condition of the issue of the Notice of substantial completion. Register: Spares register with all relevant identifying information shall be maintained and provided to the Consultant and CBK in an approved electronic spreadsheet format using Microsoft Excel or any other software as directed. The latest version of spares register shall be submitted to the Consultant and CBK together with the documents required for substantial completion.

Minimum requirements at substantial completion

The Contractor shall have completed the Works, including the following items before the issuing of a "Notice of Certificate of Substantial Completion. External Cleaning: The Contractor shall Clean out manholes, pits, sumps and drains, remove debris, nails, washers and other foreign matter from external floor slabs and sweep free of metal shavings and dust Thoroughly clean all works, , taking great care not to scratch or damage the surfaces; any scratched or damaged surfaces will be required to be repaired or replaced at the Contractor's cost, clear debris any scratched or damaged glass will be required to be replaced at the Contractor's cost Remove all hoardings, fences and temporary buildings and structure The Contractor shall: Remove debris and surplus material, paying particular attention to concealed spaces such as plumbing ducts, lift wells, lifts wells,

C2: CBK - Official

cupboards and the like Thoroughly clean internal surfaces, including glass and mirrors strictly following the manufacturer's or supplier's printed instruction and paying particular attention to removing dust, paint, spots, finger marks, stains, excess adhesive, smears and other blemishes, taking great care not to scratch or damage the surfaces; any scratched or damaged surfaces will be required to be replaced at the Contractor's cost Remove labels, protective paper and the like from sanitary ware and other items Ease doors and operable windows, adjust oil and clean hinges, locks, closers, floor springs and other hardware Check locks for satisfactory operation as appropriate and arrange for immediate remedial action where keys do not operate Account for all keys delivered to the site and pay for the supply and installation of all lock cylinders and keys where the full complement of keys cannot be produced Systematically label keys with stamped metal or plastic tags and hand over to CBK, clearly

Existing property and environment

The Contractor shall take every precaution to avoid damage to all existing property including roads, cables, drains, other services, landscaping and will be held responsible for all damage thereto, arising from the execution of this Contract, and shall make good all such damage when directed at the Contractor's own expense. The Contractor will be required to install vehicle cleaning system for all construction site entrances and exists

Business continuity

The site is a live environment with operations and the Contractor must make all efforts to ensure minimal disruption, noise, etc., during the construction of the Works. The contractor must thoroughly understand CBK operations that could be affected by the planned works, including security protocol, transport & logistics, administrative, and operational aspects of the organization. Special attention must be paid to sensitive areas and critical service zones (currency areas, Data Centres, server rooms, banking hall, etc.) to ensure no disruptions occur to essential services. Areas demarcated as restricted areas must remain operational and are off-limits to contractor staff unless authorised. Movements between approved zones must follow the approved planned pathways. Noise, Dust, Debris and Obstructions: The Contractor shall at all times take all reasonable steps to minimise nuisance to residents and occupiers of the surrounding properties and others (including nuisance from noise, dust, debris and obstructions) arising from the Works and shall promptly comply with all reasonable requests from such persons for the cessation of such nuisance. The Contractor shall comply with the provisions of local authorities in observing this clause. The Contractor is to notify CBK in advance of planned activities with excessive noise and dusty activities. Steps to reduce noise to include but not limited to: Delivery of raw materials to site to be done only during the day Noisy tasks takes place at day time only Use of serviced vehicles and machinery is also expected to reduce noise levels Notify the staff/security of the intended works prior to beginning construction. Ensure that noise & vibration levels emanating from machinery, vehicles and noisy construction activities (e.g. excavation) are kept at a minimum for the safety, health and protection of workers within the vicinity of high noise levels and nearby communities. Maintain the construction equipment in good working conditions as per the operation manual. Construction workers should be aware of the sensitive nature of work place they are operating in and advised to limit verbal and other forms of noise. Contractor will coordinate to determine timing and more importantly what specific noise controls and mitigations may be needed (beyond standard construction measures) Mitigation measures against air pollution to include but not limited to:

Choose manual demolition methods as the dust produced will be less; this has an added advantage of enabling the recovery of as much scrap as possible.

Sprinkle water on dusty materials such as gravel, sand, ballast during offloading;

Speed limit on trucks that will be ferrying demolition material

The heights from which excavated materials are dropped will be controlled to a minimum practical height to limit the fugitive dust generation from unloading; and

C2: CBK - Official

All stockpiles of aggregate will be enclosed or covered entirely by impervious sheeting or sprayed with water so as to maintain the entire surface wet.

By using water-spraying vehicle upon the unpaved road, fly off dust can be prevented

Vehicles transporting materials that have the potential to generate dust will have properly fitting side and tail boards.

Materials transported by vehicles will be covered entirely by clean impervious sheeting, with the cover properly secured and extended over the edges of the side and tail boards to ensure that the materials do not leak from the vehicle.

Materials will also be dampened, if necessary, before transportation in order to prevent earth movement from the site due to construction activity and run of onto public road drains, the site will be inspected regularly.

On-site vehicle speeds will be controlled to reduce dust re-suspension and dispersion by traffic within the sites (Vehicle speeds shall be limited to a maximum of 20km/h).

Strict measures shall be applied for the handling of construction materials in powder form such as cement, lime, concrete additives, etc.

Excavation, handling and transport of erodible materials shall be avoided under high wind conditions or covered by tarpaulin while on transit.

Wet all access roads during hauling of construction material during dry days.

Maintain periodically all equipment and machinery as per the operation manual.

Mud: The Contractor is to ensure that vehicles leaving the site do not bring mud and the like on to adjoining streets. The Contractor is to provide a wash-down area adjacent to the site boundary vehicular exits to enable the wheels and other parts of construction vehicles to be cleaned of mud and the like prior to exiting the site and entering the adjacent streets.

Mosquito Control: The Contractor shall take all reasonable steps for mosquito control by ensuring that no ponding of water is allow to remain on the site that could cause the hatching of mosquitoes.

Worker’s Behaviour: The Contractor shall ensure that the behaviour of workers on the site does not offend the occupants of the adjoining buildings and streets, and shall remove from the site anyone whose behaviour is declared unacceptable.

Noise control and monitoring: The Contractor shall monitoring systems to visually check noise and air quality levels during construction. Mitigation measures should be implemented to prevent disturbances to occupants. Additionally, the Contractor should schedule noisy activities during times when the campus has the fewest occupants. It is imperative that all CBK operations remain fully functional and uninterrupted throughout the duration of the works. The site is a highly sensitive environment, requiring the contractor to operate with 100% sensitivity to the specific needs and intricacies of the CBK. The contractor must take every step to familiarise themselves with the operations, functions, and systems of the site, ensuring that their activities are conducted in a manner that preserves the integrity of the organisation’s critical work. The contractor shall allow a contingency plan of 20 calendar days for work stoppage due to unavoidable bank events. Special attention must be paid to sensitive areas and critical service zones to ensure no disruptions occur to essential services.

Protection of existing utility, services and property

Prior to commencement of any work the Contractor is to ascertain by own initiative the exact position, depth and level of all existing electric cables, water pipes or other services in the area and shall make whatever provisions may be required by the authorities concerned for the support and protection of such services. Any

C2: CBK - Official

damage or disturbance caused to any service shall be reported immediately to the Consultant and the relevant authority and shall be made good to their satisfaction at the Contractor's expense. The Contractor shall exercise utmost care and precaution to ensure that all existing CBK property and public utilities are well protected, and that business continuity is maintained during construction operations. Any damage to such property and utilities caused by the Contractor or Sub- Contractors shall be repaired or restored at contractor's cost to the satisfaction of the Consultant and CBK. In the event of any damage to existing site services caused by the Contractor's operations, the Contractor shall be liable for liquidated damages. The amount of liquidated damages shall be as evaluated by CBK team for each day the service remains disrupted, in addition to the cost of repairs and any other associated costs.

Stockpile materials for emergency repairs.

The Contractor shall maintain a stock of essential materials and equipment on-site to address any emergencies that may arise due to accidental damage to existing services. This stock shall include, but not be limited to, pipes, fittings, cables, and other relevant items necessary for immediate repair.

Statutory regulations and bye laws

The Contractor is to comply with all local regulations and by-laws of the Local Authority including serving of notices and paving of fees.

Materials, tools, plant and scaffolding

The proposed project is regarded by the Central Bank of Kenya as a high-level sensitive project, and it is expected that the quality of material and work is to be of the highest standard. All materials and workmanship used in the execution of the works shall be of the best quality and description unless otherwise described. Any materials for the works condemned by the Consultant and CBK shall immediately be removed from the site at the Contractor's expense. All such plant, tools and scaffolding shall comply with all regulations whether general or local in force throughout the period of the Contract and shall be altered or adapted during the Contract as may be necessary to comply with any amendments in or additions to such regulations.

Off-site storage of materials

Where storage of materials for the Works is required off-site, the Contractor shall ensure that the materials are insured in the name of the Central Bank of Kenya, stored in a secure undercover location, packaged or protected to prevent damage during delivery and storage, certified as belonging to the Central Bank of Kenya where payment for unfixed materials is sought, located close enough to the site to allow inspection by CBK, and secured in accordance with the Contract where early payment is required. Generally, payment for materials stored off-site shall not be allowed unless approved by CBK. The Contractor shall arrange for inspection by the Consultant and CBK of materials, components, and fabricated items at the relevant factories, warehouses, or other sources for quality-control inspection of samples, prototypes, testing, examples of custom-made work, and similar items.

Services coordinator

The Contractor shall employ a suitably experienced Building Services Co-Ordinator, who shall be responsible for the co-ordination of the installation, testing and commissioning of the building services. The Building Services Co-Ordinator shall ensure that coordinate all-services drawings are prepared which clearly demonstrates compliance with documented requirements, Coordinate Mechanical, Electrical, Plumbing, ICT, Security, and Fire Protection designs, Review drawings for clashes and conflicts, ensure compliance with uptime, applicable standards, Local building regulations, Client technical standards and chair MEP coordination meetings. The MEP coordinator shall coordinate installation of server racks , containment systems, overhead and underfloor services, Power Whips, Busbar systems, Fibre pathways and ensure Hot aisle/cold aisle design integrity, adequate airflow management, Required maintenance clearances; coordinate

C2: CBK - Official

Utility power systems, Transformers, generators, UPS systems, ATS systems, Busways, PDUs, Earthing and bonding etc

6.Co-ordinate the services inspection and handover processes. Co-ordinate the training of the Central Bank of Kenya's and/or operators"€™staff in the operation of the services systems. Co- ordinate the integration of the new systems with the existing systems to the satisfaction of the Consultant and CBK.

Public and private roads, pavement.

The Contractor will be required to make good at their own expense any damage they may cause to the present approach road surfaces during the period of the Works.

Police regulations

The Contractor is to allow for complying with all instructions and regulations of the Police Authorities.

Contractors' superintendence

The Contractor shall constantly keep on the Works a literate English-speaking Agent or Representative, competent and experienced in the kind of work involved, who shall give their whole time to the superintendence of the Works. Such Agent or Representative shall receive on behalf of the Contractor, directions and instructions from the Consultant and such directions and instructions shall be deemed given to the Contractor in accordance with the Conditions of Contract. The Agent shall not be replaced without the specific approval of the Consultant. It is to be a specific condition of this Contract that the contractor shall provide onsite throughout the period up to the date for Practical Completion a suitably qualified, experienced and competent person to ensure that the works are carried out to the standard required by the specifications and detailed on the Drawings; and shall ensure that upon any termination of employment a suitable replacement is found. The Consultant may interview the Contractor's proposed Representative.

Curriculum Vitae of past experience and qualifications. The personnel proposed for the works shall have relevant experience in similar works. CBK's decision will be final regarding the suitability of the proposed Representative.

Traffic arrangements

The designated routes and zones outlined form the foundation of a detailed traffic management plan, ensuring the safe and efficient movement of vehicles and pedestrians within the Facility. The Contractor will be required to agree the access route to the site with the Central Bank of Kenya before commencement of the Contract Works and must adhere to this route throughout the course of the Contract, unless agreed otherwise. All Temporary Roads must be constructed and maintained to ensure stability, reduce dust, and accommodate heavy vehicle with pedestrian routes and crossings shown designated for safe passage of personnel across traffic areas. These crossings will be supported by physical barriers and appropriate signage. The Contractor may be required to observe certain traffic rules and regulations pertaining to the use by their vehicles of the roads adjacent to the site. These rules and regulations should be investigated by the contractor at the commencement of the Contract. All traffic flow, as indicated on the routes, must incorporate: Speed limit enforcement zones. Clearly marked stop points at intersections. Emergency vehicle routes that are kept clear at all times. Temporary signage and lighting must be installed at all critical points identified in the diagram to guide vehicle and pedestrian movement safely.

C2: CBK - Official

Schedule of works

The contractor shall prepare and submit a detailed project schedule of works for approval by CBK and the Consultant in accordance with the Contract. The schedule of works is to be in a computerized format done in Primavera, Microsoft Project, or any other approved software or format. The schedule of works should clearly indicate the critical path, and the Contractor will update the schedule on a monthly and/or weekly basis during the course of the Contract clearly indicating the actual dates against the approved baseline dates. The schedule shall show in detail the construction time and order in which each section of the work is to be carried out and be sub-divided into elements, trades and tasks. The time schedule is to be agreed with the Consultant. At the end of each month the Contractor is to incorporate actual start and finish dates into the time schedule and produce a construction schedule update and analysis for the Consultant. The analysis is to show actual start and finish dates, identify out of sequence work, critical activities and any constraints which have or may affect the progress of the works. During the execution of the works the Contractor will incorporate any changes to the time schedule only if approved `in writing' by the Consultant arising for whatsoever reason and produce a revised schedule. The Contractor will provide the Consultant with soft editable copy of the time schedule including monthly updates and analyses together with four printed copies of the relevant data. Note: The contractor shall allow in the overall schedule of works, published holidays as per the annual calendar.

Sub-contractors' attendance

The Contractor shall provide general and special attendance to Sub-Contractors as required for the proper execution of the Sub-Contractor Works. General attendance shall include use of the Contractor's scaffolding while erected on site, provision of power, water, lighting, watching, sanitary accommodation, mess rooms, welfare facilities, space for offices, stores, plant, and materials, and clearing away rubbish produced by Sub-Contractors. Special attendance shall include taking delivery, meaning the provision of unskilled labour necessary to unload plant and materials received on site and place them within the Sub-Contractor's storage space or store, and hoisting, meaning the provision of unskilled labour and use of the Contractor's standing plant to assist in raising Sub-Contractor plant and materials to the required levels, but not placing them in final position.

GENERAL ATTENDANCE - The following services are described as "allow for general attendance"

a) Use, for the purpose of the Sub-Contractor Works of any scaffolding belonging to or provided by the Contractor while it remains so erected upon the site, provided that no warranty or other liability on the part of the Contractor or the sub-contractors shall be created or implied in regard to the fitness, condition or suitability of the said scaffolding.
b) Provision of power, water, lighting, watching and attendance for the purpose of the Sub- Contract Works
c) Use of sanitary accommodation, mess rooms and welfare facilities
d) Provision of space for erection of offices or stores or space for storage of plant and materials) Clearing away rubbish produced by them

SPECIAL ATTENDANCE. The following services are applied under a separate item and were described under the following headings shall mean.

a) "Taking delivery" shall mean the provision of unskilled labor necessary to attend upon the sub-contractor's workmen for the purpose of unloading plant and materials when received upon the site and placing in position within the Sub- Contractor's storage space or store.
b) "Hoisting" shall mean the provision of unskilled labor and the use of any Contractor's standing plant for the purpose of assisting the Sub- Contractor's workmen in hoisting the Sub- Contractor's plant and materials to the various levels but not placing in its final position

C2: CBK - Official

Water

The Contractor shall provide at their own risk and cost all water for use in connection with the Works including the work of sub- contractors; make arrangements with the Local Authority for the installation of a separate meter for all water used by the contractor throughout the Contract and pay all costs and fees in connection therewith. The Contractor shall also provide temporary storage tanks and tubing, etc., as they may consider necessary and clear away at completion. All tanks for permanent retention/incorporation shall not be used for this item. Alternatively, the Contractor may make separate arrangements at their own risk with the Central Bank of Kenya for the use of the water from the existing water supply on site and for paying all charges thereto including connection and consumption. No guarantee is given on the availability of water or its quality. No claims for lack of water or water pressure will be entertained. All water shall be fresh, clean and pure, free from earthy, vegetable or organic matter, acid or alkaline substance in solution or suspension. Water used in the mixing of concrete shall conform to BS EN 1008:2002-Mixing water for concrete Specification for sampling, testing and assessing the suitability of water, including water recovered from processes in the concrete industry, as mixing water for concrete.

Lighting and power

The Contractor shall provide at their own risk and cost all artificial lighting and power for use on the works, including all sub-contractors and specialists' requirements and including all temporary connections, wiring, fittings etc., and clearing away on completion, The Contractor shall pay all fees and obtain all permits in connection therewith. The Contractor may install their own generator on site with the approval of the Kenya Power Company Ltd. (K.P.C.) and the Central Bank of Kenya, if required. All such temporary works shall be cleared away on completion. No claims due to lack of electricity or due to power fluctuations will be accepted. All watching and lighting shall comply with the requirements of CBK and the Consultant.

Concrete tests

Benchmark and Testing of Concrete

NOTE: The Contractor must allow for all costs in connection with the making of the cubes, curing, transport, crushing by Local Authority and obtaining the test certificate: to BS EN 206 and BS 8500 Set of four 150 x 150 x 150 mm concrete test cubes in sufficient quantity as shall be directed by the consultant.

Other tests

The Contractor shall be required to carry Site Acceptance Tests (SATs) and other tests as shall be required during the execution of the works as directed. Testing shall include provision of power, water and all other consumables where required. Such tests shall be documented and copies submitted to the Consultant. Sufficient notice shall be given prior to undertaking designated tests requiring to be witnessed. 5 working days for site tests; and10 working days for local pre-delivery tests. The contractor shall allow for submission of samples for testing by approved independent specialist authority accredited to undertake testing works. Any tests undertaken on site shall use instruments calibrated by accredited authority. Tests shall include but not limited to the following:

Note: Testing and commissioning shall include all chemicals, power, fuel amongst other pre-conditions necessary to achieve the testing procedure. This will also include connections to existing systems. The contractor shall pay for all fees required for testing.

Site office, contractor's temporary buildings

The Contractor shall visit site, inspect any temporary structures, provide, erect and maintain temporary office accommodation having adequate lighting, furniture and fittings for their use and ample temporary watertight sheds for the proper storage and protection of materials and for the use of artisans. Storage of material within

C2: CBK - Official

the existing building will not be permitted without the written authority of the Consultant. Any storage so permitted must comply with any restrictions or conditions imposed by the Consultant. The Contractor shall also provide, erect a separate temporary office with a total floor area of not less than 15 square meters having adequate lighting, furniture and fittings and separate storage space for the exclusive use of the Sub-Contractors and Suppliers. The Contractor shall provide the necessary portable eco toilet facilities for staff and workmen both for the Contractor's and the Sub-contractors' at an approved location on site. The toilets shall be provided, erected and maintained to the requirements and satisfaction of the Central Bank of Kenya and Consultant and be kept at all times in a thoroughly clean and sanitary condition. The Contractor shall also provide, erect main temporary facilities for use by workers for washing, drinking water, first aid and shelter from rain, all to the approval of the Consultant and CBK. The Contractor shall allow for provision of non-alcoholic refreshments during the site meetings. Cooking and eating facilities for workers will not be permitted on the site without CBK's written approval. Facilities required including but not limited to: Fully furnished, serviced, cleaned and maintained offices and amenities that includes all provision of consumables such as tea, coffee, sugar, soap, detergent, toilet paper, healthy potable water supply, chilled/boiling water dispensers and the like Full air conditioning of office and storage spaces; thermostatically controlled with time switch Tea room provided with appropriate cutlery, crockery, glasses, microwave oven, hot plate, large refrigerator and dishwasher Appropriate serving trays, trolley, water jugs, thermos and the like for conferences Reception area with waiting chairs and a large coat cupboard for storage of visitors coats, umbrellas and the like.

Temporary structures

The Contractor shall allow for providing and clearing away on completion of the Works such as temporary hoardings, fencing, gates, planked walkways, guard rails, etc. may be necessary for the protection of the workers, occupants of the building and adjacent structures and for the proper execution of the Works. All such temporary structures shall be constructed with the approval of the Consultant and CBK's full satisfaction and in such a manner as to cause minimum inconveniences and disturbance to pedestrians and road users using the adjacent roads. All such temporary structures shall comply in all respects with the National laws, rules and regulations currently in force and applicable to such structures. All temporary structures shall be erected in a manner so that the unloading or loading of materials causes minimum obstruction to the use of adjacent roads and other facilities.

All temporary structures shall be kept properly lit throughout the periods of darkness and any corners or projections shall be painted white.

Temporary structures shall not be used or permitted to be used for advertisement purposes except with the consent of the Consultant.

All temporary structures shall be always maintained in good order and condition to the satisfaction of the Consultant.

All temporary structures shall be removed when so required by the Consultant or at the end of the period for which it is required. The Contractor shall indemnify and shall keep CBK indemnified against any expense, loss, claim or in connection with the temporary structures

Telephone

The Contractor is not required to provide for a telephone but may do so for at their convenience and pay all costs and changes in connection therewith.

C2: CBK - Official

Adverse weather conditions

The bidder is referred to monthly historical data and records of weather patterns recorded by Kenya Meteorological department for the last 10 years (Home Kenya Meteorological Department) Contractors Method Statement and Programmed should reflect how the wet seasons envisaged during the contract period by the Kenya National Meteorological department at the time of bidding, will be accommodated within the contract period. The contractor shall, in addition, make a reasonable estimate of recovery time in overall programmed, following adverse rainfall, including but not limited to mopping up removal of water from excavations and trenches “Adverse Weather Conditions" shall mean weather conditions that are severe, unusual, and unexpected

Temporary disposal of rainwater

The Contractor shall provide and maintain all necessary temporary gutters, downpipes, chutes, drains, etc. for conveying rainwater from the buildings. The Contractor shall allow for temporary drainage, pumping and piping for keeping the premises and site free from accumulation of water at all times.

Site photographs

The Contractor shall seek approval and allow for taking digital site photographs on a weekly basis to the satisfaction of the Consultant. Soft copies of the photographs shall be provided to CBK and the Consultant. Hard copies shall be filed in a clean project album supplied by contractor on site and handed over to CBK on completion of the project Note: CBK is a restricted site and therefore the Contractor shall strictly observe security guidelines while taking photos. Photographs outside of the construction site shall not be allowed.

Sign board

The Contractor shall provide and erect where directed and maintain during the whole period of building operations and remove at completion, one approved temporary notice board to the Consultant's standard design and giving a brief description of the Works and showing the names of the Central Bank of Kenya, the Consultant and the Contractor with sufficient space to append the names of Nominated Sub-Contractors and Suppliers when known. The lettering concerning the Consultant is to be not more than 50mm high.

Contractor's report

The Contractor shall provide to the Consultant progress report on a weekly and monthly basis (or as directed by the Consultant) for onward transmission to CBK. The Contractor's report shall be in approved format, and shall include project overview, progress charts, milestones, deliveries to site, achievements and any challenges in period under review. The report shall further provide weekly look-ahead, testing results, labor and equipment statistics, approved project photographs, Quality Assurance & Quality Control (QA/QC) documentation, list of notices, claims, safety statistics, environmental statistics, comparison of planned and actual progress, matters arising, early warning, log of Request for Information (RFI) & Request for Approvals (RFA) together with any mitigation measures for any delays.

Other CBK contractors and contractor’s specialists

The Contractor shall accept responsibility for providing the following services for direct contracts and specialists as before described:

GENERAL ATTENDANCE.

The following services are described as "allow for general attendance”:

Use, for the purpose of other CBK contractor's Works of any scaffolding belonging to or provided by the Contractor while it remains so erected upon the site, provided that no warranty or other liability on the part of the Contractor or other CBK contractors and contractor's specialists shall be created or implied in regard to the fitness, condition or suitability of the said scaffolding;

C2: CBK - Official

Provision of water, lighting, watching and attendance for the purpose of the direct contractors and contractor's specialists.

Use of sanitary accommodation, mess rooms and welfare facilities.

Provision of space for erection of offices or stores or space for storage of plant and materials.

Clearing away rubbish produced by them.

SPECIAL ATTENDANCE. The following services are stated under a separate item and were described under the following headings shall mean;

"Taking delivery" shall mean the provision of unskilled labor necessary to attend upon the supplier's workmen for the purpose of unloading plant and materials when received upon the site and placing in position within storage space or store;

"Hoisting" shall mean the provision of unskilled labor and the use of any Contractor's plant for the purpose of assisting other CBK supplier's workmen in hoisting their plant and materials to the various levels but not placing in its final position.

"Providing Power" shall mean the provision of power during the course of the Works and during the period of maintenance.

Protection of work

The Contractor shall cover up and protect all finished work from damage including provision of temporary plywood or polythene sheet. In the event of any damage occurring to the Works, materials, fiber cables, power cables, security infrastructure, sewer line, drains, gullies, paths or other works on the site in temporary possession of the Contractor for the purpose of this Contract, either from the weather, want of proper protection, defects, or insufficiency of the Works or any other cause whatsoever during the progress of the Works, the Contractor alone shall be responsible and shall without extra charge, immediately make good all damage and pay all costs which may be levied.

Local regulations and by-laws

The Contractor is to comply with all local regulations and by-laws of the Local Authority including serving of notices and paying of fees particularly any works outside CBK Facility. However, the contractor shall liaise with CBK with regard to this requirement.

ISS GENERAL DESCRIPTION

General

This chapter describes the main components of the Integrated Security System (ISS) and its functional operation. Following chapters will detail the technical specifications of each of the ISS components.

The ISS shall include the following security sub-systems integrated together into single comprehensive security system:

a) Physical Security Information Management (PSIM) system.
b) Electric Fences.
c) CCTV cameras.
d) Video Management System (VMS).
e) AI analytics solutions.

C2: CBK - Official

f) Access Control System (ACS).
g) Intrusion Detection System (IDS).
h) License Plate Recognition (LPR) system.
i) Under Vehicle Screening System (UVSS).
j) Intercom system
k) Public Address (PA) system.
l) Visitors management system.
m) Physical barriers (Including gates and anti-ram barriers).
n) Local Control Rooms (LCR's)
o) Main Security Center (MSC) and Secondary Main Security Center (SMSC)
p) Dedicated Data Communication Network (DDCN) for security
q) Cyber security platform.

The ISS will operate as a multi-site system, with all sites interconnected via the CBK's WAN, which will also serve security communications. The responsibility for establishing and maintaining communication between the sites and the Main Security Center (MSC) shall lie with CBK.

The ISS will be centrally managed via the PSIM software platform. The system architecture shall follow a federated topology, where each of the sites maintains local control of its security systems while reporting to the central PSIM for monitoring, coordination, and incident management. This topology shall ensure continued operation at each site in the event of WAN or central system outages, while providing centralized visibility, control, and scalability across all sites.

While maintaining the federated topology, the ISS shall be designed according to a hierarchical architecture, comprising multiple levels of control centers. The hierarchical topology of the ISS will be implemented across the following three levels:

a. Local Control Rooms (LCRs): Each site shall have a Local Control Room responsible for direct management of all security systems on-site. The LCR shall ensure autonomous operation in the event of network or central system failure.

b. Main Security Center (MSC): The Main Security Center shall provide centralized oversight, strategic management, and cross-sites coordination. It shall have full visibility of all LCRs enabling organizational-wide monitoring, reporting, and decision-making.

c. Secondary Security Control Center (SMSC): The SMSC shall serve as a backup to the MSC, providing centralized oversight, strategic management, and cross-sites coordination in the event the MSC is unavailable.

The figure below presents a high-level representation of the ISS architecture.

C2: CBK - Official

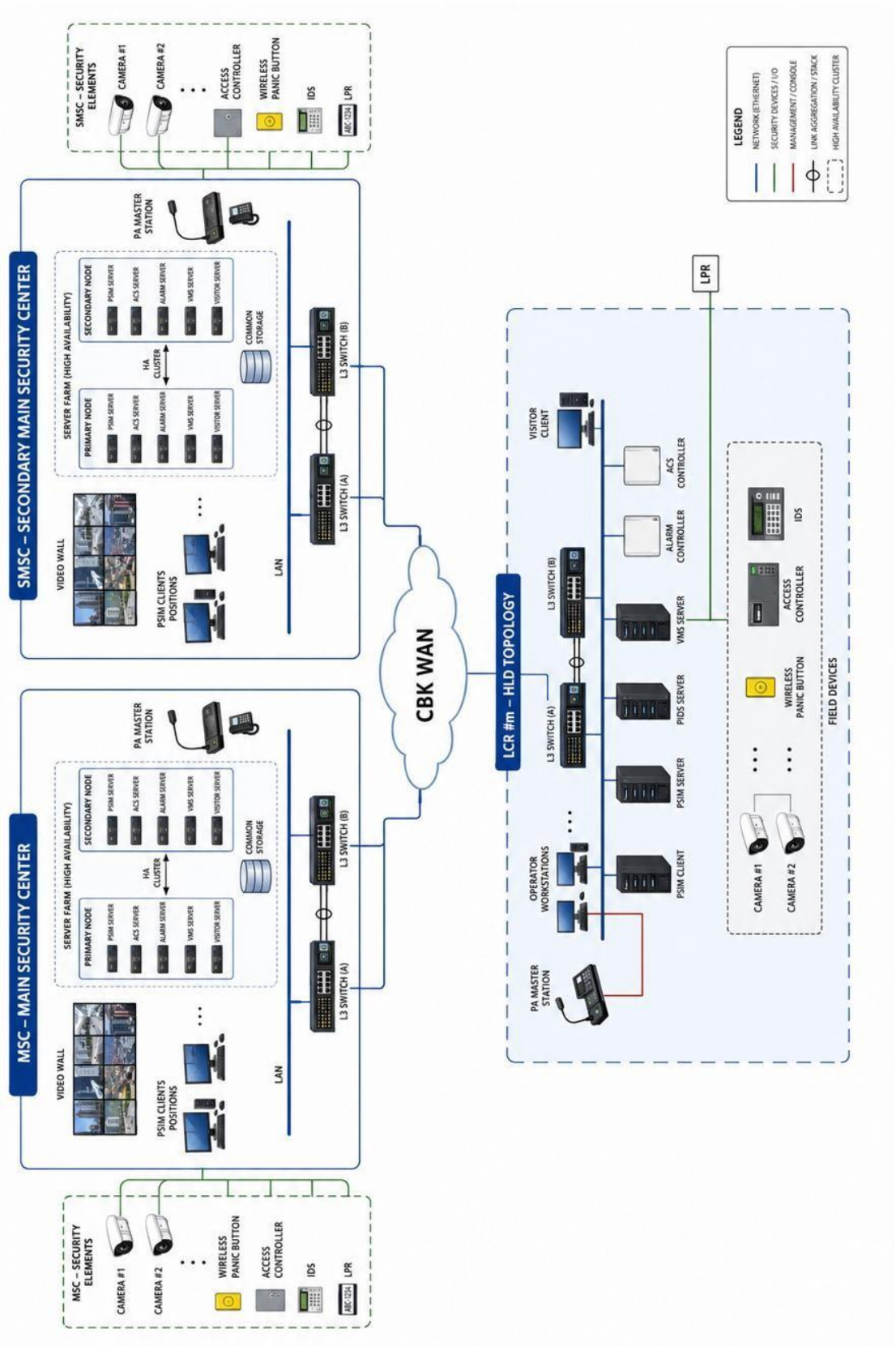

FIGURE 1 - ISS ARCHITECTURE

The figure below presents a high-level representation of the ISS architecture in the individual sites:

C2: CBK - Official

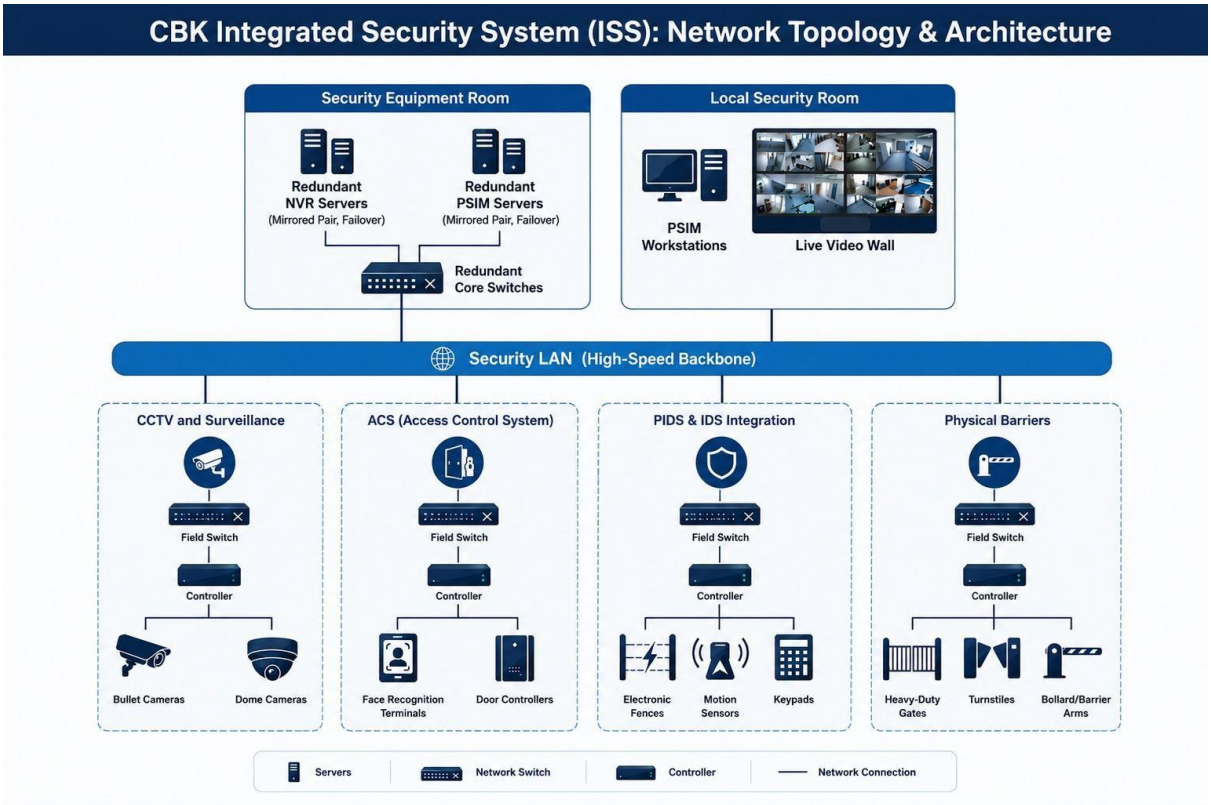

FIGURE 2: LOCAL SITES ISS HIGH LEVEL ARCHITECTURE

PSIM

The ISS shall be centrally operated and managed via a common database and a Physical Security Information Management (PSIM) software platform installed on the workstations and servers at the LCRs, MSC, and SMSC.

The PSIM platform shall serve as the primary system for events, alarms, situation management, and overall control of the security systems.

The PSIM platform shall provide control room operators with a comprehensive and efficient tool for monitoring, viewing, operating, controlling, logging, and debriefing all ISS security subsystems through a unified GUI.

The architecture of the PSIM will be based on Federated architecture where each of the sites maintains local control of its security systems while reporting to the central PSIM for monitoring, coordination, and incident management. Alerts originating from the various sites shall be transmitted to the MSC and SMSC in accordance with predefined parameters and prioritization criteria (including, but not limited to, alert type and the response time frame allocated to the LCRs). The MSC and SMSC shall maintain supervisory authority over the LCRs with respect to the management and control of the local security systems, including, inter alia, the operation of cameras and the management of all ISS subsystems.

C2: CBK - Official

The PSIM platform will be GIS-based, providing a geospatial interface that displays all system components, devices, and events on interactive maps and floor plans. This enables operators to visualize and manage security assets and incidents in their real- world geographic and spatial context.

The PSIM software at each site (LCRs, MSC, and SMSC) shall be installed on two (2) separate physical servers operating in a failover configuration (Active – Active). System recovery time during failover shall not exceed five (5) seconds.

The PSIM servers will be installed in the respective server rooms and connected to the operator workstations in the control room through KVM extenders.

The proposed PSIM system solution required to:

a) Connect and manage diverse security subsystems (CCTV, ACS, IDS, PIDS, P.A, intercom, etc.) regardless of manufacturer or protocol.
b) Use open architecture and standard communication interfaces (e.g., ONVIF, OPC, Modbus, BACnet, etc).
c) Provide a single command-and-control interface.
d) Enable operators to view live videos, alarms, and device status from all integrated systems.
e) Allows control actions such as unlocking doors, acknowledging alarms, or switching camera views.
f) Automatically correlate events from multiple systems (e.g., door forced + motion detected = possible intrusion).
g) Support rule-based automation to trigger predefined workflows or actions.
h) Present operators with step-by-step response instructions for each alarm or event type.
i) Combine data from all security systems with GIS/floor maps for real-time visualization.
j) Display device locations, event origins, and live camera feeds on graphical maps. k. Log all events, actions, and operator responses.
k) Enable incident reporting, timeline reconstruction, and audit trails for investigations.
l) Offer high availability through redundant servers (Active-Active or Active- Passive).
m) Includes role-based access, encrypted communications, and authentication mechanisms.
n) Generate multiple reports in various formats.
o) Display real-time system status via dashboards.

Electric fences

Electric fences are installed at several Project sites (including IMS, Kisii, Mombasa, and Kisumu). The existing electric fences are of various manufactures and models.

As part of the Project, the Contractor shall be required to integrate the existing electric fence systems into the ISS, ensuring that all status indications and alarms from the electric fences are displayed and monitored through the PSIM platform.

C2: CBK - Official

CCTV system

The CCTV system shall comprise Dome, Bullet, PTZ and Thermal cameras. All cameras shall be IP-based, with a resolution of either 5 MP or 8 MP (except for PTZ and Thermal cameras), as appropriate for the designated Area of Interest.

All cameras shall feature advanced, edge-based AI processing. Metadata generated by the edge AI shall be compliant with ONVIF Profile M for seamless VMS integration.

The cameras shall be installed - according to type - in the following locations:

a) 5 MP AI Bullet cameras– shall be installed along the perimeter barriers, in entrances, gates, and outdoor sensitive locations.
b) 5 MP AI Dome cameras – shall be installed in indoor locations such as communication rooms, server rooms, corridors, banking halls, and other sensitive areas.
c) 8 MP AI Bullet and Dome cameras– shall be installed in internal sensitive rooms such as strong rooms, loading bays, bricking rooms, bank notes processing halls, data centers, etc.
d) 4 MP PTZ cameras – shall be installed to provide coverage of sensitive outdoor locations such as perimeter barrier and adjacent streets.
e) Thermal cameras – shall be installed along the perimeter of the IMS.

The cameras shall be compliant with NDAA requirements and shall incorporate robust cybersecurity features. All cameras shall support ONVIF Profile S/G/T/M. The Contractor is required to provide ONVIF Profile S/G/T/M Compliance. The Contractor shall attach to their proposal official ONVIF verification documents for all proposed cameras and VMS software. This verification shall include the official ONVIF Declaration of Conformance (DoC) and the generated Feature List Document for each specific model and firmware version. Additionally, all proposed products must be actively listed in the official ONVIF Conformant Products database at the time of submission.

Video Management System (VMS)

The Video Management System (VMS) shall be an enterprise-class platform providing centralized and distributed management of video resources across all sites within the system. Access to video and related information shall be controlled based on user roles and site-specific permissions.

The system shall support a multi-site architecture enabling local recording at individual sites (implemented in an N+1 redundant configuration) while maintaining centralized access and management capabilities from designated control centers.

The system shall support recording capabilities at both the MSC and SMSC in addition to local site recording (for selected number of cameras).

C2: CBK - Official

Users at central control centers shall be able to access video from all sites, while users at individual sites shall be restricted to their respective site resources, based on defined access privileges.

The VMS shall be scalable and capable of supporting expansion to additional sites, cameras, and users without requiring fundamental changes to the system architecture.

The VMS solution must support ONVIF M profile, enabling smart integration with cameras. The integration with the AI cameras shall enable the VMS system to receive alerts and metadata from the cameras and to perform advance research including forensic search.

The system shall support integration with advanced video analytics and metadata sources, enabling enhanced search and event-based retrieval capabilities.

The contractor shall ensure full end-to-end integration and compatibility between the proposed VMS search interface and the camera's edge-AI analytics, using native plugins if required, to guarantee that all specified forensic search attributes are fully functional without any data loss. The cost of all required plugins, integration software, or dedicated search servers shall be fully included in the base price of the camera video channel license or the core system software. No additional or hidden licensing/ hardware/ integration fees shall be charged for the activation and operation of the specified forensic search capabilities.

The system shall ensure secure communication between system components and support industry-standard cybersecurity practices to protect video data and user access.

The conceptual description of VMS architecture at local sites is provided in the following figure:

C2: CBK - Official

FIGURE 3 - VMS ARCHITECTURE AT LOCAL SITES

The conceptual description of VMS federated architecture is provided in the following figure:

C2: CBK - Official

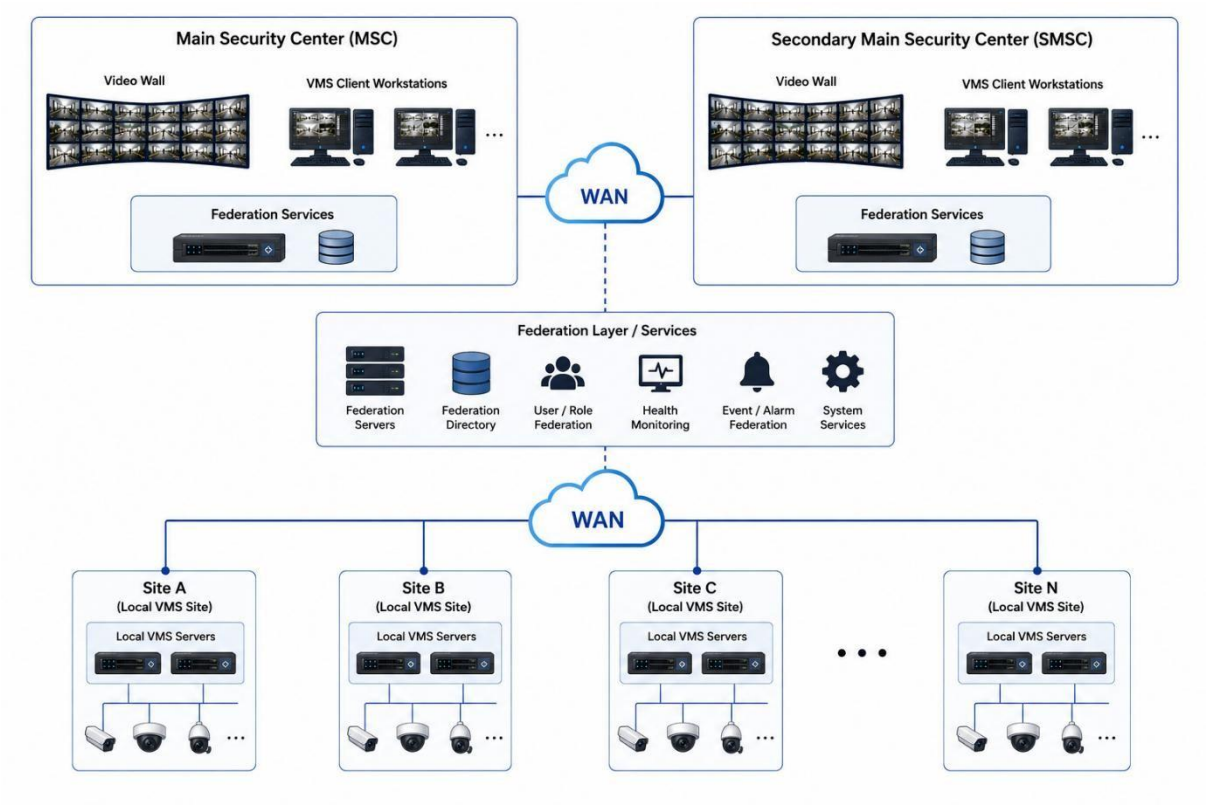

FIGURE 4: VMS FEDERATION ARCHITECTURE

AI

analytics solution

An AI-based video analytics solution shall be deployed at selected locations to support advanced outdoor security applications.

The solution shall be designed for operation in harsh outdoor environments, with the capability to reduce false alarms caused by environmental conditions such as rain, fog, snow, shadows, moving vegetation, and wildlife.

The system shall provide advanced behavior analytics for perimeter protection, including classification, detection of intrusion into sterile zones, loitering in restricted areas, and directional movement violations.

The AI solution shall be fully integrated with the central Video Management System (VMS), enabling real-time event generation and automatic operator notifications upon detection of defined rule violations.

The solution shall be based on an on-premises AI server architecture deployed at each applicable site.

Access Control System (ACS)

The proposed Access Control System (ACS) shall be a commercial off-the-shelf (COTS) solution, supported by qualified contractors trained and approved by the manufacturer. Proprietary or closed systems that restrict

C2: CBK - Official

maintenance, expansion, or support to a single vendor or contractor shall not be accepted.

The ACS solution shall be an enterprise-grade platform designed to support large- scale, multi-site deployments and to provide a scalable foundation for future expansion of sites, users, and system components.

The system shall be based on a centralized enterprise architecture, with a Main Security Center (MSC) providing overall system supervision and management of multiple remote sites. Remote sites shall operate with a degree of local autonomy while remaining part of the overall enterprise system.

Remote sites shall operate as logically segregated environments, ensuring that users and administrators at one site cannot access or modify another site's data, configurations, or permissions unless explicitly authorized. Authorized MSC users shall be able to enroll users, manage credentials, modify access rights, monitor events, and administer all sites according to their assigned privileges.

The system shall provide the capability for both centralized and local operational management, including user administration, system monitoring, and reporting functions, in accordance with defined roles and access permissions.

The system shall support coordinated data management across all sites, including synchronization of data between the MSC and remote locations.

The system shall support an open architecture, enabling integration with third-party devices and systems, including access controllers, readers, and electronic locking devices.

The system shall support integration with external PSIM platforms, enabling interoperable exchange of information and control between systems in a secure and coordinated manner.

C2: CBK - Official

The ACS architecture is shown in the figure below

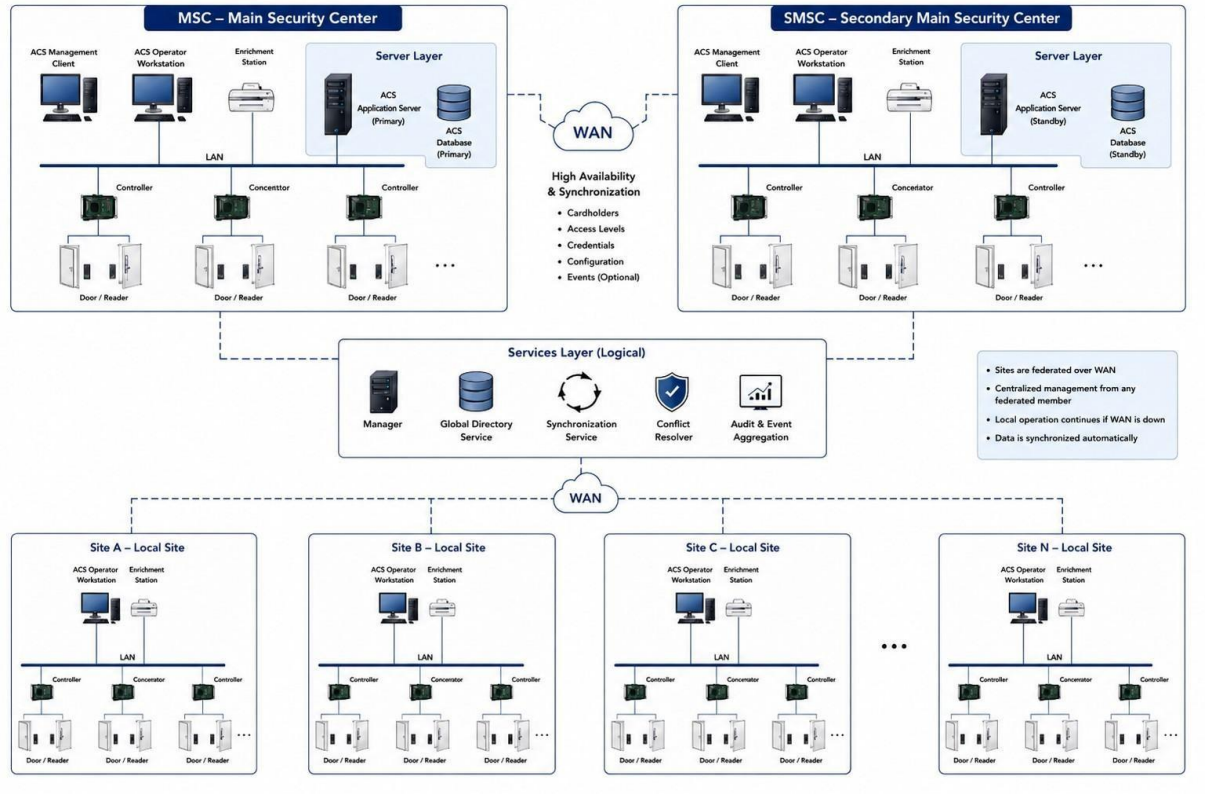

FIGURE 5 - ACS ARCHITECTURE

C2: CBK - Official

Intrusion Detection System (IDS)

The IDS will consist of two sperate systems:

a) An IDS based on DT sensors, to be installed in various rooms across the sites. b. An IDS based on seismic sensors, to be installed in strong rooms.

All system components shall comply with Grade 3 certification.
The IDS will be integrated with the PSIM. Management will be optional both locally and from the MSC and SMSC.

License Plate Recognition (LPR) system

The primary function of the LPR system shall be to record the license plates of vehicles entering the sites. The system shall not be used for automatic gate opening or access control.

The system shall have a centralized architecture, with all system servers and databases located at the corporate Main Control Center (MSC), while management functions shall be accessible from both the MSC and from each local site through LPR clients.

Contractors may propose a solution utilizing the LPR modules of the VMS or PSIM platform, provided that it complies with the functional requirements specified in the LPR chapter of this specification.

The system must be capable of identifying all valid license plates approved by the Kenyan Ministry of Transport, including diplomatic or foreign, as well as military and police numbers.
The system shall support integration with the UVSS, ACS and PSIM.

Under Vehicle Screening System (UVSS)

The Undercarriage Vehicle Scanning System (UVSS) shall be installed at some vehicle gates, as specified in the Bill of Quantities (BOQ), to provide a clear and continuous view of the undercarriage of any type of vehicle.

C2: CBK - Official

Operation of the UVSS shall combine automated AI analytics with manual verification. The system shall automatically analyze the undercarriage and highlight potential threats on the screen, while the security guards conduct the final manual review of the video and imagery before clearing the vehicle.

The Undercarriage Vehicle Scanning System (UVSS) shall be integrated with the License Plate Recognition (LPR) system to compare the vehicle's undercarriage images to a database of known vehicle profiles or previously recorded scans in order to identify inconsistencies.

The system shall support automated decision-making features that initiate specific actions (e.g., redirecting the vehicle for further inspection) based on preset thresholds or conditions.

Intercom system

Intercom units will be installed on several doors at each of the sites. The system shall be based on Internet Protocol (IP) technology.

The system shall support multiple outdoor door stations communicating directly with a single, centralized Master station without requiring a central PBX server.
The system must be scalable to support addition of unlimited number of doors or master units.

Public address (PA) system

The public address system shall be based on an IP-based solution.

The system shall allow live or recorded announcements to be broadcast by zones or to individual speakers.

System management and configuration shall be performed through the VMS software, while live and recorded PA paging operations shall be executed via a dedicated desktop hardware control panel.

Anti-ram arm barriers

Some of the existing pneumatic bollards installed at the sites shall be replaced with anti-ram arm barriers, certified to K4 level.

The Contractor shall be responsible for dismantling the existing pneumatic bollards and removing them from the site, in accordance with instructions from CBK. Additionally, the Contractor shall fill the holes, compact the soil, and repair the asphalt or concrete surfaces.

Local Control Rooms (LCR's)

Local control rooms exist at each of the project sites. Typically, each room contains operator table, large viewing screens, workstations and other equipment typical to control rooms. Servers and recorders are located in dedicated server rooms.

C2: CBK - Official

The Contractor is required to dismantle and remove all existing equipment and to install the new systems and furniture's.

Main Security Center (MSC)

The MSC's complex physical space (envelope) will be located at a site in Nairobi as designated by CBK (within one of the sites included in the Project).

The Contractor is responsible for completing the interior finishes of the MSC complex, including painting, drywall installation, carpeting, light fixtures, and other items as specified in the Bill of Quantities (BOQ). Additionally, the Contractor shall install all MSC technological systems (hardware and software).

The MSC complex will include the following components:

a) Operations Center (OC).

b) Crises Management Room (CMR).

c) Supervisor / Duty officer room.

d) Technical Equipment Room (TER).

e) Operators' rest area.

Secondary Main Security Center (SMSC)

The SMSC will be located in the space of the Local Control Room of Kisumu Branch.

The SMSC will consist of a single operator consol with PSIM workstation. It will normally be unmanned.

Dedicated Data Communication Network (DDCN)

The MSC, SMSC and the remote sites shall be connected via CBK existing Wide Area Network (WAN) which is based on Fiber Optic connection.

The Contractor shall supply and install a Local Area Network (LAN) Detected Data Communication Network (DDCN) for security at each site, including both passive and active components.

At each local site there will be two (2) core switches interconnected via 10G interfaces using HP IRF or Cisco VSS technology or similar. These switches shall operate in an Active–Active configuration, allowing continuous operation even if one switch fails.

C2: CBK - Official

Each access switch shall be connected to both CORE switches, providing redundancy and enabling load balancing. This ensures that traffic can continue to flow even if one link fails.

Redundant links and intelligent switch technologies (IRF or VSS) will allow the system to automatically balance traffic and perform failovers without disrupting ongoing operations.

The conceptual design of the network backbone topology is illustrated in the following figure:

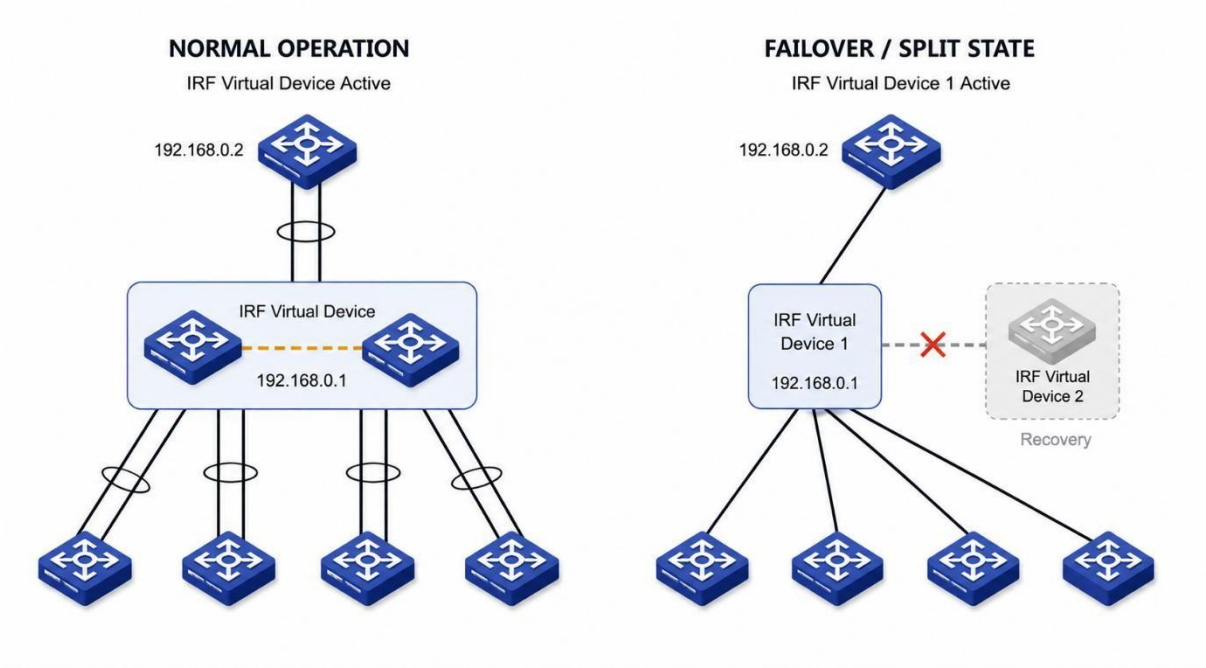

FIGURE 6 - DDCN TOPOLOGY

Cyber security

The ISS shall be protected against cybersecurity risks by dedicated software and hardware designed to provide complete visibility, protection, and threat awareness.

The cyber protection solution shall include the following key components:

C2: CBK - Official

a) Network Access Control (NAC) to control and monitor all devices attempting to connect to the network, ensuring only authorized and compliant endpoints can access critical systems.

b) Endpoint Detection and Response (EDR) to continuously monitor endpoints for suspicious activity, enabling real-time threat detection, automated response, and forensic analysis.

c) Security Information and Event Management (SIEM) to aggregate and correlate security logs from the network and endpoints, providing centralized monitoring, threat analysis, and incident reporting for proactive security management.

C2: CBK - Official

Existing equipment

Existing security systems and physical barriers are installed at all Project sites. The existing equipment includes PSIM servers, CCTV cameras, VMS and recording servers, ACS components (readers, cabinets, controllers, computers), IDS (detectors and controllers), PA (amplifiers and speakers), intercom systems, pneumatic bollards, arm barriers, electric fences, racks, communication cabinets, and network switches.

As part of the Project, the Contractor shall dismantle the existing equipment (including all cables and accessories) and remove it from the sites to approved disposal facilities. Controllers, servers and computers containing information and databases shall be delivered to the Client.

Integration phases

The Contractor shall implement the Project at each site in two (2) phases:

a) Phase A - establishment and commissioning of the core components of the new ISS system, including servers and software, comprising but not limited to the PSIM, VMS, virtualized environment, Access Control System (ACS), Intruder Detection System (IDS), Dedicated Data Communication Network (DDCN), and all associated infrastructure.

b) Phase B - dismantling of existing equipment and installation of new equipment, executed according to a detailed work plan to be submitted by the Contractor and approved by CBK SSD, ensuring minimal disruption to ongoing operations. The dismantling of existing equipment and installation of new equipment shall be done based on floors and zones and will be planned to preserve maximal operational capability of the existing system. For example, the Contractor will dismantle a number of field devices in a certain floor or area and will immediately – to the extent possible – will install the new devices and will connect them to the new ISS system.

The phased implementation approach is intended to ensure continuity of operations and maintain the full operational capability of the existing system throughout the installation and commissioning of the new system.

Equipment compliance and brand authenticity requirements

In accordance with the client's policy, all CCTV, video, communications, video management systems (VMS), command and control systems (PSIM), network equipment, and associated components must comply with NDAA requirements, pursuant to Section 889 of the U.S. National Defense Authorization Act (NDAA), including the prohibition on using technologies from banned manufacturers as defined by U.S. law and regulation.

C2: CBK - Official

All equipment shall be purchased from an official and authorized importer/distributor of the manufacturer, who is listed on the manufacturer's official website as an authorized distributor.

The supply of any Original Equipment Manufacturer (OEM) or white-label products is strictly prohibited; all equipment must be provided under the primary manufacturer's original brand

C2: CBK - Official

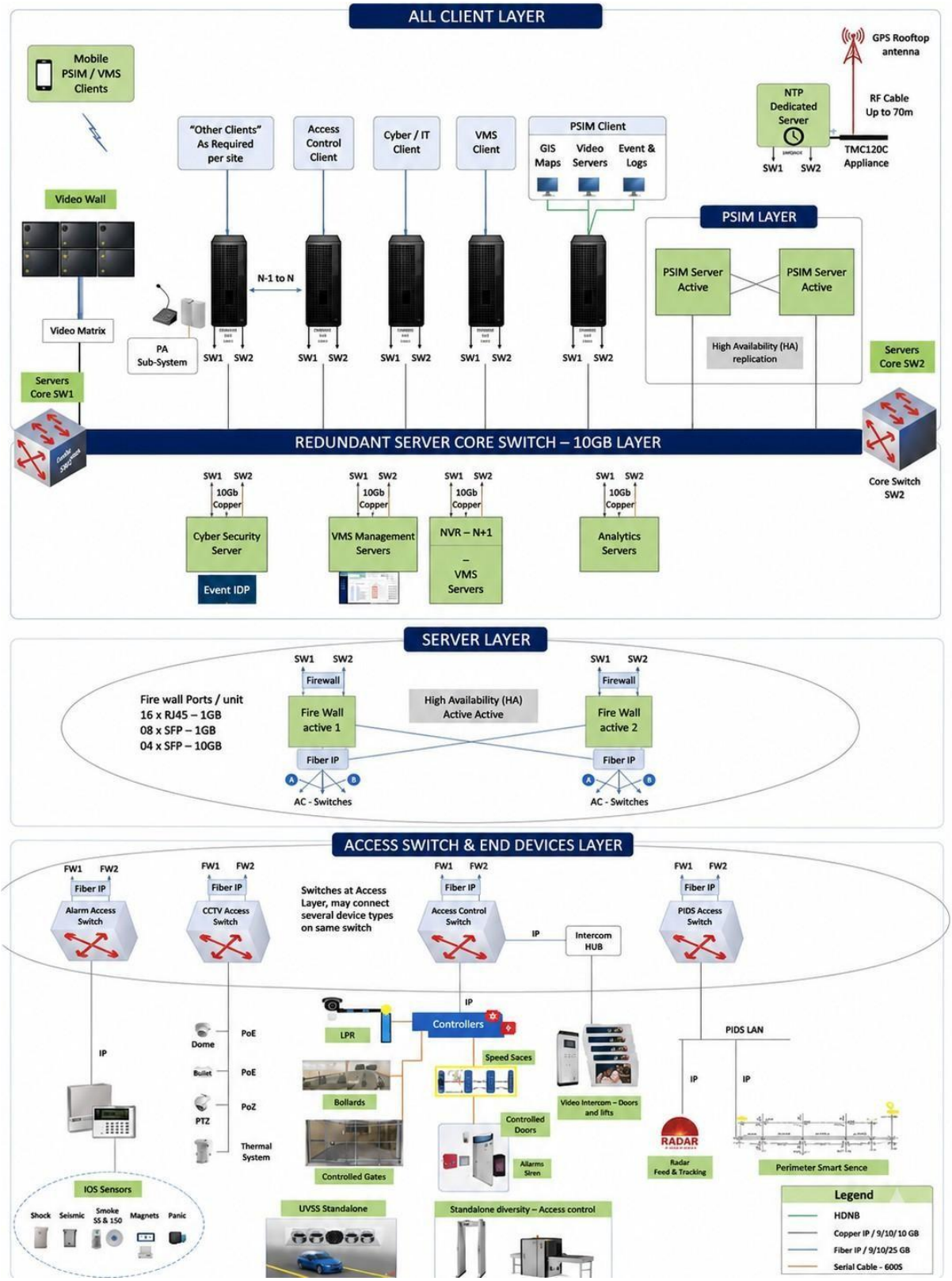

FIGURE 7: LOCAL SITES - HIGH LEVEL NETWORK ARCHITECTURE

Local sites - high-level network architecture

C2: CBK - Official

SCOPE OF WORKS

General

The scope of works required for project implementation shall include – but not limited - the following:

a) Preparation of the detailed design for the ISS system.

b) Procurement of all required equipment and materials.

c) Shipment, delivery, and storage of the equipment.

d) Manufacturing and supply of system components.

e) Installation of the system at all designated sites.

f) Execution of related infrastructure and civil works, as required.

g) System integration and configuration.

h) Execution of acceptance tests.

i) System commissioning.

j) Preparation and submission of all technical documentation.

k) Provision of training for system operators.

l) Provision of maintenance services (optional).

Detailed design

The system design presented in these specifications by the Consultant constitutes a high-level "systems engineering" design. It shall not, under any circumstances, be regarded as the detailed design of the system.

The Contractor shall be fully responsible for the detailed design of the system and for the preparation of all installation and implementation plans. As part of the detailed design process, the Contractor shall ensure the proper functionality and interoperability of all subsystems, and their integration into a unified and fully operational system, in full compliance with the requirements of these Specifications.

C2: CBK - Official

The detailed design and planning to be carried out by the Contractor shall include, inter alia, the following activities:

a) Design of all system components.

b) Electrical design of the system, including power distribution and control.

c) Mechanical design of all relevant equipment and assemblies.

d) Integration of subsystems into a fully operational unified system.

e) Definition and management of system interfaces.

f) Planning of installation works at all designated sites.

g) Cable routes, connection boards, wiring, bridging, and related activities. h. Planning of infrastructure, including pipes, ducts, and supports.

h) Planning of all necessary civil engineering works.

i) Any additional work required to ensure the complete installation, operation, and functionality of the system.

The detailed design shall be prepared by qualified engineers on behalf of the Contractor. All design work shall be based on proper calculations, specifications, and plans, and shall be duly signed and certified by the responsible engineers and the Project Manager.

The Contractor shall bear full responsibility for the quality, accuracy, and completeness of all design and planning work. Approval of any documents or plans by the Client shall not relieve the Contractor of responsibility for any errors, omissions, inaccuracies, or defects discovered at any time. The Contractor shall immediately rectify, at its own expense, any damage or deficiencies arising from such design defects.

The primary outputs of the Contractor’s detailed design shall be presented to the Client and the Consultant during a series of Design Review Meetings, in accordance with the project schedule and requirements.

Design review meetings

Preliminary Design Review (PDR)

C2: CBK - Official

a) The PDR shall be conducted within 30 working days from the date the Client issues the Work Order to the Contractor.

b) Seven (7) working days prior to the scheduled date of the PDR, the Contractor shall submit the PDR contents (in PPT & PDF formats) to the Client and the Consultant.

c) The PDR contents shall include, inter alia, the following subjects:

d) Description of the project structure, including key personnel, roles, and number of teams.

e) Block diagrams of the system down to the subsystems level.

f) Required approvals and permits necessary from the Client for system installation.

g) Initial list of proposed equipment, including a compliance table with links to specifications.

h) Gantt chart outlining project implementation milestones and timelines.

i) Preliminary Program Management Plan (PMP).

j) Any equipment or system proposed by the Contractor that does not meet the requirements of the Specifications and Appendices shall not be approved by the Client at its sole discretion. The Contractor shall propose alternative equipment that fully complies with all requirements until written approval is obtained from the Client.

k) Following the PDR, the Consultant shall issue a summary report including comments and required changes. The Contractor shall implement all design changes as indicated in the Consultants comments and obtain approval of the PDR.

Critical Design Review (CDR)

a) The CDR shall be conducted within 60 working days from the date of the Client approval of the PDR.

b) Seven (7) working days prior to the scheduled date of the CDR, the Contractor shall submit the CDR contents (in PPT & PDF formats) to the Client and the Consultant.

c) The CDR will cover, at least, the following topics:

d) Detailed Design of ISS topology.

e) Detailed design of sites (including installation drawings).

C2: CBK - Official

f) Description of architecture of sub – systems.

g) Block and single line diagrams.

h) Comprehensive description of interfaces and integration within the system.

i) Drawings of racks, communication and ACS cabinets.

j) Description of cyber security solution.

k) Topology of the DDCN.

l) Final selection of all equipment by producers and models.

m) Updated detailed Work Plan.

n) Program Management Plan (PMP).

o) Any equipment or system proposed by the Contractor that does not meet the requirements of the Specifications and Appendices shall not be approved by the Client at its sole discretion. The Contractor shall propose alternative equipment that fully complies with all requirements until written approval is obtained from the Client.

p) Following the CDR, the Consultant shall issue a summary report including comments and required changes. The Contractor shall implement all design changes as indicated in the Consultants comments and obtain approval of the CDR.

q) After the approval of the CDR, the system configuration shall be frozen, and the Contractor shall be authorized to commence execution of the works.

Factory Acceptance Tests (FAT)

a) The FAT shall be conducted on a date mutually agreed upon by the Client and the Contractor, but no later than 45 working days following the approval of the CDR.

b) The FAT shall verify the system's functionality and ensure compliance with the technical specifications.

c) The FAT shall be conducted at the Contractor's premises.

d) The Contractor shall submit the complete FAT procedure to the Client and the Consultant at least 10 working days prior to the scheduled FAT date.

C2: CBK - Official

e) The Contractor shall implement any necessary corrections identified during the FAT in accordance with the comments provided by the Client and the Consultant.

Project schedule and the Contractor work plan

Throughout the duration of the Project, the Contractor shall comply with the project schedule specified in the contract between the Contractor and the Client, or with the latest updated version of the schedule approved in writing by the Client.

Based on the Project schedule, the Contractor shall prepare and submit for the Client's approval a detailed work plan, including clearly defined milestones for each main task of the Project implementation.

The work plan shall be presented to the Client and approved at the PDR and CDR stages. The Contractor shall not commence installation works before receiving the Client's approval of the work plan.

The Contractor shall continuously update the work plan throughout the Project. In the event of any deviation from the approved work plan, the Contractor shall submit to the Client a detailed report outlining the reasons for the deviation, its implications on the Project, and the proposed corrective actions.

The Contractor's work plan shall include all the main milestones of the Project. For each milestone, the Contractor shall provide a written definition of the key tasks to be performed as part of that milestone.

The work plan shall be prepared in MS Project Gantt chart format, clearly illustrating how the Contractor will execute the work within the binding schedule specified in the contract.

The detailed work plan shall include, at minimum, the following milestones:

a) Preliminary Design Review (PDR).

b) Critical Design Review (CDR).

c) Factory Acceptance Test (FAT).

d) Submission of the installation plan for approval.

e) Submission of safety plan.

f) Commencement of on-site installations.

g) Submission of draft technical documentation for Client approval.

C2: CBK - Official

h) Completion of installations.

i) System commissioning and operational testing.

j) Acceptance testing.

k) Training.

l) Submission of final technical documentation.

m) Handover to the Client and commencement of the warranty/defects liability period.

Project management

The Contractor shall appoint a Project Manager (hereinafter "PM") who will be responsible for the overall implementation of the Project and shall serve as the primary point of contact with the Client. The PM shall have a minimum of five (5) years' experience in managing large-scale security and communication projects.

The Contractor shall appoint a Site Manager (hereinafter "SM"), who shall be responsible for all works at the site. The SM shall be with extensive experience in implementing large security and communication systems projects. The SM shall be continuously present on-site during the execution of all works.

The PM shall submit monthly progress reports to the Client. The reports shall include, at a minimum, the following:

a) Description of the actual status of the Project in comparison to the approved work plan.

b) Open issues requiring discussion and decision by the Client.

c) A list of critical problems along with recommended solutions.

The PM and other key Contractor personnel shall attend Periodic Progress Review Meetings, held as determined by the Client. The Client shall define the frequency, location, and content of such meetings.

Installation works

Installation works shall be carried out in accordance with the approved work plan, the installation dossier submitted during the CDR, and the installation sequence approved by the Client.

C2: CBK - Official

Installation works shall include the supply of all required auxiliary materials, including all necessary means and equipment, such as tools for working at height.

Electrical installations shall be performed only by certified electricians and in accordance with the latest version of the Electricity Law. Prior to commencing any electrical works, the Contractor shall provide certificates proving that the electricians assigned by the Contractor are certified and hold valid licenses under the Electricity Law.

Electrical installation works include the supply and installation of all power cables required to operate the equipment, from the Client's power connection point to all end units of the system. It is the Client's responsibility to provide a connection point; all other works and materials shall be supplied and executed by the Contractor at its own responsibility and cost.

The Contractor shall install all power cables between the Client's connection points and the equipment cabinets and items supplied by the Contractor. The Contractor shall install distribution boards and sockets on-site at locations pre-approved by the Client, as required for the supplied system.

The Contractor's scope of work shall include the supply and installation of all interconnection and bridging cables with connectors at their ends, to connect different types of equipment. This includes laying cables in conduits or tying them to cable trays, marking cable ends, connecting to junction panels, internal wiring in equipment cabinets, control desks, panels, etc., until full integration of all components into a fully operational system. Each cable shall be marked with a permanent, indelible indication of its start and end points. The marking content shall correspond to the detailed design and be approved by the Client or its Consultant.

Mechanical and electrical finishing works, such as painting touch-ups, mechanical reinforcements, cable bundling, labeling, sealing (against water, smoke, and pests), and all other works required to complete the installation in accordance with the specifications, shall be performed by the Contractor.

In all cases, unless otherwise specified, the installation works shall include all planning, manufacturing, installation, supply of installation accessories, cable routing, wiring, testing, commissioning, and any other actions required under the specifications, the contract, applicable standards, and laws (including safety regulations) to ensure that each equipment item operates correctly and fully in accordance with the technical specifications.

All equipment, materials, installation accessories, and other system components supplied by the Contractor shall comply with all relevant local safety standards and regulations.

Any changes caused by the Contractor during the Project to the infrastructure or to the equipment of the Client shall be immediately corrected by the Contractor and restored precisely to their original state to the satisfaction of the Client, at no additional cost, unless the Contractor has received explicit written authorization from the Client to perform such changes as an integral part of the Project.

C2: CBK - Official

Works at the Client premises

The Contractor shall perform all works at the Client's facilities in accordance with the existing procedures and rules in place, which shall be provided by the Client's representative upon receipt of the Work Order and prior to commencement of any on- site work, including evening and night shifts.

The Client shall have the right, at its sole discretion, to remove from the site any person employed by the Contractor without providing justification. The Contractor shall comply immediately with such request and shall not reassign the individual to the Project.

The Client shall not be obliged to provide any storage areas or offices for the Contractor. The Contractor shall be solely responsible for arranging such areas and offices, and for the security of all equipment and materials.

Detailed work procedures shall be determined with the Client prior to the commencement of on-site installations, and the Contractor must comply with these procedures.

The Contractor shall comply with all Client security, safety, and protection instructions, including those relating to entry into sites and buildings, presence therein, required cooperation, coordination of work phases, and work hours.

When connecting to existing systems, the Contractor shall ensure continued operation of the systems during all implementation works.

The Contractor shall carry out work within the hours designated by the Client and, as far as possible, without disrupting routine operations at the facility.

For the purposes of its work, the Contractor shall use only its own equipment, tools, and accessories and shall not use any Client-owned equipment.

The Contractor shall maintain cleanliness at the site during installation to the satisfaction of the Consultant. At the end of each workday, the Contractor shall remove all waste, leftover materials, and equipment to an authorized disposal site.

Where excavation or penetration through walls or partitions is required by the Client, the Contractor shall restore the wall or partition to the satisfaction of the Consultant upon completion of the work.

Any structural modifications made by the Contractor during the execution of the work shall be restored to their original condition prior to completion of the system installation.

Movement of the Contractor and its personnel within the facility shall be subject to the Client's approval, knowledge, and instructions.

C2: CBK - Official

The Contractor acknowledges that part of the work will be performed in the evening and at night and shall include these hours in its pricing. Evening and night works may include opening ceilings in public areas, while installation work on the floors may be performed during regular working hours.

Contractor technicians working on the core system (control rooms, software, equipment rooms, and switches) may be required to undergo a polygraph test as a condition of their assignment to the Project.

Safety and safety plan

The Contractor shall assume full responsibility and liability for supervising, directing, and ensuring compliance with all applicable laws, regulations, rules, guidelines, and other directives or procedures concerning workplace safety for all works related to the Project.

Prior to the commencement of on-site installation work, the Contractor shall submit a safety plan to the Client.

During the Project period, the Contractor shall provide, at its own cost, the following:

a. All necessary protective measures to prevent accidents, damage, or injury to persons and/or property in the site and its vicinity.

b. Any additional protective measures required by relevant stakeholders to ensure the safety and convenience of the public or others, including the Contractor's employees.

Should the Contractor fail to implement the required protective measures, the Client may require such measures to be provided and installed at the Contractor's cost and within the timeframe specified in the Client's notice. If the Contractor continues to fail in implementing the protective measures after such notice, the Client shall be entitled to employ a third party to provide such measures, with all associated costs bear by the Contractor.

The Contractor shall take all necessary precautions to ensure the health and safety of its personnel in accordance with applicable laws and regulations. The Contractor shall maintain records and submit reports regarding the health, safety, and welfare of personnel, as well as any damage to property, as reasonably required by the Client.

The Contractor shall appoint a qualified staff member (Safety Manager) on-site who will be responsible for the safety and protection of all personnel against accidents.

Sites drawings

The Client shall make all plans in its possession available to the Contractor.

It should be noted that the Client cannot guarantee the completeness of the drawings. In the event that the Contractor is missing a plan or part of a plan, the Contractor shall immediately notify the Client and proceed according to the Client's instructions. Such instructions may include a directive to prepare

C2: CBK - Official

drawings, and the Contractor shall be obliged to prepare such drawings at its own expense.

It is expressly clarified that the Contractor shall not use the plans for any purpose other than the execution of the Contract.

The Client may, from time to time during the execution of the works, provide the Contractor with additional instructions, including additional plans prepared or to be prepared by the Consultant. The Contractor shall carry out the works in accordance with such instructions and plan.

Protection of design materials

The Contractor shall establish, implement, and continuously enforce an information security management framework aligned with ISO/IEC 27001, including physical, technical, logical, and procedural safeguards, to ensure the confidentiality, integrity, and availability of all Client materials and all project-related design materials. No access shall be granted except to pre-authorized personnel, and all access shall be monitored, logged, audited, and revocable at any time at the Client's discretion.

All costs associated with the implementation, maintenance, and enforcement of security measures for the protection of project materials shall be fully borne by the Contractor. The Contractor shall not be entitled to seek reimbursement or make any financial claim against the Client for such costs.

The Client retains the right to visit the Contractor's offices to verify the implementation and effectiveness of such safeguards. Following such audits, the Client may issue instructions, and the Contractor shall be obligated to comply with all such instructions.

The Client may, at any time and at its sole discretion, issue requirements regarding the handling, storage, or protection of the design materials. The Contractor shall fully comply with such requirements in their entirety and at its own cost.

Design according to human factors principles

During the design phase, maximum attention shall be given to all aspects of human factors engineering to ensure ease of operation and maintenance of the system.

Mandatory considerations in terms of human factors shall include, but are not limited to:

a. Equipment placement to allow for convenient and easy operation.

b. Control and monitoring.

c. Easy access to equipment for convenient maintenance.

d. Minimization of occupied space.

C2: CBK - Official

e. Modular construction, allowing for easy disassembly and replacement.

Quality of work & equipment

The Contractor must ensure that the Project - from planning to commissioning - shall be executed in accordance with engineering best practices and a high standard of workmanship.

All equipment used by the Contractor shall be of the best quality available in the market. The use of unapproved equipment shall require the Contractor to disassemble and reinstall approved equipment, with all associated direct and indirect costs borne by the Contractor.

The Contractor shall employ professional personnel with the necessary knowledge and skills, in sufficient numbers to complete the Project in accordance with the required schedule.

The Client may request the replacement of any person employed by the Contractor on the Project who, in the Client's opinion, is unsuitable for the position. The Contractor shall comply immediately with such request and appoint a suitable replacement.

Manufacturing of "Non-Standard" equipment

Prior to manufacturing any item that is non-standard and specifically developed for this Project (such as operator panels, display panels, interconnection panels, etc.), the Contractor shall provide the Client with the technical specifications of the equipment. The technical specifications shall include detailed drawings, explanations, a list of parts, a list of components, and all other relevant technical details.

The drawings shall indicate exact measurements, markings, and standard numbers (where available). Technical data shall include packaging information, material types and their processing methods, thermal treatments, anti-corrosion measures, and other relevant information. Production may commence only after the Client provides written approval of the specifications.

This requirement shall apply, at a minimum, to the following items:

a. Command and control desks.

b. Gates and anti-ram barriers control panels.

c. Gates and bars.

d. Etc.

C2: CBK - Official

Replacements of specified equipment

The equipment supplied and installed by the Contractor shall be limited to items from the approved list of equipment submitted by the Contractor in its bid and the approved list at the CDR stage.

Any replacement of equipment during the Project shall be permitted only after obtaining the Client's written approval.

Commissioning

Upon completion of the system installation and its initial operation by the Contractor, the system shall be handed over to the Client for commissioning.

The commissioning period shall be thirty (30) days, during which the system must operate without faults. The start date of the commissioning period shall be coordinated with the Client.

In the event that any faults are detected, the commissioning period shall be extended as necessary until the system has operated for thirty (30) consecutive days without faults.

Acceptance tests

If the system has successfully operated for the entire 30-day commissioning period, as determined by the Client, it may be submitted to the Client for acceptance testing.

The scope and procedures of the acceptance tests shall be defined in the "Acceptance Test Procedure" (ATP) document.

Fifteen (15) days prior to the scheduled start of acceptance testing, the Contractor shall submit the ATP for the Client's approval. The ATP shall include a description of the test methods, required test equipment, procedures for recording results, and sample forms for documenting results for each item and the system as a whole, including detected faults and corrective actions taken.

The tests shall be performed by the Contractor in the presence of the Client's and the Consultant's representatives, in accordance with the test plan established by the Client and the Contractor. The Client shall acknowledge each test and its results by signing the corresponding form.

The Contractor shall provide all manpower, technical and administrative means necessary for performing the acceptance tests, including test equipment, instruments, auxiliary tools, test forms, and similar items. All equipment and tools shall be returned to the Contractor upon completion of the tests.

The Contractor shall provide the Client upon request, with all information in its possession required for the acceptance tests, including specifications, drawings, plans, technical data, and similar

C2: CBK - Official

documentation.

The Client shall commence acceptance tests only after the Contractor has conducted comprehensive internal tests (simulated acceptance tests) to ensure that the system to be delivered meets the technical specifications. The results of these internal tests shall be documented and submitted to the Client. No equipment shall be submitted for acceptance testing unless it has been previously tested by the Contractor and complies with the technical requirements.

The acceptance tests shall include, at a minimum, the following subjects:

a. Visual Inspection, during which the following shall be checked:

b. Final bill of quantities for all system items.

c. Completeness of the supplied components.

d. Integrity of cables and wiring.

e. Functionality and quality of labeling.

f. Mechanical installation of the equipment.

g. Operation of buttons, switches, and indicator lights in the system.

h. Any additional inspections as determined by the Client.

i. Functional Tests, which shall include, among others:

j. Operation of operator's workstation.

k. Software functions.

l. Report generation.

m. Operator displays.

n. Human factors / ergonomics.

o. Implementation of safety and security controls in the various systems.

p. Additional tests, as required.

C2: CBK - Official

In the event that the results of the acceptance tests are negative, the Client shall provide its comments to the Contractor in writing within five (5) days of the test completion. The Contractor shall rectify the issues no later than ten (10) days after receiving the document and shall resubmit the system for repeated acceptance testing.

Technical documentation

Fifteen (15) days prior to the scheduled start of acceptance testing, the Contractor shall submit the project technical documentation package to the Client in two hard copies and on electronic media.

The technical documentation package shall be prepared in English and shall include the following four main sections:

a. Operating instructions.

b. Maintenance instructions.

c. Software documentation.

d. “As-Made Drawings” for each facility in DWG format.

Operating instructions shall include:

a. A detailed description of the system, subsystems, equipment items, operator units, and equipment layout, including block diagrams, drawings, illustrations and photos of the equipment supplied and/or installed by the Contractor.

b. Detailed operating instructions for the PSIM system and all subsystems.

c. Screen descriptions for the operator workstation, with accompanying images and detailed explanations of the operation of each screen.

d. Instructions for troubleshooting at the operator level.

e. Training materials.

Maintenance instructions shall include:

a. Description of the system.

b. Detailed drawings showing the location of equipment at the facility, cable diagrams and descriptions, cable trays, various power outlets, grounding, junction boxes, and connection panels.

C2: CBK - Official

c. Detailed technical specifications from the manufacturers for all system components.

d. Wiring plans and lists, including:

e. Functional diagram showing cable and wire routing by system functions through connection panels and junction boxes.

f. Cable routing diagrams by function throughout the system via panels and junction boxes.

g. Wiring lists include each cable, functional description of each pair, and connections at both ends.

h. Wiring diagrams showing the path of cable pairs by function throughout the system via panels and junction boxes.

i. Photographs and drawings of all communication cabinets, racks and ACS cabinets.

j. Routine maintenance instructions at the operator level.

k. Preventive maintenance instructions, including periodic system inspection by the Contractor.

l. Confirmation that all equipment is properly grounded and protected against lightning strikes.

Software Documentation shall include:

a. List of all integrated software in the system, organized by subsystems.

b. Detailed functional description of the PSIM software.

c. List of passwords and IP addresses MAC addresses.

d. All hardware and software licenses registered in the Client's name.

"As-Made Drawings" shall faithfully reflect the actual installation of the system and shall include:

a. Final bill of quantities.

b. Location of all system elements at the facility.

c. Infrastructure execution drawings.

d. Cable routing and connection panels.

C2: CBK - Official

All drawings shall be computer-generated and layered by functional groups, with each layer in a separate color.

If the Contractor will fail to prepare the drawings to the satisfaction of the Client, the Client may commission the preparation of the "As-Made Drawings" by others, with all associated costs borne by the Contractor.

The "As-Made Drawings" shall not serve as a basis for any financial claims by the Contractor for changes in the works.

As an integral part of the documentation, the Contractor shall prepare a catalog of all equipment parts, indicating the manufacturer and model of each part.
After review, the draft technical documentation shall be returned to the Contractor with the Client's comments. The Contractor shall make the necessary corrections and submit two final hard copies and electronic media copies to the Client no later than fifteen (15) days after receiving the Client's comments.

The technical documentation package shall be updated by the Contractor following any system modifications (such as added elements, software changes, etc.).

Training

The Contractor shall provide comprehensive training for control room operators.

The Contractor shall train the Client's control room operators to a level that will enable them to operate the system (including operation of all functions of the system at operator's level).

Training shall be conducted for the security personnel of each site included in the Project, at their respective locations (total of 10 training courses).

The duration of each training course shall be five (5) days, including at least three (3) days of practical training in the Client's control room.

The training shall include familiarization with the system covering all hardware components of the entire system, detailed operating instructions for each component of the system and specific step-by- step operating procedures. It shall include simulation of operating conditions with demonstration of various types of alarms, malfunctions and emergency situations.

Training material and reference books regarding specific subjects shall be issued to each participant prior to the training.

The training sessions shall be conducted using training aids and shall be based on the technical documentation prepared for the systems. Prior to the training, the Contractor shall prepare dedicated technical

C2: CBK - Official

materials to be distributed to the participants.

This training shall not relieve the Contractor of any of its obligations regarding service, warranty, and maintenance of the systems described in this specification and in accordance with the Contract.

System hand – over

The system handover and final acceptance by the Client shall take place only after all the following requirements have been fulfilled:

a. The Client has provided written approval confirming the successful completion of the acceptance tests.

b. The Contractor has completed the required training program to the Client's satisfaction.

c. The Client has approved the submission and completeness of the technical documentation.

Supervision

Client supervision of the Contractor's work shall be carried out by the Client's representative and shall include, inter alia:

a. Monitoring compliance with the detailed work plan.

b. Periodic reports (monthly or bi-monthly) prepared by the Contractor.

c. Project status review meetings and discussions.

d. Continuous and overall supervision of the Contractor's work at the site.

Status meetings regarding the project shall be held on-site at pre-determined intervals and/or upon the Client's request. These meetings shall include representatives of both the Contractor and the Client and shall be intended to update the Client on the progress of the Project.

At least once a month, or more frequently if required by the Client, the Contractor shall provide a written report on the project status, progress of works, performance against the plan, description of issues requiring resolution, items for the Client's attention, and forecast of future project progress.

The Contractor shall provide the Client/Inspector, in writing and/or in drawings, within fourteen (14) days, any information that the Client/Inspector may reasonably request, provided that such information relates to the Contractor's activities and/or the system equipment and/or the design and/or manufacturing of equipment items for the Project.

The Contractor shall participate in coordination meetings or discussions on any matter convened by the Client for the execution of the Project, without limitation on the number or duration of such meetings.

C2: CBK - Official

Meeting minutes shall be prepared and distributed by the Client.

The Contractor shall immediately take all necessary actions to correct deviations from the technical specification requirements if such deviations are identified by the Client during the Project execution.

The Contractor shall provide the Supervisor, on behalf of the Client, with all assistance required to perform their duties.

Warranty period

The warranty period shall commence on the date of system handover to the Client (upon successful completion of the Acceptance Tests).

During the warranty period, the Contractor shall be responsible for the functional performance and proper operation of the system in accordance with the standards specified in this specification.

The warranty shall apply to all system components supplied by the Contractor.

During this period, the Contractor shall, at its own expense and in coordination with the Client, replace and install at the site any defective item of the system components supplied by the Contractor, including all parts, accessories, travel, lifting equipment, and labor, provided that the defect was not caused by intentional action or by force majeure.

During the warranty period, the Contractor shall be responsible for the quality of the work performed and for the quality of all materials and equipment included therein. Without limiting the generality of the foregoing, the Contractor shall be responsible for the proper operation, integrity, durability, suitability for purpose, output, capacity, and quality of the works performed, of all system components, and of each item individually.

During the warranty period, the Contractor shall provide, at no additional cost, the following services:

a. Repairs.

b. Periodic inspections (during the warranty period, the Contractor shall perform periodic inspections every four months). The periodic inspections shall include a full system check, preventive maintenance, software updates, software upgrades, and inspection and cleaning of cabinets.

The Contractor shall provide at least the following services as part of the warranty:

a. Software maintenance.

C2: CBK - Official

b. Sensitivity adjustments for all system components and software.

c. Equipment calibration for all system components and software.

d. Synchronization, stabilization, interface coordination, etc.

e. As required, performing repairs to restore the system to full operational condition at the level of the start of the warranty period.

Each system inspection during the warranty period shall be accompanied by a summary report submitted by the Contractor to the Client, detailing all inspections, adjustments, and repairs performed by the Contractor.

Repair of faults

Repair of faults shall be performed in accordance with the SLA defined in this tender.

Repair of faults shall be carried out continuously at the Client's site until the fault is fully resolved.

The Contractor shall maintain a service center (capable of receiving fault reports) 24 hours a day to receive notifications of system faults. A telephone or automated notification of a fault to the Contractor's offices shall be considered a valid notification, obligating the Contractor to take all necessary measures to correct the reported fault as described above.

Supplementary warranty

In the event that a defect is caused by malicious action or by force majeure beyond the system's intended capacity, the Contractor will be required to replace, at the site, any defective item or component of the entire system, including all its accessories and parts.

For this service, the Client shall pay the Contractor as follows:

a. According to the prices specified in the contract's Bill of Quantities.

b. Supply of equipment not included in the Bill of Quantities shall be paid based on the supplier's/manufacturer's invoice plus 30%.

Licenses and passwords

C2: CBK - Official

All software and hardware licenses for the Project shall be registered in the name of the Client.

The cost of license renewals shall be borne by the Contractor throughout the entire duration of the maintenance contract.

All licenses, passwords, and IP addresses for all software and equipment items shall be delivered to the Client as part of the submission of the technical documentation.

C2: CBK - Official

PSIM

General

The Physical Security Information Management (PSIM) software platform shall serve as the primary system for events and alarm management, situational awareness, generation of reports, and control within CBK's security environment.

The PSIM shall provide control room operators and other authorized users with a comprehensive and efficient tool for monitoring, viewing, operating, controlling, logging, and debriefing all Integrated Security System (ISS) components through a single, unified user interface.

The PSIM shall be installed and operated on the CBK security LAN/WAN, which will consist of clustered servers and switches located within servers rooms and at user workstations.

The proposed PSIM system solution required to:

a. Connect and manage diverse security subsystems (CCTV, ACS, IDS, PIDS, P.A, intercom, etc.) regardless of manufacturer or protocol.

b. Use open architecture and standard communication interfaces (such as ONVIF, OPC, Modbus, BACnet).

c. Provide a single command-and-control interface.

d. Support seamless control of all workstation screens and monitors using a single computer mouse and keyboard. Solutions requiring separate input devices (e.g., one mouse for the event screen and another for the video matrix/VMS screens) are strictly unacceptable. The proposed solution must feature continuous, seamless mouse roaming across all monitor borders (Borderless KM Switching) regardless of the display's source application or hardware.

e. Enable operators to view videos, alarms, and device status from all integrated systems.

f. Allows control actions such as unlocking doors, acknowledging alarms, or switching camera views.

g. Automatically correlate events from multiple systems (for example: door forced + motion detected = possible intrusion).

h. Support rule-based automation to trigger predefined workflows or actions.

i. Present operators with step-by-step response instructions for each alarm or event type.

C2: CBK - Official

j. Combine data from all security systems with GIS/site maps for real-time visualization.

k. Display device locations, event origins, and live camera feeds on graphical maps.

l. Log all events, actions, and operator responses.

m. Enable incident reporting, timeline reconstruction, and audit trails for investigations.

n. Offer high availability through redundant servers (Active-Active or Active- Passive).

o. Includes role-based access, encrypted communications, and authentication mechanisms.

p. Generate multiple reports in various formats.

q. Display real-time system status via dashboards.

General requirements

The PSIM software shall be a Commercial Off-The-Shelf (COTS) product that is fully tested and free of defects. The software package must have a proven track record of continuous, reliable, and failure-free operation in projects comparable in scale and complexity to the requirements of this Project.

The PSIM platform shall be an enterprise-class, distributed solution capable of controlling multiple sites, sub-systems systems and large number of end devices through a hierarchical topology. The platform shall support a minimum of:

a. 20 sites.

b. 150 concurrent operator sessions.

c. 20,000 field devices.

d. The PSIM software application shall be based on client-server architecture.

The server application shall be installed on a Windows Server operating system. The client application shall operate on Windows client workstations or via a web interface accessible from any supported environment.

The platform shall support Microsoft SQL Server 2022, or later versions that are certified and supported by the PSIM manufacturer at the time of installation.

C2: CBK - Official

The PSIM platform shall support virtualized environments such as VMware or Hyper- V. As an alternative failover method, the platform shall support native redundancy.

The PSIM platform will be GIS-based, providing a geospatial interface that displays all system components, devices, and events on interactive maps and floor plans. This enables operators to visualize and manage security assets and incidents in their real- world geographic and spatial context.

The PSIM software shall support the addition of new elements, systems, or sites at any stage of the system lifecycle through standard interfaces.

The PSIM software shall be configurable to meet the Clients' specific requirements, including customization of maps, procedures, devices, tasks, and operator response schemes.

The PSIM software shall be supplied with all tools, utilities, administrative software, and other components required for system management, control, and configuration.

The PSIM solution shall include all software and hardware components required to ensure continuous system operation, regardless of the number of users, sites, video streams, or field devices. Hardware components, including CPU, RAM, and storage shall be designed to withstand the maximum planned load (e.g., number of users and video streams) and shall include a minimum of 30% spare capacity (e.g., CPU utilization shall not exceed 70% at peak load).

The PSIM platform shall support standard communication protocols such as Modbus, OPC DA, OPC UA, BACnet, KNX, SNMP, ASCII, NMEA, ONVIF, ESPA, SIA, SIP, and MQTT.

The PSIM shall support integration with AI systems through REST APIs, MQTT, ONVIF Profile M and message queues.

All PSIM servers, clients, databases and integrated subsystems shall synchronize to the supplied NTP source.

The PSIM software shall support English, French and Spanish language.

The PSIM software at each site (LCRs, SMSC, and MSC) shall be installed on two (2) separate physical servers operating in an active - active configuration.

The proposed PSIM platform shall be modular system with open APIs (REST, SOAP, SDKs) for any third-party integration.

The system shall support load balancing and clustering for large deployments.

The system event throughput: >10,000 events per second sustained.

C2: CBK - Official

PSIM architecture

The architecture of the PSIM will be based on a multi-site, Federated architecture where each of the sites maintains local control of its security systems while reporting to the central PSIM for monitoring, coordination, and incident management.

The PSIM shall support operation from a geographically separate Disaster Recovery site.

The solution shall enable each local PSIM server to independently monitor and manage its respective site, using its own local database. A two-way communication between the local site servers and the central servers located at the MSC and SMSC shall allow real-time exchange of information and commands between them and the sites.

Local sites shall continue operating autonomously during WAN outages. Upon restoration of connectivity the following shall occur without operator intervention:

a. Automatic resynchronization.

b. Conflict resolution.

c. Event reconciliation.

Alerts originating from the various sites shall be transmitted to the MSC and SMSC in accordance with predefined parameters and prioritization criteria (including, but not limited to, alert type and the response timeframe allocated to the LCRs).

The MSC and SMSC shall maintain supervisory authority over the LCRs with respect to the management and control of the local security systems, including, inter alia, the operation of cameras and the management of all ISS subsystems.

The local PSIM servers shall be fully and automatically synchronized in real time with the central servers. The configurations of the federated servers shall be either partially or fully replicated to the federating server, as required.

From the central servers it shall be possible to perform the following functions:

a. Monitor events, alarms, and device statuses from all connected sites.

b. Send control commands to field devices across multiple sites.

c. Configure system parameters, device settings, workflows, and response procedures for all sites.

C2: CBK - Official

d. Retrieve events from devices connected to local site servers.

e. Retrieve changes/additions/deletions made to configurations on local site servers.

f. Automatic synchronization of information from local site servers to the central servers.

g. Distribute configuration updates to local servers automatically or on demand.

h. Create, modify, and delete operator accounts.

i. Assign user roles, permissions, and access rights across all sites.

j. Collect and consolidate logs, alarms, and operational data from all local servers.

k. Maintain unified audit and reporting databases.

l. Generate system-wide reports on alarms, events, operator performance, device health, and system usage.

m. Provide dashboards and analytical tools for multi-site situational awareness.

n. Monitor the status of local servers, communication links, hardware resources, and database availability.

o. Deploy software updates, patches, and firmware upgrades to local servers and devices.

p. Manage system-wide backup schedules.

q. Perform restore operations and coordinate failover between central and local servers.

r. Configure and maintain integrations with third-party systems across all sites.

s. Manage federated server connections, synchronization rules, and data-sharing policies.

t. Apply global security policies and ensure compliance across all site-level systems.

The platform shall support Active-Active and Active-Passive redundancy configuration with load balancing and failover mechanisms. Optional support of geographically distributed data centers is required.

The platform shall include automated backup mechanisms.

A conceptual drawing of the PSIM architecture is provided below

C2: CBK - Official

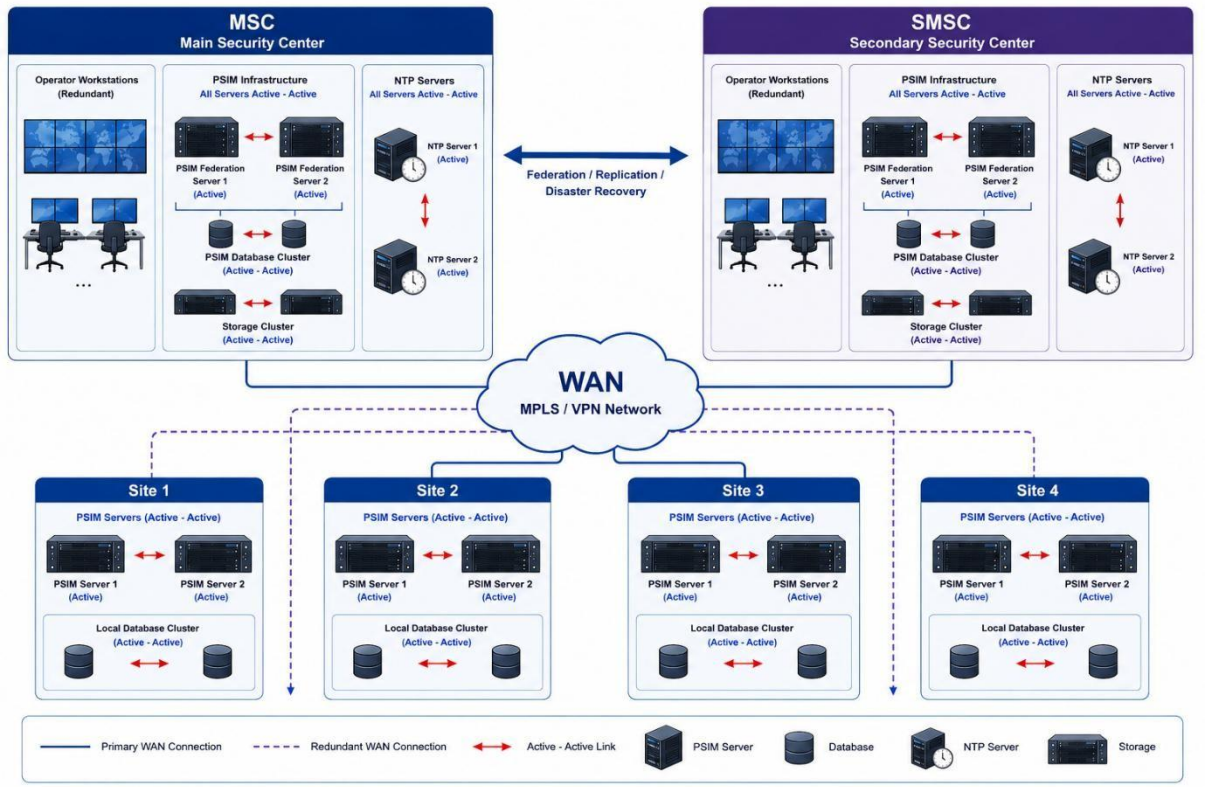

FIGURE 8 - CONCEPTUAL TOPOLOGY OF THE PSIM

Redundancy

The PSIM shall be fully redundant and shall not contain any single point of failure that may cause a major malfunction of the entire system.

Redundancy shall be ensured across all hardware and software layers. All databases shall operate in a fully redundant configuration.

The PSIM shall implement an Active–Active redundancy architecture to ensure continuous system availability and load sharing.

High - Availability

The PSIM system shall provide high availability and reliability at all times.

The PSIM shall operate in a true Active–Active clustered architecture. In the event of failure of any cluster node, all critical services shall continue operating on the remaining node(s) without loss of alarms, events, operator actions, audit records, or incident data. Recovery Point Objective (RPO) shall be close to zero. Any service interruption shall not exceed five (5) seconds.

C2: CBK - Official

The system shall support continuous operation: 24 hours a day, 7 days a week, 365 days a year.

The PSIM system availability shall be 99.9%, achieved through a redundant system architecture, modular design, and use of high-quality hardware and software components.

The system shall ensure secure protection of all data within the PSIM, as well as data exchanged between the PSIM and other integrated security subsystems.

Capacity

There shall be no limitation on the number of workstations or operators within the security LAN/WAN of the overall PSIM system.

The system shall allow the definition of at least 32 distinct functional groups for operators.

Each operator shall be capable of responding to simultaneous alarms from up to 4 different protected sites. In cases where more alarms occur, a queuing mechanism shall be provided.

Each operator shall be capable of simultaneously monitoring up to 16 video streams from a single protected site, or 2 video streams from 8 different protected sites, or 4 video streams from 4 protected sites, with equivalent combinations supported.

PSIM core modules

The PSIM software will include the following core modules and applications:

a. Events management module.

b. Video management module.

c. Geographic Information System (GIS) and map module.

d. Reports generation module.

e. Massages and mass notification module.

f. Rules engine module.

g. KPI’s and dashboards module.

h. Standard operating procedures module.

i. Subsystems integration module.

C2: CBK - Official

j. User administration & permissions module.

Events management module

The Events management module will manage, display and log all the events reported by the various electronic subsystems and all the actions taken by the operators.

The module shall support the management of the following types of events:

a. Online Events: Events received automatically from the various security subsystems integrated with the PSIM.

b. Offline Events: Events reported to the security control room via telephone, radio, WhatsApp, SMS, or any other communication method, and created manually by the operators.

Offline events entered manually by an operator into the module shall be assign a priority level and shall be handled in accordance with that priority.

Both online and offline events shall be displayed to operators in chronological order based on their time of occurrence and assign level of priority. The system configuration tool shall enable filtering and displaying events according to predefined severity levels (for example: a fence alarm shall be displayed as a high-priority event).

Each event shall include– at least – the following details:

a. Event serial number.

b. Date, time of occurrence.

c. Type of event.

d. Event location.

e. Event description.

f. Subsystem source.

g. Time of acknowledge (activated by Acknowledge functional key).
h. Event status.

The module shall include a text entry field that enables the operator to edit an entry and record an unlimited number of notes. Certain entries shall be designated as mandatory for specific event types, as defined

C2: CBK - Official

by the system administrator's configuration.

a. Events shall be classified into one of the following statuses:

b. Alarmed – The event has been generated in the system.

c. Acknowledged – The event has been acknowledged by an operator.

d. Handled – The event has been completed and transferred to the history files.

e. Pending – The event has been received and acknowledged but not yet completed by the operator. Operators shall be able to select any event from the pending list and resume its handling.

f. Suspended – The handling of the event has been suspended by an operator for delayed actions. When an event is suspended, the operator shall be required to specify the suspension duration. Upon expiration of this duration, the event shall automatically return to the "Received Events" list.

g. Escalated Event – An event that meets any of the following conditions:

h. It was not acknowledged within a predefined time frame.

i. It was acknowledged but not handled within a predefined time frame.

j. It was not completed within a predefined time frame.

k. It was escalated according to a predefined scenario triggered by other events (as a result of a logical rule).

Alarms shall be displayed in clear text in the alarm list or in graphic form by an animation.

Different colors shall be assigned to the various statuses of events to enable immediate visual identification.

Each alarm event shall generate an audio alert (e.g., sound or spoken message) in the control room. The system shall allow assigning specific audio alerts to particular types of alarms and shall provide the ability to mute audio alerts as required.

Once an event is acknowledged (Ack command), the corresponding sensor icon on the map shall stop flashing. A pop-up window containing event-handling instructions shall appear on the screen for the operator.

C2: CBK - Official

Upon completion of event management (Handled status), the alarm shall be cleared and recorded in the history log. The handled event shall be removed from the events list, and the corresponding sensor icon shall return to its normal status on the map screen.

If the number of events exceeds the number of visible lines on the module display screen, the operator shall be able to scroll through the list to view all events.

The event module shall continuously display, in a clearly visible manner, both the total number of events and the number of events that have been acknowledged but are still pending completion.

The module shall support simultaneous incident management, allowing multiple users to work on the same incident. Users shall be able to share information, images, and updates within the incident record. The module shall also support transferring an incident to another user for continued handling.

The module shall support sending notifications upon an alarm, including:

a. Email notifications.

b. SMS notifications.

c. The module shall support the generation of incident reports with various (at least 10) filtering and grouping options. The platform shall enable to attach images, screen shots, and video clips to incident reports.

Video management module

The video management module will include the following key main features:

a. Live and playback viewing for all cameras.

b. Display of multiple cameras on a single monitor (configural).

c. Display of cameras on multiple screens.

d. Control of PTZ, Dome cameras and digital zoom through a dedicated joystick, mouse, or keyboard interface.

e. Video search by date and time, motion or bookmark.

f. Definition of cameras groups and tours.

g. Configuration of camera’s presets.

C2: CBK - Official

h. Selection of camera from map or sensors list.

i. Capture, save and export video.

j. Monitor and generate alarms for faults, video loss, communication loss, camera masking.

k. Protection of video against deletion (deliberate or accidental).

l. Protection of video against tampering with digital signatures.

The video module shall support a minimum of seven simultaneous users viewing cameras.

The module shall support display of video overlay from a third-party system (such as video analytics system).

The video module will provide functionality to move a camera display from one monitor to another and present it in full-screen mode.

C2: CBK - Official

When operating in “floating window” mode, the system will automatically resize the window and proportionally adjust the size of all contained camera views

The module will support configuration of the maximum number of camera views per screen, with automatic resizing of each image according to the selected layout. Supported display grids shall be 1×1, 2×2, 3×3, and 4×4. If the number of cameras exceeds the capacity of a single grid, the system will automatically create additional partitions and enable user browsing between partitions.

The video screen layout shall be configurable, allowing the selection of multiple multi- window presentations with varying numbers and sizes of windows

The module will support defining camera groups that are consistently displayed together in a single partition.

The module shall provide functionality to create a timeline with bookmarks.

The module shall allow users to view and control cameras from either the map or the sensor list. A newly selected camera will be prominently highlighted among all displayed cameras. Selection for display shall be performed by double-clicking the camera icon on the map or in the sensor list.

The module will provide options to program automatic video display on the workstation screen in the following three scenarios:

a. Automatic display of camera images triggered by a sensor rule in the event of an alert.

b. Display initiated by a pre-planned task.

c. Display triggered by a specific event type configured to run a designated display layout.

In all three scenarios, images from the camera associated with the event will be displayed on the video screen. Once displayed, control room operators will have the option to change or disable the camera view.

The module will enable configuration of presets, tours and groups for all cameras.

The module shall support transmission of video streams to remote users via a mobile application. The application will display a list of video streams that each remote user is authorized to access, allowing them to select and view a specific camera from the list.

The module shall allow simultaneous display of pre-alarm recorded video and live video.

The module shall support configurable playback modes, including Playback, Frame- by-Frame, Slow Forward Search, Fast Forward Search, Slow Rewind, and Fast Rewind.

C2: CBK - Official

The module will enable user to select video sources to display using the following methods:

a. From the list of cameras in the cameras tree.

b. From camera list (using drag and drop or click).

c. From GIS / plans (using click or drag and drop).

d. From selected video sources triggered by alarms.

Cameras shall be selected for display on the monitors using drag-and-drop or double click functionality.

The module shall provide notifications for video signal loss, recording system malfunctions, and disk capacity status.

The module shall allow users to capture screenshots of video images and print them directly from the interface.

The module shall allow users to select and save video clips.

The video management module shall support management of cameras at remote sites, including:

a. Viewing video streams from local remote VMS / NVRs and cameras.

b. Retrieving stored video from local remote VMS / NVRs and distributing it to other workstations.

c. Receiving status information from remote devices, including cameras and NVRs.

The module will support a Video Overlay functionality, allowing interaction with an object overlaid on the video stream in the matrix. For example, the video feed will enable real-time actions such as opening/closing a controlled door, initiating an intercom call, arming/disarming a sensor, etc.

The PSIM shall support H.264, H.265, H.265+, MJPEG, ONVIF Profile S/T/M.

GIS and map module

The PSIM platform shall include enterprise grade GIS engine either Native / built-in GIS engine or Embedded third-party GIS engine (integration with GIS engine such as ArcGIS Runtime or GeoAnalytics Engine).

C2: CBK - Official

The GIS and map module will enable the display of data layers and assets, including geographic road maps, satellite imagery, security element layers, and site and building layers.

The GIS and map module will allow the display of data from various sources (e.g., GPS localization software and different web applications) on a unified map in a layered configuration.

The module will support a GIS engine, with site selection enabled via double-click. Clicking on a specific site on the GIS map will allow users to drill down into a hierarchical view of different maps and drawings of the site.

The module will support a Synoptic Overlay functionality, enabling the animation and movement of objects on the map.

The module will support working with "floating" or fixed windows, depending on the user profile.

The module will include tools for importing plans or photographs, onto which icons will be placed to indicate the types and locations of devices. It will support the import of all common file types for storing graphic and photographic information, such as JPEG, DWG, GIF, WMF, DXF, BMP, etc. Floor plans (or any other maps) in AutoCAD DXF format will be fully supported by the system without the need for conversion to another format.

GIS map refresh rate shall not exceed 2 seconds following a status change.

The module will include a drawing tool for creating simple sketches or for adding to or editing imported plans.

From the map module it will be possible to:

a. Pan and zoom.

b. Navigate through different maps.

c. Span a single map through multiple monitors.

d. Manage and control security elements and sensors (for example opening video of a specific camera, opening a door, etc.).

e. Show information about various objects.

f. Find entities on the map and locate other nearby entities.

g. Monitor mobile assets (such as patrol cars).

C2: CBK - Official

The operational status of the various security elements will be displayed by icons on “site plans”, pictures, photos and diagrams.

The various maps will be superimposed with the individual elements in overlays (as transparent sheets). “Status change” of an individual element will be shown by change of color, flashing, etc.

The module will allow users to create or modify the custom icons library. Users shall also be able to import backgrounds or symbols created with other graphic tools using standard formats such as DWG, DXF, JPG, PNG, GIF, WMF and PDF.

The various icons on the map module will indicate the exact location of security devices. The icons will dynamically indicate the device status. The system will be capable of displaying different types of icons for different types of devices.

The maps will be dynamic, allowing users to zoom in or out on a selected section.

The icons will display the devices status in real time.

The system will allow hierarchical display of different maps and drawings for each site (at least 5 levels are required). While changing the map, the scale of the symbols’ size shall be adopted to each map.

In alarm events, the alarming element and its area will be displayed automatically or at the user's request with any number of predefined overlays, as a part of a pre-configured alarm management procedure. It will be optional to automatically zoom in on the area of the alarmed device.

Clicking on the camera symbol on the map will open a pop-up displaying the camera feed.

When selecting a symbol of a device which can be managed remotely, the relevant functions such as “on” “off”, reset, activate, etc. will be selected and activated. Additional actions according to various scenarios may also be carried out.

Off-line status will indicate the number of elements that are not communicating with the PSIM.

Mobile application

The mobile application will support both iOS and Android.

The mobile client screen display shall be fully customizable, allowing personalization at multiple levels. Customization options will be available for specific user profiles, or for individual users, enabling tailored views, layout arrangements, and display settings according to preferences or roles.

The mobile client shall support the ability to capture and transmit live video directly from the device's built-in camera to the PSIM system.

C2: CBK - Official

Mobile client features will include:

a. Playback video.

b. Viewing live streams.

c. Real-time video streaming from the device built-in camera.

d. Send and acknowledge alarms.

e. Display events.

f. GPS tracking.

g. Instant messaging.

The PSIM mobile app will incorporate end-to-end encryption to ensure the confidentiality and security of messages sent to users on mobile devices. This encryption will apply to all message types, including text, alerts, and multimedia content, preventing unauthorized access during transmission.

Mass notifications module

The PSIM software shall support both manual and automatic messaging to individuals or predefined groups, with an integrated confirmation mechanism to ensure receipt and acknowledgment of each message.

The system will support the following types of massages:

a. SMS (SMS bundle will be supplied by Client).

b. Chat.

c. Push notifications.

The solution shall include integrated instant messaging and chat capabilities, enabling users to exchange text-based messages with colleagues, supervisors, and management personnel. The chat feature shall support one-on-one and group conversations.

The PSIM messaging system will incorporate end-to-end encryption to ensure the confidentiality and security of messages sent to users on mobile devices. This encryption will apply to all message types,

C2: CBK - Official

including text, alerts, and multimedia content, preventing unauthorized access during transmission.

All message transactions, including both sent and received messages, shall be automatically saved in the system's database.

When sending the message through the application it will be possible to specify:

a. List of recipients.

b. Means of communication (Push, Chat, SMS).

c. Priority: high, low, normal.

d. Topic.

e. Appendices.

The system will send the user an immediate indication that the sending request has been forwarded to the server.

The system administrator will be able to track messages using the administration tool according to the following criteria: date, status, username, sender name, method of communication.

Reports generation module

The PSIM platform shall allow users to generate customized reports on entities, resources, events, and activities from their workstations, with report generation capabilities limited based on user authorization levels.

The system shall support generating reports in various formats, including but not limited to plain text, tables, columns, stacked columns, pie charts, rows, and stacked rows, according to client preferences.

The reports generation module shall allow users to generate customizable reports based on specific parameters.

The system shall support the generation of reports for specific facilities as well as for the entire system.

The system shall support exporting reports directly from the software to a file.

The system shall support, at a minimum, the generation of the following types of reports:

a. Event and Incident Reports - including open, closed, and escalated events with timestamps, classifications, and handling status. The platform shall enable users to attach images, screen shots, and

C2: CBK - Official

video clips to incident reports for visual documentation and analysis.

b. Operator Activity Reports - detailing user login, actions performed, command executions, and system interactions. Filtering options by operator name and/or specific date.

c. Alarm Activity Reports - summarizing all alarm activations, acknowledgments, responses, and resolutions within a defined period.

d. Video Recording and Retrieval Reports - documenting recording availability, footage retrieval logs, and storage utilization.

e. Access Control Reports - including access events, denied entries, door status changes, and credential usage trends.

f. Intrusion Detection Reports - including alarm events, IDS status changes.

g. Audit and Compliance Reports - covering system changes, configuration updates, and policy compliance checks.

h. System Usability Report - documenting system errors, downtime, and performance issues. Reports shall support filtering across the entire system, individual sites, and subsystems.

i. Anomalies Report - detailing system irregularities, with filtering options across various cross-sections.

j. Shift Report - summarizing events, activities, and operator actions per shift.

k. Historical Reports - providing detailed records of all system events over different time intervals (hour, day, week, month). The system shall retain all events for a minimum of 12 months.

l. Statistical Reports - presenting metrics and performance statistics of the system and its subsystems across multiple cross-sections.

m. Custom Reports - Up to additional 10 non-standard reports, to be defined by Client before the end of the warranty period.

Examples of subsystem reports:

a. IDS Work Regime Report - detailing day/night operation and the status of detectors and areas (normal, warning, malfunction). Reports shall support filtering by facility section, detector type, groups of areas, combinations of sections, and other relevant criteria.

C2: CBK - Official

b. b. ACS User List by Section - listing users with details including name, surname, and card number, filtered by facility sections.

c. ACS User Activity Report - detailing user access by location, date, and time, with reporting intervals configurable from 1 hour up to 24 hours, and summarizable by day, week, or month.

d. ACS User Restrictions Report - showing card restrictions per door or controlled gate, including detailed card movements at reader level, area, and time settings.

e. ACS Door Report - Generates a list of all transactions that occurred within a selected time period for a specific controlled door or for all controlled doors in a facility. The report can be filtered by date, time, cardholder name, event type, and other criteria.

f. ACS Expired/Lost/Unreturned Cards Report - listing all cards that have expired, are reported lost, or have not been returned.

g. ACS Alarms and Element Status Report - summarizing alarms, their status, and the condition of system elements.

h. CCTV Device Malfunction Report - listing all cameras and devices with detected malfunctions.

i. Communication Loss Report - documenting instances of communication failure between system components or subsystems.

C2: CBK - Official

Rules engine module

The definition of scenarios and work processes shall support a variety of logical functions, including If, Then, Else, as well as various arithmetic functions.

The Rule Engine module shall allow defining the outcomes of rules, including:

a. The type of incident to be generated.

b. The Standard Operating Procedure (SOP) to be deployed with the incident. c. And, the subsystems to be triggered as part of the rule.

The Rule Engine module shall provide the ability to mute, disable, or copy rules as needed.

The Rule Engine module shall be capable of controlling an unlimited number of sensors.

KPI's and dashboards module

The KPI and Dashboard module shall enable users to monitor, measure, and display the performance of the Integrated Security System (ISS) through clear and intuitive graphical interfaces.

The dashboards shall display, in real time, active events and incidents. The display shall include color-coded icons or heatmaps indicating the severity and location of each incident. All main information shall be displayed on a single screen.

KPI dash boards shall include metrics such as response times, incident resolution rates, alarm counts, patrol coverage, system health, and other performance indicators.
Data shall be displayed using charts, graphs, heatmaps, gauges, geographical maps, and other visual elements.

Users shall be able to customize the dashboards by adding, rearranging, or removing elements based on their roles and priorities.

The KPI and Dashboard module shall support the configuration and display of at least twenty (20) different Key Performance Indicators (KPIs) and a variety of graphical presentation formats, including charts, graphs, gauges, heat maps, geographic maps, and tabular views.

The dashboards module shall allow users to generate and export reports. Reports may be customized to include specific data, incident history, and performance metrics.

C2: CBK - Official

FIGURE 9 - EXAMPLE FOR DASHBOARD DISPLAY

Standard Operating Procedures (SOP's) module

The SOP module will allow assigning a set of procedures to specific incident types.

The SOPs will be displayed to the operator in a dedicated window that will include at least the following:

a. Sequence of required actions.

b. Telephone numbers of stakeholders ("Auto dial command" is required).

c. List of internal stakeholders.

d. Communication means with external emergency services.

The module will include an option for action verification (via checkboxes). An event will only be marked as complete once all action items have been executed and verified. Event escalation will be triggered if any SOP stage is not fulfilled within the defined timeframe. The action verification option could be cancelled by the Clint administrator.

The module will support the triggering of automated actions.

C2: CBK - Official

All operator actions during an incident will be recorded in the system database, including time and date.

Integration with subsystems

The PSIM system shall be capable of integrating, at a minimum, with the following subsystems:

a. CCTV system.

b. Video Management System (VMS).

c. Intrusion Detection System (IDS).

d. Access Control System (ACS).

e. Perimeter Intrusion Detection System (PIDS).

f. Electric fence.

g. Public Adress System (PA).

h. Radar.

i. VA and AI.

Integration with CCTV system

a. The PSIM software will automatically display cameras that cover Areas of Interest (AOI) where alerts received by other systems (such as: ACS, PIDS, IDS, VA).

b. The system will enable viewing live and recorded video in the PSIM client workstations.

c. The integration between the PSIM and the CCTV system shall enable the display of indications from the CCTV system within the PSIM, including the following:

- Automatic display of cameras covering Areas of Interest (AOIs) associated with alerts received from other systems (e.g., ACS, PIDS, IDS, VA).
- Control of cameras.
- Viewing live and recorded videos.
- Display of camera malfunction.

C2: CBK - Official

- Display of communication loss.
- Tamper alarm.

d. From the PSIM workstations, it will be possible to perform – at least - the following actions:

- Select a camera to display on viewing screens.
- Define camera tours and display them on viewing screens.
- Define camera groups.
- Display "alarm" camera on the viewing screens.
- Manage cameras displays on the operators' workstations.

Integration with Video Management System

a. The integration between the PSIM and the recording system will allow the PSIM to display indications from the recording system, including the following:

- Communication loss.
- Recording system fault.
- Disk fault.
- Recording capacity.
- Shutdown of the recording system.
- From the PSIM workstations, it will be possible to perform – at least - the following actions:
- Manage video in the recording management system.
- Display Pre-alarm and Post alarm videos stored in the recording system.
- Send a "Set Time" command to synchronize clocks throughout the system.

Integration with IDS

a. The IDS will integrate with CCTV, VMS and PSIM system

C2: CBK - Official

b. The integration between the PSIM and the IDS will enable the PSIM system to display indications received from the IDS, including the following:

- Sensor alarmed, reset, neutralized, or bypassed.
- Sensor fault.
- Controller communication loss.
- Controller cabinet tamper.
- Controller fault.

c. From the PSIM workstations, it will be possible to perform – at least - the following actions:

- Arm and disarm sensor.
- Disable controller.

Integration with Access Control System (ACS)

a. The ACS will integrate with CCTV, VMS and PSIM system.

b. The integration between the PSIM and the ACS will enable the PSIM system to display indications received from the ACS, including the following:

- Controller / reader communication loss.
- Controller malfunction.
- Controller cabinet tamper.
- Reader tamper.
- Authorized card passed in reader.
- Unauthorized access (incorrect card, expired card, lost card, unauthorized for the reader, etc.).
- Door open.
- Door closed.

C2: CBK - Official

- Door opened over the preset time.
- Low voltage (battery).
- “Pass back” attempt.

c. From the PSIM workstations, it will be possible to perform – at least - the following actions:

- 1. Open doors.
- Disable doors.
- Set time windows.
- Area lockdown/unlock.

Integration with Perimeter Intrusion Detection System (PIDS)

a. The PIDS system will integrate with CCTV, VMS and PSIM system.

b. The integration between the PSIM and the PIDS will enable the PSIM system to display indications from the PIDS, including the following:

- Fence sensor activation.
- Fence wire cut.
- Sensor’s line cut.
- Controller cabinet tamper.
- Gate open / close.
- Sensor / sensor line / section malfunction.
- Communication loss.
- Low voltage.
- System malfunction.

C2: CBK - Official

c. From the PSIM workstations, it will be possible to perform – at least - the following actions:

- Arm / disarm zone.
- Set time windows.
- Mask alarms.

Integration with Electric fence

a. The electric fence will integrate with the PSIM, CCTV system and VMS.

b. The integration between the PSIM and the Electric Fence will enable the PSIM

c. system to display indications from the Electric Fence, including the following:

- Energizer status.
- Section malfunction.
- Low voltage.
- Wire cut.

d. From the PSIM workstations, it will be possible to perform – at least - the following actions:

- Arm / disarm zone.
- Set time windows.

Events management workflow

Event management will be carried out using the event screen, map/GIS screen, and video screens.

The system will support multiple screens at the hardware level (multi-screen video card).

Each workstation will be connected to a minimum of three screens: one for the graphics map, one for the event log and operator messages, and one for video operation.

All functional screens (event log view, maps, video displays, sensor lists, etc.) will be available as “floating windows.” Operators will be able to drag any display to any monitor connected to a single client workstation. It will also be possible to return any floating window to the main window.

C2: CBK - Official

When logging out of the PSIM software, the user's most recent screen configuration will be saved, so that upon the next login, the display returns to the same layout.

Administrators will be able to configure, save, and lock views. Once locked, lower hierarchy users will not be able to move windows between screens.

Screen configurations will be stored locally on the client workstation and will not be transferred to the server.

The following window management options and views are required:

Dock/Undock screens.

a. Maximizing display.

b. Lock configuration.

c. Save configuration.

d. Reset configuration.

The events will be displayed on the PSIM workstations according to various configurable parameters, such as:

a. By physical location of the event.

b. By priority level.

c. By subsystem type.

d. In chronological order.

e. By detector type.

f. Etc.

Event management will be carried out according to the following workflow:

a. Selection of an event from the "Events List."

b. The map or GIS will display the relevant area of interest (building, floor, fence section, etc.).

C2: CBK - Official

c. The associated cameras for the device in the scenario will be shown on the video screen, including live and pre-alarm videos.

d. Operators will manage the event using the "Operator Instruction Window," which provides detailed action instructions for each stage of event handling.

The display of any event—such as an alarm, a change in the working mode of an element, an element malfunction, or a communication failure—will cause the corresponding icon on the map module to change color and flicker, indicating its updated status.

System configuration and management

The PSIM will include a user-friendly configuration and management module.

The administrator will be able to perform the following user management actions:

a. Add new users.

b. Block or remove existing users.

c. Rest passwords.

d. Notify users to change the password at the next login.

e. Cancel all user sessions to block them immediately.

The administrator will be able to define different combinations of user credentials and assign roles to each of them.

The system administrator will be able to set workstation access functions as follows:

a. Restrict access to workstations with specific IP addresses.

b. Restrict certain users to access specific workstations only.

c. Define the types of events that will appear on the specific workstation according to user groups.

d. The system will support setting the following password rules:

e. It will be possible to set different policy definitions and assign roles to these definitions.

C2: CBK - Official

f. It will be possible to set the duration for which a password remains valid, after which a password change will be required.

g. It will be possible to set a minimum number and type of characters for a password.

h. It will be possible to define whether it is necessary to use uppercase or lowercase letters, special characters and numbers.

i. All system users will be required to enter a password when logging into the system.

j. Any unauthorized attempt to access the system will trigger an alert in the control room. The alert will include the IP address of the attempting computer and the reason for the alert: unknown username or incorrect password.

k. Users will have the option to save their work configuration, which will be automatically restored the next time they log into the system.

Tasks management module

The platform shall provide task management capabilities that enable managers and users to create and assign tasks to designated personnel. The system shall allow tasks to be categorized, prioritized, and monitored in real time.

The module shall support automated actions such generations of status reports.

Health monitoring capabilities

The PSIM system will perform periodic health monitoring to detect faults and report them to the relevant stakeholders.

If a fault is detected, a self-recovery mechanism will be automatically activated.

Health monitoring will be conducted at multiple levels:

a. Sensor’s level.

b. Controllers level.

c. Server’s level.

d. The system will include a health monitoring mechanism that continuously monitors predefined software components. This will cover, at a minimum, all software installed on the server, Microsoft operating system applications, and databases.

C2: CBK - Official

e. If a failure is detected in any component, multiple automatic attempts will be made to restore it to proper operation (the exact number of attempts can be configured). If all recovery attempts fail, a reporting mechanism will be triggered.

Cyber security

The platform is required to support:

a. Integration with enterprise IAM - Identity and Access Management:

b. Multi-Factor Authentication (MFA) for privileged and remote users.

c. LDAP / Active Directory.

d. Encryption in transit (TLS 1.2+).

e. Encryption at rest (AES-256 or equivalent).

f. Network segmentation support.

g. Secure device-to-platform communication.

h. Compatibility with firewall and IDS/IPS controls.

i. Secure API authentication and authorization.

j. Centralized security logging.

k. Audit logs shall be protected against unauthorized modification and support export to external SIEM or long-term archival platforms.

l. Time-synchronized logging (NTP).

m. ISO/IEC 27001.

Critical security patches shall be deployable without requiring complete system shutdown.

The PSIM shall support integration with enterprise SIEM platforms through Syslog, CEF and REST APIs.

The system shall support Multi-Factor Authentication (MFA) for privileged and remote users.

C2: CBK - Official

Audit logging

The PSIM shall provide a tamper-resistant audit trail and retain audit records for all security-relevant activities including:

a. User logins/logout.

b. Failed login attempts.

c. Configuration changes.

d. Device control commands and operator actions.

e. Incident creation, modification, and closure.

f. Alarm acknowledgements and alarm handling activities.

g. Report generation and report exports.

h. Video exports and evidence extraction activities.

i. User account creation, modification, disabling, and deletion.

j. Role, privilege, and permission changes.

k. Integration status changes, including connection and disconnection of external systems, devices, and services.

Each audit record shall include the user identity, timestamp, originating workstation, action performed, affected object, and action result.

C2: CBK - Official

PSIM server

All requirements are minimum requirements. The Contractor shall provide a PSIM server that meets the PSIM manufacturer's specified hardware requirements. The server hardware and software shall ensure uninterrupted operation under maximum load without any performance degradation.	
Make	Dell, HP or approved equivalent
Operating system	Windows server 2022 or latest
Processor	Dual Intel Xeon Silver/Gold 3rd Generation Scalable processors, minimum 16 cores per CPU
RAM	Minimum 64 GB DDR4 ECC RAM, scalable to at least 512 GB
Memory	2 x 1 TB NVMe SSD
Graphic card	Integrated graphics adapter supporting remote management and dual display output minimum
Lan	2 X 1 Gb/s ports + 2 x 10 Gb/s ports
RAID	Hardware RAID controller supporting RAID 1, 5, 6, 10 with cache memory and battery backup / flash-backed cache
Fan	High performance fan, at least dual, swappable
Power Supply	100–240 V AC, auto ranging, Dual Redundant hot-swap PSUs —
Operating temperature	10–35°C
Operating humidity	20% to 80% RH, non-condensing

C2: CBK - Official

Fail-over	The PSIM server architecture shall support native High Availability (HA) and automatic failover without loss of events, alarms, or operator sessions
Form factor	1U or 2U rack-mount server chassis

PSIM workstation

All requirements are minimum requirements. The Contractor shall provide a computer for workstations that meets the PSIM manufacturer's specified hardware requirements. The computer hardware and software shall ensure uninterrupted operation under maximum load without any performance degradation.	
Make	Dell, HP or approved equivalent
CPU	14th Generation Intel® Core™ i9 processor or approved equivalent, minimum 20 cores / 28 threads
Operating system	Windows 11 Pro, 64-bit
RAM	32 GB DDR5
Storage	Minimum 1 TB NVMe SSD
Graphics card	Dedicated professional GPU with minimum 8 GB dedicated VRAM
Interfaces	Dual Ethernet interfaces, minimum 1GbE each
Monitors support	Support simultaneous operation of minimum six (6) monitors, including at least four (4) 4K outputs via HDMI and/or DisplayPort
Cyber security	TPM 2.0, Secure Boot, BitLocker support

C2: CBK - Official

Power supply	High-efficiency PSU, minimum 80 PLUS Gold certified
Input voltage	90 V AC to 264 V AC
Operating temperature	10–35°C
Operating humidity	20 -80% RH (non-condensing)
Graphics card	Dedicated professional GPU with minimum 8 GB dedicated VRAM
Interfaces	Dual Ethernet interfaces, minimum 1GbE each
Monitors support	Support simultaneous operation of minimum six (6) monitors, including at least four (4) 4K outputs via HDMI and/or DisplayPort
Cyber security	TPM 2.0, Secure Boot, BitLocker support
Power supply	High-efficiency PSU, minimum 80 PLUS Gold certified
Input voltage	90 V AC to 264 V AC
Operating temperature	10–35°C
Operating humidity	20 -80% RH (non-condensing)

24” monitor

Size	24" LED display
Panel type	IPS, LED-backlit LCD, Anti-glare, matte
Refresh rate	75 HZ
Resolution	1920x1080
Response Time	Maximum 5 ms response time
Brightness min.	Minimum 300 cd/m²

C2: CBK - Official

Interface	HDMI, DisplayPort
Operation	Monitor shall support continuous 24/7 operation
Aspect ratio	16:9
Operating temperature	0 to 40°C
Power supply	100–240 VAC, 50/60 Hz
Operating humidity	10% to 80% (non – condensing)
Certifications	CE, FCC, RoHS, Energy Star or equivalent

C2: CBK - Official

NTP server

Stratum level	Stratum-1 time server
Time source	Integrated multi-GNSS receiver supporting GPS, GLONASS, Galileo, and BeiDou satellite systems
Time synchronization protocols	The system shall support NTP v4 (RFC 5905), SNTP (RFC 4330), and advanced NTP authentication mechanisms (including SHA-256 and Network Time Security - NTS)
Holdover accuracy	Internal OCXO (Oven-Controlled Crystal Oscillator) for stable holdover operation during GNSS signal loss
Time accuracy	≤1 µs to UTC when synchronized via GNSS
Network interfaces	Minimum 2 × GbE interfaces
Capacity	The NTP server shall support synchronization of at least 1,000 clients and a minimum processing capacity of 10,000 NTP requests per second without degradation of timing accuracy.
Hardware processing	Hardware-based timestamping and packet processing using FPGA or equivalent dedicated hardware acceleration
Antenna	External GNSS antenna included, suitable for outdoor installation, with operating temperature range of at least - 10°C to +85°C
	The Contractor shall supply all required low-loss coaxial cabling and a dedicated inline surge protector / lightning arrestor, fully sized and matched for the physical installation path.
Security features	Hardware NTP Reflector / DoS protection

C2: CBK - Official

Protocols	HTTPS secure web interface, SSH, and SNMPv3 support
Power supply	Dual redundant, hot-swappable power supplies (1+1 configuration)
Operating temperature	0 to 40°C
Operating humidity	10% to 80% non – condensing
Rack mounting	19-inch rack mountable, maximum 1U or 2U
EMC/certification requirements	CE, FCC, IEC 61000 or equivalent

HIGH AVAILABILITY

General

The ISS described in this document shall be implemented using a high-availability (HA) configuration for all system servers. The HA configuration shall ensure uninterrupted operation during hardware failures, network disruptions, or maintenance activities, with minimal impact on system performance and user access.

Each ISS subsystem shall support automatic failover, data redundancy, and real-time synchronization to ensure continued subsystem operation with no loss of critical data and minimal interruption to operator functionality.

To implement the HA environment, the Contractor shall establish dual servers for each sub-system at the LCRs, MSC, and SMSC server rooms.
The Contractor shall ensure that their design of the HA contains no critical single points of failure (SPOF) that could result in the failure of an entire subsystem.

C2: CBK - Official

HA Environment Architecture

The HA architecture shall operate in Active-Active or Active-Standby mode, as applicable to each subsystem and according to the manufacturer's best practices. Critical databases and configuration data shall utilize synchronous replication.

The automatic failover process shall restore full subsystem operation within a maximum of 60 seconds for Active-Standby configurations and shall support near- instantaneous (sub-second) failover for Active-Active configurations, with no loss of critical functionality or data.

The inter-server heartbeat network shall be physically or logically isolated from the production network infrastructure

Physical Architecture

a. The HA environment's physical array shall include the following components:

b. Two (2) separate physical servers from enterprise-grade tier-1 manufacturers.

c. The dedicated internal network connection (Interconnect / Heartbeat) between the two servers shall be implemented using a minimum of two (2) bonded/ aggregated network links to eliminate any single point of failure within the link itself.

d. The inter-server connection shall support sufficient throughput and low latency to ensure seamless real-time data replication and failover monitoring. For video management, AI analytics, and other bandwidth-intensive subsystems, the inter- server connection shall support a minimum bandwidth of 10 Gbps.

e. The shared storage system shall be fully redundant, including dual controllers, dual power supplies, RAID protection, and redundant SAN/iSCSI paths, eliminating any storage single point of failure.

The Contractor shall be fully responsible for the design of the high-availability (HA) array, including its hardware, software, and configuration, ensuring full compliance with all availability and performance requirements specified in this document.

To determine the hardware requirements for this array, the Contractor shall take into consideration the following factors:

a. The designed system must meet or exceed the performance requirements outlined in this chapter and elsewhere in this document.

b. The Contractor shall calculate the expected system load based on the assumption that all subsystems operate at full capacity simultaneously, as determined by the Contractor.

C2: CBK - Official

c. The Contractor shall account for a minimum of 30% future growth margin for all critical hardware resources, including CPU, memory, network bandwidth, and storage capacity, ensuring the system can handle future expansions and unexpected peak loads without degradation.

The proposed solution shall provide a minimum annual availability of 99.99%.

The HA architecture shall support software upgrades, security patching, and hardware maintenance without requiring subsystem shutdown.

The servers and storage technical specifications provided in this document represent minimum requirements only. The Contractor bears full responsibility for selecting appropriate hardware. System performance shall be thoroughly tested. Any degraded system performance caused by the server array's capabilities shall be resolved by the Contractor at its own expense, without any cost to the Client.

The Contractor shall perform HA failover and redundancy tests during FAT and SAT to demonstrate uninterrupted subsystem operation, data integrity, and automatic recovery capabilities

C2: CBK - Official

CCTV SYSTEM

General

All CCTV cameras in the project must comply with NDAA requirements.

All cameras in the project shall comply with applicable ONVIF profiles, including Profile S (streaming), Profile T (advanced video encoding and imaging), and Profile M (metadata and analytics).

All proposed fixed cameras shall include native, hardware-level edge AI processing powered by dedicated onboard Deep Learning Processing Units (DLPU/NPU) within next-generation System-on-Chip (SoC) architectures.

All video analytics, forensic metadata extraction (including person and vehicle classification), and behavioral rules shall be processed at the camera edge or through a hybrid architecture integrated with the VMS, with zero perceptible latency and no additional licensing fees.

All AI cameras shall support native metadata export to the VMS platform, enabling forensic search based on:

a. Human attributes.

b. Vehicle attributes.

c. Object classification.

d. Direction of travel.

e. Time and location.

Integration with PSIM

The PSIM system shall automatically display cameras monitoring the Areas of Interest (AOI) in which alarms are generated by other integrated systems (e.g., ACS, IDS, Etc).

The PSIM system shall allow operators to control PTZ cameras and perform digital zoom directly from the PSIM interface.

The PSIM system shall enable live and recorded video viewing from client workstations within the PSIM environment.
The integration between the PSIM and the CCTV system shall allow alarms and events from the CCTV system to be displayed in a format consistent with other system events. Such events and alarms shall include,

C2: CBK - Official

but not be limited to:

a. Camera malfunction.

b. Camera video loss.

c. Communication malfunction.

d. Tamper alarm.

From the PSIM workstation, it shall be possible to transmit at least the following commands to the CCTV system:

a. Manual selection of any camera for display on a selected monitor.

b. Manual selection and activation of a camera tour on a selected monitor.

c. Automatic display of alarm-triggered camera images on the PSIM workstation monitor or any other designated monitor.

5 MP AI Dome camera

Sensor type	1/2.8" CMOS
Lens	3.3 mm – 10 mm, Varifocal, motorized lens
Max resolution	2560 × 1920
Number of streams	2 Minimum
Viewing angle	Horizontal: 101.4° – 30.1°, Vertical: 69.6° – 21.8°
WDR	120 dB
Video compression	H.265/H.264
Frame rate	25 FPS at all resolutions
Video streaming	Multiple, individually configurable frame rate and bandwidth.

C2: CBK - Official

Edge AI analytics	Object classification (human, vehicle) Object type search filtering (Metadata) False alarm filtering Line crossing Intrusion / Area detection Loitering detection
	Region of Interest (ROI) encoding (smart compression) Tamper alarm
Deep learning	Required
Communication interface	1 RJ45 10M/100M self-adaptive Ethernet port
Inputs	1 input, 1 output
Shutter speed	1/15,000 max
Minimum illumination	Color: 0.14 Lux, B/W: 0 Lux with IR
IR illumination	Up to 30 m
Day/Night switch	IR cut filter
Users	20 simultaneous users and multi-cast support.
Protocols	IPv4; IPv6; UDP; TCP; HTTP; HTTPS; RTP/RTCP; IGMP V2/V3; ICMP; ICMPv6; RTSP; FTP; ARP; DHCP; APIPA (Auto-IP, link local address); NTP (SNTP); SNMP (V1, MIBII); SNMP (V3, MIBII); DNS; DNSv6; DDNS (DynDNS.org, selfHOST.de, no-ip.com); SMTP; iSCSI; UPnP (SSDP); DiffServ (QoS); LLDP; SOAP; CHAP; Digest authentication
Security	Password protection and user access control, HTTPS encryption and digest authentication, 802.1X port- based network authentication, Secure Boot, signed and encrypted firmware
ONVIF conformity	Support of S, T, M profiles
Power supply	PoE IEEE 802.3af / 802.3at

C2: CBK - Official

Operating temperature	-30 °C to 50 °C
Operating relative humidity	95% or less (non-condensing)
IP rating	IP 66
Impact protection	IK10
Protection	Against power surge
	Against lightening
	Against RFI

5 MP AI Bullet camera

Sensor type	1/2.8" CMOS
Lens	2.8 to 10 mm Varifocal motorized lens
Max. resolution	2592 × 1944
Min. illumination	0.0440 Lux, 0 Lux with IR
Number of streams	2 Minimum
Viewing angle	horizontal FOV: 98°to 28° vertical FOV: 71° – 22°
WDR	120 dB
Video compression	H.265/H.264
Frame rate	30 FPS at all resolutions
Video streaming	Multiple, individually configurable frame rate and bandwidth

C2: CBK - Official

Edge AI analytics	Object classification (human, vehicle) Object type search filtering (Metadata) False alarm filtering Line crossing Intrusion / Area detection
	Loitering detection Region of Interest (ROI) encoding (smart compression) Tamper alarm
Deep learning	Required
Communication interface	10/100BASE-T
Alarm inputs/outputs	1 input, 1 output
Shutter speed	1/25 min to 1/15,000 max
IR Illumination	Up to 50 m
Day/Night Switch	Auto/Schedule/Triggered by alarm in
Users	20 simultaneous users and multi-cast support.
Protocols	IPv4; IPv6; UDP; TCP; HTTP; HTTPS; RTP/RTCP; IGMP V2/V3; ICMP; ICMPv6; RTSP; FTP; ARP; DHCP; APIPA (Auto-IP, link local address); NTP (SNTP); SNMP (V1, MIBII); SNMP (V3, MIBII); 802.1x, EAP/ TLS; DNS; DNSv6; DDNS (DynDNS.org, selfHOST.de, no ip.com); SMTP; iSCSI; UPnP (SSDP); DiffServ (QoS); SOAP; CHAP; Digest authentication; SCEP
Encryption	Full end-to-end data encryption with supported VMS
ONVIF conformity	Support of S, T, M profiles
Power supply	PoE IEEE 802.3af / 802.3a
Operating temperature	-30 °C to 55 °C

C2: CBK - Official

Operating relative humidity	95% or less (non-condensing)
IP rating	IP 66
Impact protection	IK 10
Protection	Against power surge
	Against lightening
	Against RFI

8 MP AI Dome camera

Sensor type	1/2.8" CMOS
Lens	3.2 mm – 10 mm, Varifocal, motorized lens
Max resolution	3840x2160
Number of streams	2 Minimum
Viewing angle	Horizontal: 101.4° – 30.1°, Vertical: 55° - 17°
WDR	120 dB
Video compression	H.265/H.264
Frame rate	25 FPS at all resolutions
Video streaming	Multiple, individually configurable frame rate and bandwidth.
Edge AI analytics	Object classification (human, vehicle) Object type search filtering (Metadata) False alarm filtering Line crossing Intrusion / Area detection Loitering detection Region of Interest (ROI) encoding (smart compression) Tamper alarm
Deep learning	Required

Communication interface	1 RJ45 10M/100M self-adaptive Ethernet port
Inputs	1 input, 1 output
Shutter speed	1/5 - 1/12,000s Max
Minimum illumination	Color: 0.06 Lux, B/W: 0 Lux with IR
IR illumination	Up to 30 m
Day/Night switch	IR cut filter
Users	20 simultaneous users and multi-cast support.
Protocols	IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP, RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, UPnP, Bonjour, LLDP, CDP, SRTP (TCP, UDP Unicast), MQTT
Security	Encrypted firmware, Secure boot, signed firmware, Digest authentication, IEEE802.1X, HTTPS, WSS, IP- based access control, Encryption credentials
On-board analytics	Motion detection, video tampering alarm
ONVIF conformity	Support of S, T, M profiles
Power supply	PoE IEEE 802.3af / 802.3at
Operating temperature	-30 °C to 50 °C
Operating relative humidity	95% or less (non-condensing)
IP rating	IP 66
Impact protection	IK10
Protection	Against power surge
	Against lightening
	Against RFI

C2: CBK - Official

8 MP AI Bullet camera

Sensor type	1/2.8 " CMOS
Lens	2.8 to 10 mm Varifocal, motorized lens
Max. resolution	3,864 x 2,192
Min. illumination	0.0460 Lux, 0 Lux with IR
Number of streams	2 Minimum
Viewing angle	Horizontal 105° – 31°, Vertical 57° – 18°
WDR	120 dB
Video compression	H.265/H.264
Frame rate	30 FPS at all resolutions
Video streaming	Multiple, individually configurable frame rate and bandwidth
Edge AI analytics	Object classification (human, vehicle) Object type search filtering (Metadata) False alarm filtering Line crossing Intrusion / Area detection Loitering detection Region of Interest (ROI) encoding (smart compression) Tamper alarm
Deep learning	Required
Communication interface	10/100BASE-T
Alarm inputs/outputs	1 input, 1 output
Shutter speed	1/25 min to 1/15,000 max
IR Illumination	Up to 45 m

Day/Night Switch	Auto/Schedule/Triggered by alarm in
Users	20 simultaneous users and multi-cast support.
Protocols	IPv4; IPv6; UDP; TCP; HTTP; HTTPS; RTP/RTCP; IGMP V2/V3; ICMP; ICMPv6; RTSP; FTP; ARP; DHCP; APIPA (Auto-IP, link local address); NTP (SNTP); SNMP (V1, MIBII); SNMP (V3, MIBII); 802.1x, EAP/ TLS; DNS; DNSv6; DDNS (DynDNS.org, selfHOST.de, no ip.com); SMTP; iSCSI; UPnP (SSDP); DiffServ (QoS); SOAP; CHAP; Digest authentication; SCEP
Encryption	Full end-to-end data encryption with supported VMS
On - board analytics	Object in field, Line crossing, cameras tampering
ONVIF conformity	Support of S, T, M profiles
Power supply	PoE IEEE 802.3af / 802.3a
Operating temperature	-30 °C to 55 °C
Operating relative humidity	95% or less (non-condensing)
IP rating	IP 66
Impact protection	IK 10
Protection	Against power surge
	Against lightening
	Against RFI

PTZ IR camera 4 MP

Image sensor	1/1.8" CMOS
Lens	4.3 – 137 mm
Digital zoom	X16
Resolution	2592x1520
Video compression	H.265/H.264/MJPEG
Min. illumination	Color: 0.04 Lux 0 Lux with IR illumination on
Day and night	Automatically removable infrared-cut filter
IR range	150 meter
Shutter speed	2 - 1/12,000sec
Frame rate	60fps/50fps (60Hz/50Hz) (WDR off) / 30fps / 25fps (60Hz/50Hz) (WDR on)
Network	RJ45, 10BASE-T/100BASE-TX PoE RJ45 Push-pull Connector (IP66) Audio and I/O connectivity
Streaming	The camera shall support a minimum of 20 simultaneous unicast and multicast connections
Protocols	IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP, RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SFTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, UPnP, Bonjour, LLDP, CDP, SRTP (TCP, UDPUnicast), MQTT
Security	Password protection, IP address filtering, HTTPSa encryption, IEEE 802.1x (EAP-TLS) a network access control, Digest authentication, User access log,
	Centralized Certificate Management, Brute force delay protection, signed firmware, secure boot, secure keystore (CC EAL4 certified), TPM

C2: CBK - Official

Edge AI analytics	Object classification (human, vehicle) Line crossing Intrusion / Area detection Loitering detection Auto-Tracking Tamper alarm
ONVIF conformity	Support of S, T, M profiles
On- board analytics	Line crossing, Enter / leave field, Loitering
IP rating	IP 66
Impact protection	IK 10
Pan/Tilt range	Pan: 360° endless
Pan / Tilt speed	0.1°/s - 120°/s (pan)
Local storage	SD/SDHC memory card slot
Power source	24 VAC, IEEE802.3bt, Type 3 standard
Operating Conditions	0 C to 55 C
Operating humidity	10–100% RH (condensing)

C2: CBK - Official

Thermal camera

Image sensor	Vanadium Oxide Uncooled Focal Plane Arrays
Focal length	35mm
Digital zoom	×2, ×4, ×8
Resolution	640 × 512
NETD	< 35 mk
Temperature range	-20 °C to 150 °C
Network	RJ 45 (10/100 Base T)
Edge analytics	line crossing, intrusion, region entrance, and region exiting
Analytics range	350 M, Minimum
Security	Password protection, IP address filtering, HTTPS encryption, IEEE802.1x network access control
ONVIF conformity	Support of S, T, M profiles
Dry contacts	At least 1
IP rating	IP 66
Impact protection	IK 10
Power supply	24 VAC ± 25%, PoE
Operating Conditions	0 C to 55 C
Operating humidity	90% RH (condensing)

C2: CBK - Official

Camera pole

The pole shall be engineered to support a maximum weight, which will be calculated based on the weight and cross-sectional area of:

a. Three (3) CCTV cameras with their housing. b. One (1) horn speaker.

The pole shall include a pre-manufactured opening at its base to provide access to the camera cables. This opening will be covered with a secure, screw-locked cover, ensuring a tight seal to prevent water ingress.

The pole shall be constructed from steel and will be hot-dip galvanized on both the internal and external surfaces, in accordance with the national standard for zinc galvanization. The galvanization thickness will be no less than 90 microns.

The pole's cross-section and material thickness shall be engineered to ensure high stability, such that the top of the pole does not deviate by more than 1° from its vertical axis at wind speeds of up to 120 km/h.

The pole shall be mounted on a concrete foundation designed by a certified civil engineer, based on the pole's weight, required stability, and the soil conditions at the installation site.

A lightning rod shall be installed at the top of each pole and properly grounded in accordance with the relevant national standards.

The drawing below presents a conceptual representation of the required camera pole.

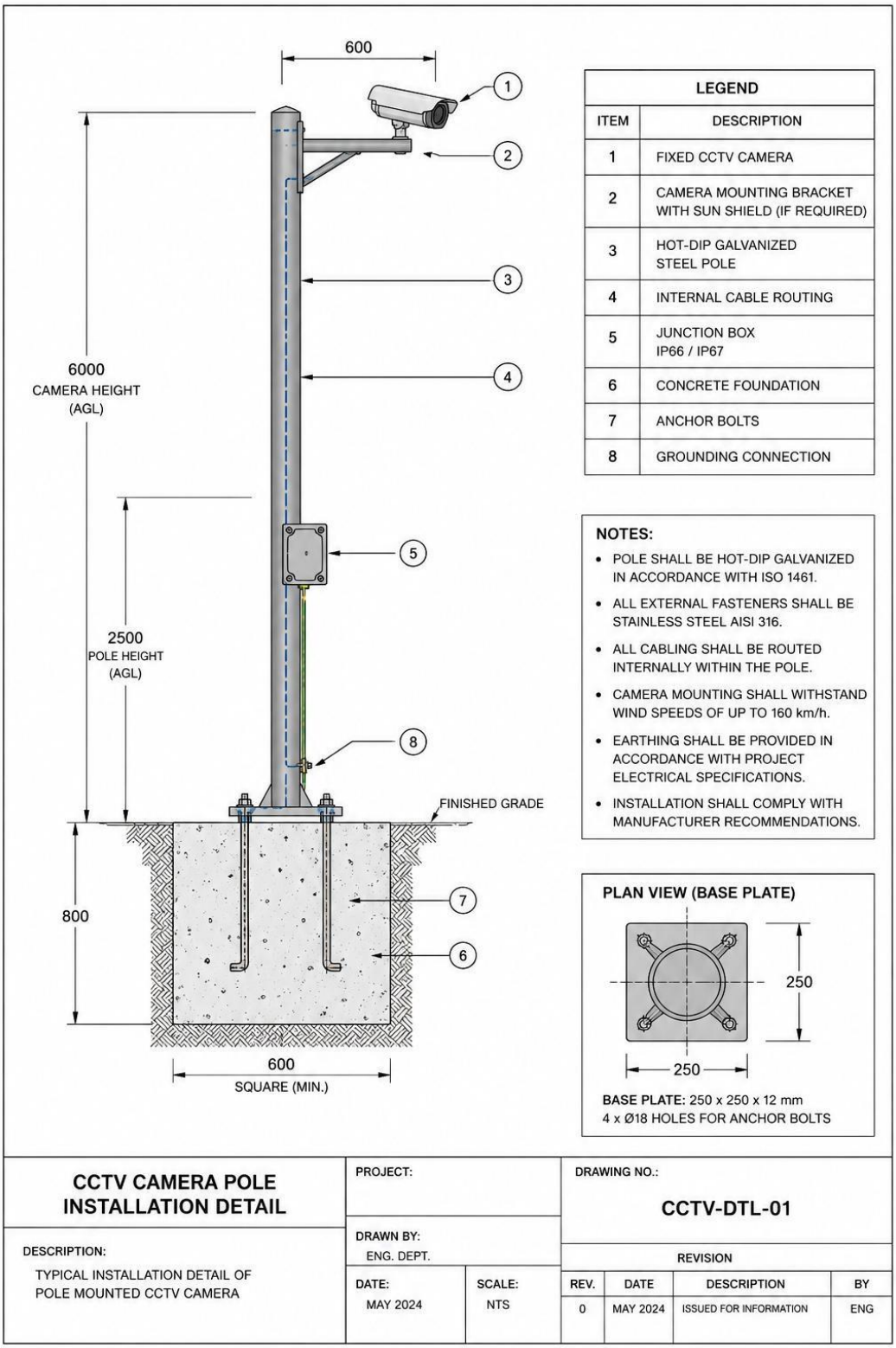

FIGURE 10 - DEDICATED CAMERA POLE

Wall/fence mounted pole

The wall-mounted camera pole shall extend at least one (1) meter above the perimeter wall (including any fence above it) and shall be specifically designed for CCTV camera installation.

The wall-mounted pole shall comply with the same technical specifications as the self- supported pole.

The drawing below presents a conceptual representation of the required wall mounted camera pole.

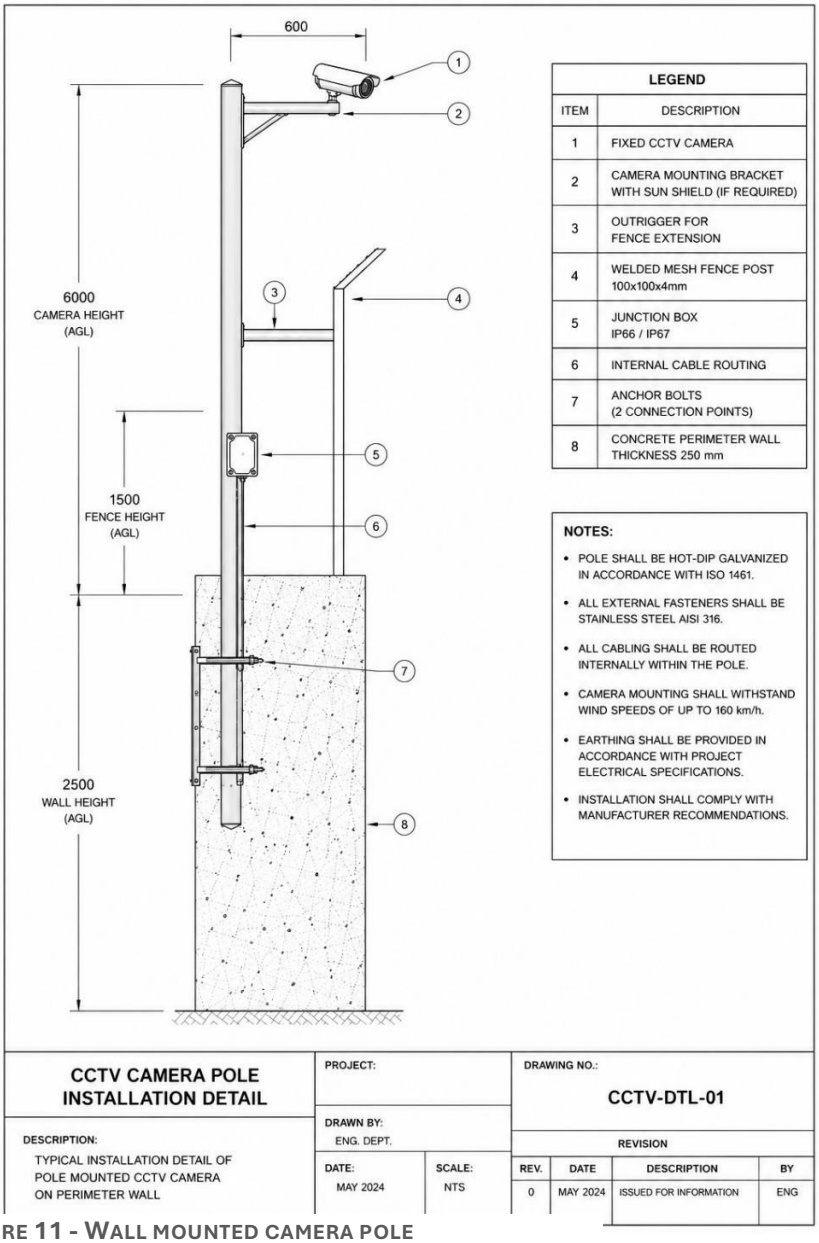

FIGURE 11 - WALL MOUNTED CAMERA POLE

VIDEO MANAGEMENT SYSTEM

General

The Video Management System (VMS) solution shall be an enterprise-class platform supporting centralized and distributed access to video, audio, metadata, and related system resources across the ISS, with access rights enforced per user role and per site in accordance with predefined user roles, privileges, and site-specific permissions.

The VMS shall support multi-site, multi-client operation and large-scale CCTV camera deployments.

The VMS solution shall be fully scalable and capable of supporting enterprise-scale expansion of sites, cameras, workstations, recording servers, and storage resources through software licensing and hardware expansion without requiring replacement of the core VMS platform.

The VMS shall support simultaneous live viewing, recording, playback, export, analytics, and management operations without degradation of recording integrity or system stability.

The VMS shall provide storage capacity for all camera video streams, at the cameras' resolution for retention period as specified in the BOQ.

System architecture

The VMS shall be based on a federated architecture enabling multiple independent VMS sites to be interconnected under a unified management framework.

Each site shall operate autonomously, including local video recording, storage, and playback, and shall continue full operation in the event of loss of connectivity to other sites.

The system shall keep video streams local to each site and shall transmit video over inter-site networks only upon user request or in response to defined events or alarms. The system shall support recording capabilities at both the MSC and SMSC in addition to local site recording for a selected number of cameras.

Loss of the federation management server shall not affect local site recording, playback, alarm handling or operator functionality.

The users at the MSC and SMSC shall be able to access video from all sites, while users at individual sites shall be restricted to accessing video from their respective sites only. Additionally, administrators shall be able to centrally manage all sites within thehierarchy through the Management Client, in accordance with their administration rights for each individual site.

C2: CBK - Official

The VMS shall support centralized and/or distributed user management, including role-based access control (RBAC), allowing permissions to be defined by site, camera, function, and time schedule.

All communications between servers, clients, storage systems, and federated sites shall be authenticated and encrypted using industry-standard protocols including TLS 1.2 or higher. All network communications between clients and servers, as well as between servers, shall be encrypted. The VMS shall implement strong data protection measures, including encrypted password storage and automatic user logout following a defined period of inactivity.

The VMS solution shall be scalable and shall allow the addition of new sites, servers, and cameras without degradation of performance or availability of existing sites.

Failure, maintenance, or network disconnection of any single site shall not affect the operation or availability of other sites within the federation.

The local recording at each site shall be implemented in an N+1 redundant configuration.

The required VMS solution shall enable the LCR's at the various sites to operate independently and perform all tasks including:

a. Manage the VMS (users view, creating groups and tress, camera tours and schedules, adding and removing devices, schedules and time, exporting and coping video streams, etc).

b. View live video.

c. View recording video.

d. Select and operate cameras (PTZ, digital zoom, etc.).

The required solution shall enable MSC and the SMSC to:

a. Manage the configuration of VMS at remote sites.

b. View of live and recorded videos, audio, and metadata from the remote sites.

c. Retrieve scheduled and/or event-triggered and/or user-initiated, and/or automatic recordings from remote sites to the MSC.

d. Record video from local sites.

C2: CBK - Official

e. Ensure stable client login times not exceeding ten (10) seconds, regardless of the number of sites, response time of remote sites, or network connection state.

f. Select and operate cameras (PTZ, digital zoom, etc.).

g. Select and operate cameras (PTZ, digital zoom, etc.).

The VMS solution shall support ONVIF Profiles S, G, T, and M for interoperability with IP cameras, recording devices, and metadata/analytics systems.

The VMS solution shall be based on a client-server application. The servers will provide functionality to all connected clients using Windows services. These Windows services will run in the background.

Edge intelligence and forensic search integration

The VMS solution shall support integration with edge intelligence (camera-based analytics) and third-party server-based analytics. The platform shall support the following AI analytics and forensic search capabilities:

a. Object Classification (Human, Vehicle): The VMS shall natively (or through integration) ingest and process real-time edge-classification metadata from camera sensors, accurately differentiating between humans, vehicles, and other moving objects.

b. Object Type Search Filtering (Metadata): The VMS forensic search interface shall allow operators to query archived metadata timelines using multi-conditional filters. Users shall be able to filter search results by object type (e.g., "Person" or "Vehicle") and secondary attributes (e.g., color, direction).

c. False Alarm Filtering: The VMS shall support and preserve object-classification metadata and nuisance-alarm filtering information generated by edge analytics or integrated analytics engines.

d. Line Crossing: The VMS shall ingest directional line-crossing events generated by edge cameras and allow operators to map these events to real-time alarms, map pop-ups, and automated forensic bookmarks.

e. Intrusion / Area Detection: The VMS shall seamlessly receive and log "Object Entered Area" and "Object Loitering Inside Area" triggers from the edge. The VMS interface shall support the visual overlay of these detection zones during both live view and playback modes

f. Loitering Detection: The VMS shall recognize time-threshold metadata transmitted by edge cameras. If an object remains inside a designated zone longer than a user-defined period, the VMS shall instantly generate a high-priority alert and tag the video archive for rapid forensic retrieval.

g. Region of Interest (ROI) Encoding (Smart Compression): The VMS shall fully support edge-based smart compression technologies (e.g., H.264/H.265 ROI encoding). The VMS shall record the stream ensuring non-ROI background areas are highly compressed to optimize storage, while moving objects and ROI zones maintain maximum forensic image quality

h. Smart Motion Search (Post-Incident): The VMS shall enable operators to find motion within specific regions of interest (ROI) defined after an event occurs, without requiring pre-configured server or edge analytic rules.

i. Bookmarks and Evidence Export: The VMS shall enable tagging relevant video segments with user notes and exporting them in secure, encrypted formats with digital signatures to maintain a verifiable chain of custody.

j. Tamper Alarm: The VMS shall immediately alert operators to camera tampering events, including lens masking/blocking, sudden defocusing, and severe camera redirection or camera angle changes.

Performance criteria

a. A multi-conditional metadata search query spanning up to 30 days of archives across at least 150 cameras shall return initial results within 20 seconds under normal operating conditions and manufacturer-recommended hardware sizing.

b. latency between the event trigger at the camera level (e.g., Tamper Alarm, Line Crossing) and the visual/audible alert rendering on the VMS Operator Client workstation shall not exceed two (2) seconds (assuming a network latency under 20ms).

Should the required capabilities detailed above necessitate any specialized add-ons or dedicated licenses, all associated costs shall be fully absorbed and included within the baseline VMS software or the video channel license pricing.

While the analytics and forensic search framework specified herein is primarily based on edge intelligence, the Contractor shall be permitted to propose a hybrid topology combining edge processing and server-side VMS analytics (Edge + VMS Server-Side). Should the proposed solution require dedicated servers, hardware appliances, or specialized software licenses to fulfill these analytical and indexing requirements, all associated costs shall be fully absorbed and included within the baseline VMS software or individual video channel license (Camera License) pricing. No additional or separate line-item costs for dedicated analytic servers or software middleware shall be accepted. No additions or exceptions shall be approved in any configuration, including software, hardware, or system settings.

C2: CBK - Official

Live viewing

Live video images shall be viewable at configurable frame rates up to 30 frames per second (FPS) and at configurable resolutions up to 4K (3840 × 2160). The system shall allow individual configuration of frame rate and resolution per camera channel, independently from the recording parameters.

Recorded video viewing shall not interrupt, degrade, or otherwise affect continuous video recording under any operating conditions.

Live video streams shall be displayed on live video monitors through the PSIM software. The system shall support simultaneous display of up to sixteen (16) camera streams on a single monitor.

Live video streams shall be viewable within the PSIM workstation interface as part of event-driven incident and alarm management, without the need to launch external applications.

The recording servers shall support simultaneous streaming of live video to VMS clients and PSIM workstations at the configured recording frame rate and resolution, without impacting recording performance.

Live video viewing shall be possible through manual selection of cameras for display on a specific monitor, and Predefined viewing layouts or scenarios. Camera selection and viewing control shall be available from both the VMS client and the PSIM workstation interface.

Virtual Matrix

The Virtual Matrix shall manage the display of live and recorded video streams from all connected cameras across operator workstations and large monitors.

Display of camera images shall be managed via a virtual matrix configuration, enabling all standard display modes, including but not limited to “Full Screen,” “Quad,” etc.

The virtual matrix shall be fully integrated with the PSIM software, ensuring seamless correlation between PSIM alarm event handling and the display of associated camera images. This integration shall support, at a minimum, the following features:

a. Displaying an array of cameras on predefined monitors in various display modes (e.g., “Full Screen,” “Quad,” etc.) triggered by an alarm event or any other event, such as an intercom call or an ACS access event.

b. Returning all screens to a predefined scenario when no active alarm is being handled in the PSIM.

c. Advanced management of video for several events occurring at the same time on a dedicated alarm monitors (for example displaying one camera in a full screen mode on one monitor then changing into quad when the second alarm occurs, then displaying the 3rd event on a second monitor and displaying any additional

event in a sequence on that second monitor).

d. Closing specific video displays in response to acknowledgment or resetting of an alarm event on the PSIM workstation.
e. Displaying predefined live video, recorded video, or a combination of both, side by side, in response to a PSIM event.

f. Manual activation of predefined video scenarios, including selection of cameras and arrangement of various screen layouts.

g. Automatic positioning of PTZ cameras to a predefined location ("Preset") in response to an event or following a predefined period of PTZ inactivity.

Operators shall be able to manually configure, save, and recall display scenarios.

The system shall allow drag-and-drop camera assignment to any display window.

The Virtual Matrix interface shall support intuitive control of PTZ cameras, including presets and tours.

Operators shall have access to event logs correlated with video actions

VMS software features

The VMS platform shall provide centralized management of all cameras, recording servers and video walls.

The VMS platform shall be fully integrated with the PSIM platform, access control system, intrusion detection system intercom, LPR, and building management systems (BMS).

The platform shall support multi-site and federated architectures, allowing multiple recording servers and management servers across geographically distributed locations.

The VMS platform shall support standard protocols for IP cameras (ONVIF Profile S/G/T), analog encoder devices, and third-party integration via SDK/API.

The VMS shall provide continuous, scheduled, and event-triggered recording for all cameras.

The VMS shall Support multiple video streams per camera (high resolution, low resolution, sub-streams) with configurable frame rates and compression (H.264, H.265, MJPEG). Support of recording frame rate shall be up to 60 FPS.
The VMS solution shall support redundant recording servers and failover recording in case of server failure.

Archival storage shall be configurable, including local, network, and central storage options.

The VMS shall support enterprise-scale scalability of at least 10,000 cameras, 50 concurrent users, and 50 client workstations within a single federated deployment. Expansion to these capacities shall be achieved through software licensing and hardware scaling without requiring replacement of the core VMS platform or architectural redesign.

Recording retention policies shall be configurable per camera, per event type, and per site.

Playback initiation of recorded video shall commence within a maximum of 2 seconds from the time of operator request.

The VMS shall provide live viewing of all cameras via various Client options, with support for multi-monitor and multi-screen layouts.

Operators shall be able to drag-and-drop cameras, define custom grids, and save/recall predefined views.

Playback shall support simultaneous review of multiple cameras, timeline navigation, and event-based search.

Integration with Smart Wall / virtual matrix shall allow displaying live and recorded video on large monitors and video walls.

The VMS shall support alarm/event handling, including:

a. Input from access control, intrusion detection, LPR, and intercom systems. b. Event-triggered camera recording, PTZ presets, or layout changes.

Operators shall receive notifications of events with live camera feed pop-ups and linked maps.

Event correlation and rules shall be configurable to automatically respond to complex scenarios.

Analytics shall be integrated with event rules, enabling automatic camera actions, alarms, and logging.
The VMS shall support third-party AI analytics modules via SDK or NVIF extensions.

The VMS shall support Role-based access control (RBAC) with configurable user permissions for cameras, playback, alarm handling, and configuration.

The VMS shall include audit logging of all user actions and system events.

The VMS shall include End-to-end encryption of video streams, client-server communications, and storage.

The VMS shall support integration with Active Directory / LDAP for user authentication and management.

The VMS shall support Failover and load balancing for continuous operation under maximum load. When a previously failing recorder comes back online, the system shall automatically revert to the original recorder without operator intervention. Failover and fallback operations shall occur transparently, with no disruption to connected clients, including live viewing, playback, and recording. All connected clients shall continue operating normally during failover and fallback, maintaining uninterrupted access to video streams.

The VMS shall support integration with PSIM systems, access control, intercom, LPR, and building automation systems.

The VMS shall support event-triggered actions such as PTZ presets, camera popping, and video wall layout changes.

Video storage shall be managed using a FIFO (First-In, First-Out) mechanism, excluding recordings marked as protected or permanently retained.

The retention period of stored videos shall be configurable via the workstation on a per-video-channel basis, and such video shall be protected from being overwritten.

The system shall automatically detect video loss conditions (including camera disconnection or stream interruption) and generate corresponding alarms on PSIM operator workstations. Video loss events shall be monitored continuously and shall trigger real-time alarms displayed on PSIM workstations.

The On-Screen Display (OSD) text shall support a minimum of 16 characters.

The VMS shall support at least the following recording modes:

a. Continuous Recording: Cameras shall record continuously 24/7 or during configured operating hours.

b. Recording on Demand: Operators shall be able to manually start and stop recording for selected cameras at any time.

b. Pre-Scheduled Recording: Recording shall follow predefined schedules, configurable per camera, allowing automatic start and stop based on time, day, or event triggers.

The VMS shall support at least the following recording and playback Features:

a. Regular Playback: Support continuous playback of recorded video for at least the last 24 hours.

b. Synchronized Playback: Allow synchronized playback of up to 16 cameras according to timestamp.

c. Frame-by-Frame Playback: Enable precise review of video frame by frame.

d. Slow Motion Playback: Support slow forward playback at 1/2 of the normal recording rate.

e. Fast Forward Playback: Support fast forward playback at speeds of at least 2×, ×, and 8× the normal recording rate.

The VMS platform shall support the following video review tools a. Snapshot: capture still images from video playback.

a. Digital Zoom: zoom into a section of the playback window without altering the original video.

b. Visual Timeline: graphical representation of recording and events for easy navigation.

c. Split Playback: simultaneous review of multiple camera streams in the same window.

d. Lock: protect selected video segments from being overwritten or deleted. f. Tag: add annotations or bookmarks to video segments for quick retrieval. g. Smart Search: search for motion, objects, or events within recorded video.

e. Video Synopsis: summarize long-duration video into condensed playback highlighting motion or events.

f. Thumbnail View: display a grid of frame thumbnails for fast navigation.

g. Event Mask: overlay event markers or zones on video playback to highlight larm or analytic events.

The VMS shall support video Enhancement. The platform shall provide an image toolkit utility that allows users to enhance individual video frames. Available enhancements shall include, at a minimum: brightness, contrast, sharpness, saturation, white balance, and digital zoom. Enhancements shall be applied only to copies of video frames. The original recorded video shall remain unaltered. During video playback, the user shall be able to zoom into a section of the playback window.

The system shall support digital zoom function. Video playback shall continue normally while zoomed. The zoom operation shall be non-destructive and shall not alter the original recorded video.

Users shall log in to the system using a unique username and password. Unsuccessful login attempts shall prevent access to the system, with configurable lockout policies to protect against unauthorized access. Access to cameras, monitors, playback, and system functions shall be governed by the user's assigned authorizations.

The system shall support server-based privacy zones that can mask or pixelate designated areas of camera images. Hidden or masked areas can be made visible only with appropriate authorization.

The system shall allow deletion of recorded video only with proper authorization and documented justification.

All user actions related to privacy, recording suspension, and deletion shall be fully logged to ensure traceability and accountability.

The system shall support real-time audio streams that are lip-synchronous with the associated video streams, ensuring audio and video are synchronized during live monitoring and playback.

The system shall support storage of video data on all well-established media, including but not limited to:

a. Internal hard disks.

b. RAID-protected configurations.

c. USB hard disks.

d. Storage volumes including enterprise-supported RAID

e. SAN (Storage Area Network).

f. NAS (Network-Attached Storage).

The system shall allow simultaneous display of live and archived video from the same camera. Operators shall be able to view the live feed alongside historical recordings in a single interface without interrupting either stream. This functionality shall support synchronized playback, allowing easy comparison of live and archived footage.

The system shall allow export of continuous and non-continuous video data from one or multiple cameras. Exported video shall be in a standard, displayable format, such as MP4. Exported video shall preserve timestamps, metadata, camera identifiers, and evidentiary integrity through watermarking or digital signature mechanisms. Exported files shall be accessible only to authorized users according to system RBAC policies.

The system shall support cascading site plans, allowing hierarchical linking of maps and floor plans (e.g., floor plans linked to each other and to the building map). Linking shall enable both quick navigation between levels and summary visualization of camera and alarm status across the entire building or site.

The system shall support placing cameras, views, and IO ports on site plans and GIS maps. The status of all items on the map or site plan shall be updated dynamically in real time. Quick access to cameras and views shall be enabled via double-click or drag- and-drop operations.

C2: CBK - Official

The VMS shall support cybersecurity hardening features including secure boot, certificate management, role-based administration, audit logging, password policies, and secure API authentication.

The system shall continuously monitor the operational health of cameras, recording servers, storage systems, analytics services, and network connectivity, and shall generate alarms upon detection of faults or degradation.

All VMS components, recording servers, clients, and cameras shall support synchronization with centralized NTP time sources.

VMS server

All requirements stated herein are minimum requirements. The Contractor shall provide a VMS server that fully meets the functional and technical requirements of the system. The server hardware and software shall be designed to ensure continuous, uninterrupted operation under maximum load conditions, without any degradation in performance.	
Make	Dell, HP or approved equivalent
Operating system	Microsoft Windows Server 2022/2025, Standard
CPU	Intel Xeon Scalable Gen 4 or newer processor, minimum 20 physical cores, minimum base frequency 2.2 GHz, enterprise-class server CPU optimized for virtualization and 24/7 operation
Storage	2 × 960 GB SSD (RAID1)
RAM	64 GB DDR5 ECC RAM
Network	2x10 GbE
Security	TPM, Secure Boot, Lifecycle Controller, signed firmware
Communication outputs	Ethernet Port, 2 USB 3.0 ports ,VGA, RJ 45

C2: CBK - Official

Fan	Hot-swappable, redundant fans, high performance gold, Variable speed, Front-to-back airflow, Designed for 24/7 operation
Power supply	100–240 V AC, 50/60 Hz, Redundant, hot-swappable PSUs (1+1 configuration), Power failure alert via iDRAC9
Operating temperature	10–35°C
Humidity	80% RH, non-condensing
Form factor	1U Rackmount

Recording server

All requirements stated herein are minimum requirements. The Contractor shall provide a recording server that fully meets the functional and technical requirements of the system. The server hardware and software shall be designed to ensure continuous, uninterrupted operation under maximum load conditions, without any degradation in performance.	
Make	Dell, HP or approved equivalent
Operating system	Microsoft Windows Server 2022/2025 Standard or newer supported version
Redundancy	N+1 failover recording support required
CPU	Dual Intel Xeon Scalable processors (4th Generation or newer), minimum combined 24 physical cores
RAID configuration	Hardware RAID controller supporting RAID 1, 5, 6, and 10 with cache memory and battery-backed or flash-backed write protection
RAM	Minimum 64 GB DDR5 ECC RAM, expandable to 256 GB minimum

Throughput	Support continuous recording, playback, and live streaming simultaneously without frame loss
Recording storage	Storage sizing shall be calculated based on: Number of cameras Resolution and frame rate Compression type (H.264 / H.265) Retention period as specified in the BOQ
HDD type	Enterprise-grade hot-swappable HDDs designed for continuous 24/7 surveillance workloads
Number of cameras for machine	As per specified in the BOQ. Recoding at 25 FPS at cameras resolution.
OS / Database storage	2 × 480–960 GB SSD in RAID1 for OS + database
Security	Hardware TPM 2.0 (Trusted Platform Module), Secure Boot enabled, signed firmware enforcement, secure out-of-band remote management, and support for Microsoft BitLocker full-disk encryption
Network	2 × 10 GbE or higher
Fan	Hot-swappable, redundant fans, high performance gold, Variable speed, Front-to-back airflow, Designed for 24/7 operation
Power supply	100–240 V AC, 50/60 Hz, Redundant, hot-swappable PSUs (1+1 configuration), Power failure alert via iDRAC9
Operating temperature	10–35°C
Humidity	80% RH, non-condensing
Form factor	2U Rackmount

VMS client workstation

All requirements stated herein are minimum requirements. The Contractor shall provide a VMS Client workstation that fully meets the functional and technical requirements of the system. The Clint workstation hardware and software shall be designed to ensure continuous, uninterrupted operation under maximum load conditions, without any degradation in performance.	
Make	Dell, HP or approved equivalent
CPU	12th Generation Intel® Core™ i9 or equivalent
Operating system	Windows 11 Pro or Enterprise 64-bit
SSD	1 TB NVMe SSD minimum.
Memory	Minimum 64 GB DDR5 RAM, expandable to 128 GB
GPU	NVIDIA RTX A-Series professional GPU with minimum 8 GB dedicated VRAM and support for hardware decoding of H.264/H.265 streams
Audio/video decoding	The workstation shall support simultaneous decoding and display of multiple H.264/H.265 video streams without frame loss
Network	10 GbE
Security	TPM 2.0, Secure Boot, BitLocker support
Display	Support simultaneous operation of minimum four (4) monitors at 4K resolution (3840×2160) at 60 Hz
Ports	4 × USB 3.x 2 × USB-C Audio interface
Display output	4 × DisplayPort 1.4 or HDMI 2.1 outputs
Input voltage	90 V AC to 264 V AC

Operating temperature	10–35°C
Operating humidity	20 -80% RH (non-condensing)
Accessories	Supplied complete with keyboard and mouse

24’ monitor

Size	24" LED display
Panel type	IPS, LED-backlit LCD, Anti-glare, matte
Refresh rate	60 HZ
Resolution	1920x1080
Response Time	5 ms or lower
Brightness min.	250 cd/m²
Interface	HDMI, DisplayPort, USB-C, audio line-out
Aspect ratio	16:9
Contrast ratio	Minimum 1000:1
Operating temperature	0 to 40°C
Operating humidity	10% to 80% (non – condensing)

VIDEO WALL

Functional requirements

The proposed solution may consist of an integrated video wall processor, matrix switcher, software-based video wall management platform, or a dedicated video wall controller integrated with a Video Management System (VMS), provided that all functional requirements specified herein are fully supported.

The system will enable the display of various sources (workstation screens, cameras, live video feeds, documents, web pages, TV) simultaneously, in varying sizes, or as one large image.

he system shall support multiple display modes, including auto view, quad view, parallel view, Picture-in-Picture (PIP) view, and full-screen view.

The system shall allow rapid switching or reassignment of content sources across different zones or the entire video wall.

The system shall allow content to be displayed flexibly, either as a single unified image across all screens (“video wall mode”) or as multiple content sources assigned to different zones or individual screens.

The system shall allow creation of customizable layouts (e.g., windows, quadrants) and enable saving and recalling of preset arrangements.

The system shall display content at its native aspect ratio and resolution without distortion, stretching, or pixelation. The system shall support Full HD, 4K UHD, and 8K input sources and shall allow scaling for display across the video wall while maintaining image quality.

The system shall allow overlay of text, graphics, or tickers on video content.

The system shall support the display of up to four image layers on a single screen, allowing multiple content sources (such as video feeds, graphics, or documents) to be overlaid simultaneously. Each layer shall be independently controllable in terms of size, position and transparency.

The system shall support drag-and-drop functionality, allowing users to assign content sources to specific screens or zones by simply dragging them onto the desired location on the video wall.

The system shall support 1/4/9/16/32 window division modes and full-screen switch of the window.

The system shall support live viewing in both roaming windows and a live view list, allowing users to monitor multiple sources simultaneously. Roaming windows shall be movable, resizable, and maintain live playback independently of other display configurations. The function shall support drag-and-drop, zoom, and full-screen expansion features.

C2: CBK - Official

The system shall allow programming of presets for the various viewing modes and shall support at least 16 preset configurations. The system shall allow automatic tours between presets, including the ability to set the display duration for each preset.

The system shall support moving video content across multiple screens, allowing users to dynamically reassign sources from one screen or zone to another without interrupting playback.

The system shall be modular and scalable to accommodate future growth and changing organizational needs, such as adding more input sources or expanding the display size.

The system shall support real-time video processing and display. The end-to-end latency between the source input and the video wall display shall not exceed 200 milliseconds under normal operating conditions and manufacturer-recommended system sizing.

The system shall support automatic recovery following power interruption and shall restore the last active layout, presets, and display configuration upon restart.

The system shall support multi-user access with configurable user roles and permissions for operators, supervisors, and administrators.

The system shall support automatic display actions triggered by events or alarms received from integrated systems such as VMS, PSIM, access control, or intrusion detection systems.

The system shall support seamless KVM control, allowing operators to manage multiple sources on the wall using a single mouse and keyboard

Video wall management console

Control of the video wall shall be performed via a dedicated management touchscreen panel.

The management panel shall have a screen size of 10 to 12 inches and a resolution of at least 1920 × 1200 pixels. The screen brightness shall be at least 500 nits, suitable for indoor environments with controlled or high ambient lighting

The management panel shall allow the user to assign any input to any output anywhere on the video wall.

The panel shall provide the ability to power on/off individual wall-mounted screens and to control the audio volume for each input, output, or screen.

Audio management functional requirements

Each source shall be connected to the input card along with its corresponding video input.

The system shall support both analog and digital audio formats.

The matrix shall be capable of connecting to multiple speakers within the room.

The matrix shall allow complete separation between video and audio, enabling audio playback from a source even if its video is not displayed.

Audio volume shall be controllable from a computer, tablet, or the control panel system.

The system shall support audio routing independently of video routing, including audio breakaway functionality between inputs and outputs.

Cyber security

The Video Wall Management system shall support:

a. Role-based access control (RBAC).

b. Active Directory / LDAP integration.

c. TLS 1.2 or higher.

d. Audit logging.

e. Secure password policies.

55’ screen

Operation hour	24/7 continuous operation
Screen Size	55"
Bezel	0.9 mm
Panel Type	IPS / Direct-LED backlit panel
Resolution	Native resolution: 1920 × 1080 (Full HD). The display shall support input resolutions up to 3840
	× 2160 (4K) at 60Hz and support 4K signal daisy-chain functionality
Brightness	500 nits (Minimum)
Contrast ratio	1,300:1 (Minimum)
Refresh rate	60 Hz or higher
Anti-glare panel	Anti-glare industrial-grade panel with minimum 28% haze
Image retention protection:	Embedded anti-image retention mechanism including pixel shifting and burn-in prevention features

Response time	8ms
Viewing angle	178°(H) / 178°(V)
Display color	10 Bit (1.07 Billion colors)
Inputs	2 × HDMI 2.0, 1 × DisplayPort 1.2, 1 × RS232, 2 × USB, 1 × Audio, 1 × IR
Outputs	1 × DisplayPort (Loop-through) and/or 1 × HDMI (Loop-through), 1 × RS232 (Loop- through), 1 × Audio
Daisy-chain capability	Video walls support built-in video wall controller with daisy-chain capability
Control mode	IR remote control and RS232 control interface with support for centralized remote PC management
Panel lifetime	Minimum 50,000 hours
MTBF	Minimum 50,000 hours
Power supply	100–240VAC, 50/60Hz
Operating temperature	0°C to +40°C minimum
Mounting Compatibility	VESA compliant mounting interface (minimum 400 × 400 mm)
Certification	Certifications CE, FCC, RoHS compliant

Video Wall Mounting Structure and Brackets

The contractor shall provide a heavy-duty, industrial-grade mounting structure (wall- mounted or floor-standing) capable of supporting the combined weight of the entire video wall array.

The mounting brackets must support full front-service access, allowing any individual screen within the matrix to be extended forward independently for maintenance without disturbing adjacent screens.

The brackets shall feature multi-axis toolless micro-adjustments (X, Y, and Z planes) to ensure flawless alignment and seamless leveling of the 0.9 mm screen bezels.

The mounting solution shall include integrated cable management paths to ensure all power and signal cables are safely routed, organized, and free from strain during bracket extension

INTELLIGENT VIDEO ANALYTICS

General

AI analytics solution shall be used in selected locations for outdoor applications. The solution shall support reliable operation in outdoor surveillance environments under varying lighting and weather conditions.

The IVA solution shall enable automated detection, classification, and analysis of security events using advanced AI and deep-learning algorithms applied to video streams.

The system shall convert video data into actionable events, alarms, and automated workflows within the security management system.

AI detections shall generate alarms, trigger automated actions, and assist operators in real-time incident response.

The proposed solution shall be based on either native AI video analytics embedded within the Video Management System (VMS) or on third-party IVA analytics solutions fully integrated with the VMS via certified SDK/API interfaces.

The proposed solution shall be based on a server–client architecture, with all core system components installed on-premises. Cloud-based or SaaS solutions shall not be accepted. All video processing, analytics, storage, and system management functions shall be performed within the local infrastructure.

The analytics solution shall incorporate AI-based nuisance alarm filtering mechanisms designed for outdoor environments.

The AI analytics engine shall utilize deep-learning and neural-network-based algorithms trained for security and surveillance applications and shall support continuous model optimization and updates.

The system shall support analytics calibration, scene adaptation, and configurable sensitivity settings to optimize performance according to environmental conditions and operational requirements.

Exported evidence shall support standard video formats and include associated metadata, timestamps, and integrity verification.

System architecture

The system architecture shall ensure optimal performance, scalability, and reliability, while maintaining full integration with the Video Management System.

The proposed AI video analytics solution may be based on edge-based analytics (camera-side processing), server-based analytics (central processing), or a hybrid architecture combining both approaches. In hybrid deployments, the system shall support seamless distribution of analytics workloads between edge devices and central servers without degradation of performance or functionality.

The proposed AI video analytics solution shall support high availability (HA) and failover mechanisms to ensure continuous system operation with minimal downtime. Failover processes shall be automatic and shall not require manual intervention by the operator. The failover mechanism shall ensure continuous operation with minimal loss of video streams, analytics metadata, or alarms during any failover event.

The proposed solution shall be fully scalable, allowing for future expansion without requiring any major system redesign. System expansion shall be achieved through the addition of software licenses and, where required, gradual hardware resources only, without impacting existing system functionality or performance.

The system shall support rule-based automation, allowing detected events to trigger actions such as alarms, notifications, or system responses. AI analytics events shall automatically trigger:

a. Alarm notifications.
b. Video pop-ups.
c. Operator alerts.
d. Recording triggers.
e. Automated workflows.

The system shall support the generation of a minimum of 10 types of reports cross multiple categories, including but not limited to:

a. Graphical reports such as pie charts, bar charts, and line graphs.
b. Event and alarm reports.
c. Analytics and metadata reports.
d. Operational and performance reports.

Reports shall be configurable, exportable, and viewable via the client interface, allowing operators and administrators to analyze trends and metrics effectively.

The system shall support alarm and notification generation for analytics failures, camera disconnections, GPU failures, or degraded processing performance.

Server-based analytics components shall support GPU acceleration for AI processing to ensure real-time analytics performance and scalability.

The system shall support integration with ONVIF Profile S,T,M compliant cameras and video devices and shall support open API/SDK interfaces for third-party integrations.

Cyber security

The system shall support the following cyber security features:

a. End-to-end encryption.

b. Secure authentication.

c. Role-based access control.

d. Active Directory integration.
e. Audit logging.

f. TLS 1.2 or higher encrypted communications.

g. Secure password policies and account lockout mechanisms.

h. Syslog and SIEM integration support.

i. Secure boot.

j. Signed firmware/software.

Performance requirements

The system shall support the following performance requirements:

PARAMETER	REQUIREMENT
Processing	Real-time AI analysis
Latency	≤ 2 seconds detection delay

Accuracy	Minimum 90% detection accuracy under manufacturer-recommended installation and environmental conditions
False alarms	Maximum 10% total alarm rate, achieved via advanced
	environmental noise-suppression and filtering mechanisms to minimize nuisance alarms.
Scalability	Minimum 500 cameras per system
Metadata storage	The system shall retain analytics metadata independently of video retention policies for a minimum of 30 days.

Detection and classification

The system shall detect and classify:

a. Humans.
b. Vehicles.
c. Animals.
d. Unattended objects.

Behaviour analytics

The system shall support detection of abnormal behavior including:

a. Intrusion detection. b. Loitering detection. c. Zone/Line crossing.

Image-based search (Forensic Search)

The system shall support forensic search allowing operators to:

a. Search object by type.
b. Retrieve all matching occurrences across recorded video.
c. Filter results by time, location, and confidence level.

Human attribute search

The system shall support searching for people based on attributes such as:

a. Clothing color (upper/lower garments.)
b. Carrying items (bag, backpack, etc.).
c. Motion direction.

The system shall allow combination of multiple attributes to refine search results.

Bookmarking and export

Operators shall be able to:

a. Bookmark AI-detected events.
b. Export video clips with metadata overlay.
c. Maintain evidentiary integrity (watermarking/signatures).

Privacy masking

The system shall support privacy masking and restricted viewing areas in accordance with organizational privacy and data protection policies.

Analytics Management Requirements

The system shall provide centralized management of all analytics rules, cameras, alarms, and detection parameters.

Operators shall be able to configure analytics rules, zones, schedules, sensitivity levels, and alarm actions through a graphical user interface.

The system shall support analytics scheduling profiles based on time, day, or operational scenarios.

The system shall support health monitoring of analytics services, cameras, and processing nodes, including generation of fault alarms upon analytics failure.

ACCESS CONTROL SYSTEM

General

Existing access control systems are deployed across all sites. The systems are based on Mercury EP1501 controllers and Morpho Sigma Lite biometric readers.

C2: CBK - Official

The existing Access Control System shall be replaced with a new system that shall include different types of readers (Face+Finger+RFID, Finger+RFID, RFID) installed in the various sites according to the BOQ and drawings.

Replacement of the existing access control system shall be performed in accordance with the Bill of Quantities (BOQ) for each site.

The proposed ACS solution shall be commercial off-the-shelf (COTS) product that can be supplied and maintained by any qualified Contractor who has received the necessary manufacturer approval and training. Closed or proprietary systems, which operate only with the supplier's or manufacturer's exclusive equipment or can only be maintained by the winning Contractor, will not be accepted. Systems for which the Contractor holds exclusive distribution or installation agreements with the manufacturer will also not be accepted.

System architecture

The proposed Access Control System (ACS) shall be an enterprise-class solution, scalable to support large multi-site deployments, with the capability to expand to additional sites, readers, client workstations, and access control panels without significant system redesign or the need for additional core system servers.

The ACS shall be deployed as an on-premises solution based on a server–client architecture, comprising centralized system servers located at the Main Security Center (MSC) and distributed client workstations at remote sites.

The system shall support a distributed architecture enabling each remote site to maintain local operational autonomy while remaining centrally managed from the MSC. Site-level data, configurations, and permissions shall be logically segregated to ensure that users at one site cannot access or modify another site's data unless explicitly authorized.

The MSC shall provide centralized administration, monitoring, and management capabilities for all connected sites. Authorized MSC users shall be able to enroll users, manage credentials, modify access rights, monitor events, and administer all sites in accordance with assigned access privileges.

Remote site client workstations shall support local operational administration, including at minimum:

a. Enrollment of new users, including badge issuance.
b. Deletion of cardholders.
c. Modification of user access rights and privileges.
d. Local monitoring of access events and alarms.

The system shall support centralized global cardholder management across all locations, including synchronization of cardholder records, credentials, and access rights between the MSC and all remote sites, while maintaining role-based access control and site-level segregation.

The system shall support an open architecture, enabling integration with third-party devices and systems, including but not limited to access controllers, card readers, and electronic locking devices.

System main features

The system shall support multiple-reader technologies, including but not limited to:

a. Integrated readers combining facial recognition, biometric (fingerprint) identification, and RFID card authentication.
b. Integrated readers combining biometric (fingerprint) identification and RFID card authentication.
c. Standalone RFID readers.
d. Mobile identification.

The ACS system shall implement cybersecurity best practices, including secure authentication, role-based access control, encrypted communications, and end-to-end secure data exchange between servers, clients, and controllers. All communications shall be protected using industry-standard encryption protocols such as TLS 1.2 or higher, with data encryption at rest using AES-256 or equivalent.

The ACS solution shall enable generation of reports, alarm management for operator workflow, and a rules-based Automations Engine.

The ACS shall feature an intuitive, user interface that simplifies user management and operations.

The system shall include features such as:

a. Anti pass-back (Soft, hard, scheduled).
b. Double-identification mode.
b. Door interlocks without requiring PLCs (To ensure only one door can be open at any given time in a secure area).
c. Mobile credentials support.
d. Native Access Manager and Directory failover (including for archiving). f. Elevator control (With or without PLCs).
e. Customize reports without requiring any third-party tools (including Activity, audit, and configuration reports).
f. Configurable user-access privileges.
g. Synchronization of databases between remote sites and central servers. j. Export of reports to CSV, EXCEL, and PDF.
h. Cardholder verification (picture and status) and additional info in display.

The ACS controller shall operate independently, allowing full offline functionality in the event of communication loss with the ACS application or a server failure.

The ACS shall support OSDP (Open Supervised Device Protocol) Version 2 or higher with secure channel communication between controllers and readers.

C2: CBK - Official

All ACS servers, controllers, and connected devices shall support synchronization with centralized NTP time servers.

The system shall maintain tamper-resistant audit logs of all operator actions, configuration changes, alarms, and access events.

In the event of communication loss, controllers shall locally buffer transactions, alarms, and events and automatically synchronize the data with the ACS server once communication is restored.

Integration with the PSIM

The integration between the ACS and the PSIM shall be implemented at the server level.

The interface between the PSIM and ACS shall support real-time bidirectional exchange of events, alarms, status updates, and control commands.

The ACS server shall transmit to the PSIM server the following data:

a. Valid transactions data.
b. Non-valid transactions attempts.
c. All system's alerts (such as door forced, door forced open, equipment and communication failures, etc.).

The PSIM shall transmit to the ACS the following commands:

a. Lock gate/door or gates'/doors groups.
b. Unlock gate/door or gates'/doors groups.
c. Unlock all.

The transactions and the alerts data shall be displayed on the PSIM workstations in a similar format and scenarios, to other subsystem's data.

ACS software

Access technologies	The ACS software shall support a variety of access authentication technologies, including but not limited to: Facial recognition authentication. Fingerprint biometric authentication. RFID smart-card technologies operating at 13.56 MHz including ISO 14443, MIFARE, and DESFire. Mobile credentials utilizing NFC, BLE (Bluetooth Low Energy), and virtual credential technologies. Multi-factor authentication combining biometric, card, or mobile credentials.
Database	ACS database shall be based on a commercial off-the- shelf relational SQL database platform.
Client workstation	The system shall support multiple workstations, allowing simultaneous operation by multiple users
Users' levels	Each user shall be assigned a user level. The system shall support a minimum of three operator levels
Users' data	The system shall allow the recording and editing of, at a minimum, the following data: Name (Last, first, middle) Type (employee, subcontractor)
	National ID number Employee number Organizational assignments Permanent address Telephone (office, home, mobile) Vehicle license plate Start of employment date Photo Site code User validity date (start, end) Status (active, deactivated, retired etc.)

Software configuration	The system shall enable configuration of all end devices - including controllers, readers, locks, and related components - via a user-friendly graphical interface. The system shall support configuration of at least 30 access authorization levels, each comprising readers and associated time schedules. The system shall support configuration of the operational mode for each reader, with the ability to change the mode automatically according to pre-scheduled timetables, manually by the operator, or in response to system events.
Flow of data	The system shall record all transactions and events at all readers and controllers in real time, including user identification, authorization, and transmission of access rights to the readers. The system shall support downloading of access tables to readers in offline mode in the event of communication failure or other system malfunctions and automatically update the system server with all reader actions once communication is restored.
	The system shall register all exit entries, capturing user number, username, date, and time.
Data backup	All ACS data - including system parameters, field device configurations, user data, access configurations, and transaction history - shall be stored automatically in the ACS database and backed up by system tasks. The backup process shall not interfere with normal system operation
	Users' definition Users' authorization levels Configuration of anti-pass back for selected doors Configuration of maximum open time for open door (authorized access) Door interlocks
Interface with third-party systems	The system shall support interface with third-party systems such as SAP to enable automated data exchange and system integration.

	The system shall generate alarms and log events for at least the following conditions: Unauthorized access attempt Attempt to open a door without authorization (break-in) Attempt to access with an invalid or unauthorized card Door held open longer than the defined time Tampering with the housing of a reader or controller Communication failure Low battery or power interruption System failure
Reports	The ACS shall include an advanced report generation tool, enabling operators to create statistical and historical reports in alphanumeric or graphical formats. These
	reports shall cover transactions, events, and other system occurrences, based on the data stored in the ACS database. The report generation tool will allow configuring and creating of the following lists and reports: Lists of elements and devices Lists of system configuration parameters Lists of users according to name, last name and user number Lists of users according to time and date (in detail of day, week, month and hour) List of users according to different parameters (including user, card, controlled door) List of lost tags, not returned or not valid Lists of system operator's actions Events and alarm history reports Transactions history reports Events and alarms statistic reports Transaction statistic reports Additional 10 reports (to be determent Clint) The system shall support export of reports to CSV and EXCEL Formats

System operation	Access to the system shall be controlled via username and password. The system's operation mode shall be determined according to user privileges. All operator actions shall be recorded and stored in the system database. Entry of data shall be supported in at least two modes: manually and via Excel import.
	Abnormalities and alarms shall be displayed by default; other system data shall be displayed on demand. Data updates shall be processed without disruption to continuous system operation. The system shall support report generation in parallel with routine operation. Any alarm indication received during data entry or report generation shall automatically trigger a popup of the event screen.
Time zones	The system shall natively support scalable configuration of access authorization levels and time zones, with support for a minimum of 256 active configurations without system degradation. It shall allow each time zone to include a minimum of six (6) intervals. The system shall enable each interval to be assigned to any day of the week and restricted according to at least eight (8) types of holidays. The system shall support downloading of time zones to all relevant controllers for distributed processing and local decision-making.
Lockdown	The software shall include Lockdown functionality
Access groups and levels	Users shall be organized into functional groups, with each group granted access to specific AIUs during designated time zones. The ACS shall allow to define an unlimited number of access groups. The ACS shall allow to assign an Access Level name of up to 64 characters. Each AIU shall grant access only to users assigned to the corresponding access levels.

	The ACS shall support the creation of as many access levels as required during system configuration and setup.
Users' management	The user management function shall allow enrolment of users into the database, including capturing images and signatures, as well as importing and exporting personnel data. All ACS management and administration tasks— including defining access groups, access levels, access rights, and assigning each cardholder to a group—shall be performed at the ACS client stations. Access badges shall be produced in various colors and designs as requested by the Client. The access badges production system shall ensure that each access badge is linked to the corresponding cardholder data in the ACS.
Manual control	Control room operators shall have the ability to manually control all output and input points connected to the ACS. Manual commands shall not interfere with the normal operation of subsystems monitored and controlled by the ACS. All manual and automatic control commands shall be recorded in the system log, along with all other events and messages. Manual control functions shall provide operators with the following capabilities: Lock controlled doors (to not accept any cards, face or fingerprints) Unlock controlled doors (allowing free access) Set controlled doors to facility code mode Reset the access reader to its pre-defined default setting. Readers manual override
	The ACS shall support the creation of as many access levels as required during system configuration and setup.

Users' management	The user management function shall allow enrolment of users into the database, including capturing images and signatures, as well as importing and exporting personnel data. All ACS management and administration tasks— including defining access groups, access levels, access rights, and assigning each cardholder to a group—shall be performed at the ACS client stations. Access badges shall be produced in various colors and designs as requested by the Client. The access badges production system shall ensure that each access badge is linked to the corresponding cardholder data in the ACS.
Manual control	Control room operators shall have the ability to manually control all output and input points connected to the ACS. Manual commands shall not interfere with the normal operation of subsystems monitored and controlled by the ACS. All manual and automatic control commands shall be recorded in the system log, along with all other events and messages. Manual control functions shall provide operators with the following capabilities: Lock controlled doors (to not accept any cards, face or fingerprints) Unlock controlled doors (allowing free access) Set controlled doors to facility code mode Reset the access reader to its pre-defined default setting. Readers manual override

Management of operators	Management of operators and assignment of authorizations shall be an integral part of the ACS management system. Users shall log on and log off workstations using their username and password, and optionally a smart card. Only the System Administrator at the highest authorization level shall be permitted to configure users. User functional privileges shall consist of the full list of system functions. Assigning privileges to a user shall be done by selecting the desired function(s) and specifying the level of access: view only, edit, or execute. The system shall allow configuration of the exact access levels that a specific user is permitted to assign to cardholders. The system shall support creation of user templates, which are pre-defined profiles that can be assigned to users without configuring each individual function manually. Screen menus shall be customizable, so that upon logging in, each user sees only the functions they are authorized to access.
Capacity	The proposed ACS solution shall support a minimum system capacity: • 15,000 cardholders/users with scalability for future expansion. • 2,000 readers. • 500 controllers.
Cyber security	The system shall support secure password policies, configurable password complexity rules, account lockout mechanisms, and role-based authentication policies.
Compliance	UL 294 or IEC 60839 or EN 60839

ACS server

All requirements are minimum requirements. The Contractor shall provide a server that meets the ACS manufacturer's specified hardware and software requirements. The unit hardware and software shall ensure uninterrupted operation under maximum load without any performance degradation.	
Manufacturer	Dell or HP or approved equivalent
Operating system	Enterprise-grade relational SQL database (Microsoft SQL Server, Oracle, PostgreSQL or approved equivalent)
Processor	Intel Xeon Silver processor (or approved newer equivalent), minimum 8 Cores / 16 Threads
Memory	Minimum 64 GB ECC RAM
Storage	Minimum 2 × 1 TB enterprise-grade SSD configured in RAID 1
Network interface	2 × 1GbE (teamed)
Database	Microsoft SQL Server 2022 or newer supported version
NTP	NTP client enabled
Capacity	The system shall support a minimum of 10,000 cardholders and scalable event logging capacity limited only by available storage resources.
Cyber security	The operating system shall support secure boot, TPM 2.0, disk encryption, and regular security patch management.
Electromagnetic emission	FCC Class A, EN 55032 Class A, VCCI Class A or equivalent
Electromagnetic immunity	EN 55035 or equivalent
Operating temperature	10 °C – 40°C

C2: CBK - Official

Power supply	Dual, redundant, hot-swappable power supplies (1+1 configuration)
Humidity	20% to 80% (non-condensing)
Input voltage	90 V AC to 264 V AC
General	The server shall be supplied complete with all required hardware accessories including monitor, keyboard, and mouse.

ACS client workstation

All requirements are minimum requirements. The Contractor shall provide a workstation that meets the ACS manufacturer's specified hardware and software requirements. The workstation hardware and software shall ensure uninterrupted operation under maximum load without any performance degradation.	
Manufacturer	Dell or HP or approved equivalent
Processor	Enterprise-grade multi-core Intel Core i7 Intel Ultra 13th generation or newer, AMD Ryzen 7, or approved equivalent
Memory	32 GByte
Hard Disk	Minimum 1 TB NVMe SSD
Network interface	1 GbE (10/100/1000 Mbps)
Audio	Integrated High-Definition Audio sound card and speakers
Graphics accelerator	Dedicated or integrated graphics adapter supporting minimum 2 GB graphics memory and multi-monitor operation
Electromagnetic emission	EN 55032

C2: CBK - Official

Electromagnetic immunity	EN 55035
Operating temperature	10 °C – 35°C
Humidity	20% to 80% (non-condensing)
Input voltage	90 V AC to 264 V AC
Operating system	Operating system Windows 11 Professional 64-bit or newer supported version
Cyber security	The workstation shall support TPM 2.0, secure boot, endpoint protection, and operating system security updates.
General	The workstation shall be supplied complete with all required hardware accessories including workstation unit, minimum 24-inch monitor, keyboard, and mouse.

C2: CBK - Official

Controller, 2 readers

Compliance standard	UL 294 or equivalent EN or CE
Communication with the server	The controller shall be fully independent in its operation. It shall maintain constant communication with the ACS server and immediately transmit to the central system every transaction and message received. The controller shall transmit to system server – at least - the following information: Authorized access Unauthorized access attempt Door left open above predefined time Attempts to tamper with reader/controller Communication malfunction Power interruption Communication between the controller and the ACS server shall utilize bidirectional full-duplex TCP/IP communication over Ethernet networks. When communication with the server is restored after a communication failure, the controller shall transmit all
	stored transaction messages to the server and download any modified parameters. Each message includes a timestamp, which the server shall use for proper storage and processing. If communication is not restored before the controller's memory becomes full, newly generated messages will overwrite the oldest ones using a FIFO (First-In, First- Out) method.
Off-line operation	Required, On-board non-volatile memory

C2: CBK - Official

Self-diagnostic checks	The controller shall regularly perform self-diagnostic checks on all its components, including software integrity, data corruption, internal memory, power supply, and the backup battery. In the event of a malfunction, the controller will generate an alarm. The alarm shall be both local and remote, providing audible and visual indications, and will be transmitted simultaneously to the central computer.
Time zones	128 time zones 64 holidays 32 Smart Links (If/then) on panel Minimum 10,000 access groups
Additional features	Interlock Auto re-lock Extended unlocked time activation/deactivation Anti pass-back (hard/soft/timed)
Memory capacity	30,000 credentials
Event Log size	20,000 events
Cyber security	Cyber security Server communications shall support TLS 1.2/1.3 encryption and AES-128/AES-256 encryption where applicable. The controller shall support IEEE 802.1X port-based network authentication.
Firmware security	The controller shall support secure firmware updates and digitally signed firmware validation.
Interface to readers	OSDP Version 2 Secure Channel communication

C2: CBK - Official

Interfaces	RS-485 RS-232 10/100 Ethernet
Inputs / Outputs	Minimum 4 supervised inputs and 4 programmable relay outputs
LED indicators	TCP/IP, RS-485, outputs, power
Tamper switch	Required, opening and ripping tamper
Power backup	The controller shall support minimum 2-hour backup operation using dedicated rechargeable batteries supplied as part of the system.
Operating voltage	12vdc / 24vdc
Operating temperature	-5° to 50°
Relative humidity	85%, non – condensing

Controller, 4 readers

Same requirements as for a 2-reader controller.

Face recognition / Finger / RFID reader

Reader type	Mult technology
Compliance standard	CE, FCC, KC, UL, or equivalent international compliance certifications
Interface to controller	OSDP Version 2 Secure Channel or higher
Authentication technologies	a. Facial recognition authentication b. Fingerprint biometric authentication c. RFID smart-card authentication d. Mobile credentials (NFC/BLE) e. multi-factor authentication combinations

C2: CBK - Official

Face recognition performance	Capacity: 10,000 Recognition distance: 0.5 m to 1.3 m Recognition height: 130cm - 200 cm Matching speed: Less than 0.5 sec
Figer print performance	Capacity: 20,000 Resolution: 500 DPI Live fingerprint detection: supported
RF	RFID technologies 13.56 MHz smart-card technologies including MIFARE, MIFARE Plus, DESFire EV2/EV3, or equivalent Reading range: Minimum 5 cm
Mobile	NFC, BLE
Security	a. Secure boot support b. AES-128 / AES-256 encrypted communications and biometric credential storage c. Secure firmware validation and signed firmware updates
Protection	Immunity to RFI, EMI interference Protection against lightning strikes and power surges.
LCD type	7" IPS color LCD
LCD resolution	800 x 1280 pixels
Audio indication	Required
Interface	RS-485 Ethernet E10/100 Mbps
Relay	At least 1
Memory	16 GB Flash + 2 GB RAM

C2: CBK - Official

Tamper	Required
Life cycle	At least 30,000 hours
IP rating	IP 65
Voltage	DC 12V ~ DC 24V
Operating temperature	-10° to 50°
Relative humidity	0% to 80% noncondensing

Finger / RFID reader

Reader type	Mult technology
Compliance standard	CE, FCC, KC, UL, or equivalent international compliance certifications
Interface to controller	OSDP Version 2 Secure Channel or higher
Authentication technologies	Fingerprint RFID card Mobile
Figer print performance	Capacity: 20,000
	Resolution: 500 DPI
RF	RFID technologies 13.56 MHz smart-card technologies including MIFARE, MIFARE Plus, DESFire EV2/EV3, or equivalent Reading range: Minimum 5 cm
Mobile	NFC, BLE

C2: CBK - Official

Security	a. Secure boot support b. AES-128 / AES-256 encrypted communications and biometric credential storage c. Secure firmware validation and signed firmware updates d. Protection against unauthorized configuration changes
Anti-spoofing	The reader shall support liveness detection and anti- spoofing protection for fingerprint authentication.
Protection	Immunity to EMI/RFI interference
Audio indication	Required
Interface	RS-485 10/100 Mbps Ethernet
Relay	At least 1
Memory	16 GB Flash + 2 GB RAM
Tamper	Required
Life cycle	At least 50,000 hours
IP rating	IP 65
Voltage	DC 12V ~ DC 24V
Operating temperature	-10° to 50°
Relative humidity	0% to 80% non-condensing

RFID reader

Reader type	Mult technology
Compliance standard	CE, FCC, KC, UL, or equivalent international compliance certifications

C2: CBK - Official

Interface to controller	OSDP Version 2 Secure Channel or higher
Authentication technologies	a. RFID smart-card authentication b. Mobile credentials (NFC/BLE)
RFID technologies	13.56 MHz smart-card technologies including MIFARE, MIFARE Plus, DESFire EV2/EV3, or equivalent Reading range: Minimum 5 cm
Mobile	NFC, BLE
Security	Secure boot support AES-128 / AES-256 encrypted credential communications Secure firmware validation and signed firmware updates Protection against unauthorized configuration changes
Credential security	The reader shall support secure encrypted credential technologies and mutual authentication mechanisms.
Protection	Immunity to EMI/RFI interference Protection against lightning surges and power fluctuations
Audio indication	Required
Interface	RS-485 with OSDP Version 2 Secure Channel support
Relay	At least 1
Tamper	Required
Life cycle	At least 40,000 operational hours
IP rating	IP 65
Voltage	DC 12V ~ DC 24V
Operating temperature	-10° to 50°
Relative humidity	0% to 80% non-condensing

C2: CBK - Official

Electromagnetic lock, single leaf door, 600 Lbs

Holding force	600 lbs. (270 Kg)
Compliance standard	UL 294, CE or equivalent
Housing material	All stainless-steel corrosion resistant or Anodized aluminum, tamper resistant, heavy-duty construction
Installation	Indoor or Outdoor, “L” Bracket or “Z” Brackets included
Security	Fail safe
Life cycle	At least 100,000 actions
Mounting	Mounting plates for use on in and out-swing doors, conduit fitting for exterior gates installations
Indication	Local buzzer for remote opening
Door status indication	Integrated in lock
LED indicator	Included
Voltage	12 VDC / 24 VDC
Operating temperature	-10° to 50° C
Relative humidity	0% to 85% non – condensing

Electromagnetic lock, double leaf door, 600 Lbs

Same requirements as for a single leaf 600 Lbs Electromagnet lock.

Electromagnetic lock, single leaf door, 300 Lbs

Same requirements as for a single leaf 600 Lbs. electromagnet lock but for 300 Lbs.

Electric strike lock

C2: CBK - Official

Mode	Fail safe
Break-in resistance	3000 N
Load-cycle durability	50,000
Adjustable latch radius	3 mm
Latch bolt engaging depth	5 mm
Reversible DIN orientation	Required, swap left/right
Operating voltage	10–24 V AC/DC
Operating temperature	-10° to 50° C
Relative humidity	0% to 85% non – condensing

Request To Exit (REX) - Contactless

Compliance standard	CE or equivalent
Detection range	Minimum 50 mm
Detection technology	IR
Shell material	Stainless steel or aluminium alloy
Installation method	Flush mounted / surface mounted
LED indication	Green / Blue
Output contact	NO/NC/COM
Labelling	WAVE TO OPEN / PRESS TO EXIT
Power supply	12 to 24 VDC
Operating temperature	-20° to 55° C

C2: CBK - Official

Operating humidity	0-95% (relative humidity)

Emergency door release

Chassis material	ABS
Installation	Surface mount
Output contact	NO/NC/COM
Labelling	EMERGENCY DOOR RELEASE
Power supply	DC12-24V
Operating temperature	-20° to 55° C
Operating humidity	0-95% RH, non-condensing

High security magnetic door position switch

Compliance standard	UL 634 Level 2 or equivalent
Type	Balanced magnetic contacts
Installation method	Surface mount, concealed
Anti-tamper	Anti-tamper output, Hidden
Gap distance	Up to 3/8 in
Tamper output	Closed when secure
Operating temperature	-10° to 60° C
Relative humidity	0% to 95%

Hydraulic door closer

C2: CBK - Official

Compliance standard	EN1154, CE Marked or equivalent
Material	Zinc-alloy
Speed adjustment	2 speeds
Closing power	Adjustable
Maintenance	Maintenance free
Mounting	Push or Pull side
Maximum door opening	120°

Enrolment workstation

General

The enrolment workstation shall support face image capture, fingerprint biometric enrolment, badge printing, and cardholder management operations.

The enrolment workstation shall include:

- ACS workstation with all required licenses for image capture and biometric enrolment operations
- badge printer
- camera
- fingerprint biometric acquisition unit
- and all required accessories and software.

Computer functionalities	The workstation shall interface directly with the ACS server database to store and retrieve cardholder information, biometric templates, images, credentials, and enrolment records

C2: CBK - Official

	All data shall be stored in the database. The data will contain at least the following information: serial number, issuing code, date of issue, cancellation dates, and personal codes. The data of the badge holders shall also be stored in the database and will contain at least the following information: name, surname, picture, biometric characteristics of the owner of the badge, ID number, employee number, vehicle number, parking location, organizational affiliation, Mobile phone, security officer's note, general comment.
Computer minimum requirements	The Contractor shall supply a workstation fully compliant with the ACS manufacturer's hardware and software requirements. Minimum requirements: • Intel Core i7 or approved equivalent • 128 GB RAM minimum • 1 TB SSD • Windows 11 Professional or latest LTS Linux version supported by the ACS manufacturer
Cyber security	The workstation operating system shall support secure boot, TPM 2.0, disk encryption, anti-malware protection, and regular security patch management.
Badge printer	
Printing method	Dye sublimation / retransfer printing technology
Resolution	300 dpi (11.8 dots/min)
Color capability	Up to 16.7 million colors (256 shades per pixel)
Full-color printing speed	Up to 20 seconds per card maximum
Print speed – Monochrome	Maximum 6 seconds per card
Print area	Edge to edge
Input hopper capacity	Minimum 100-card capacity

C2: CBK - Official

Duplex printing	Required
On-the-fly encoding	Supported (encoding during print process), support DESFire EV2/EV3
Memory	64 MB RAM
Software compatibility	Full compatibility with Windows 11
Interfaces	USB 2.0/3.0 and Ethernet
Security features	Password-protected access; AES-256 encrypted network communication (configuration dependent)
Operating temperature	18°C – 27°C
Operating humidity	20% – 80% non-condensing
Camera	
	The camera shall contain a driver that is suitable for connecting to the enrollment computer for capturing image of person directly from the ACS software.
	The camera shall contain all the accessories necessary for connecting it to a fixed tripod.
	Minimum Full HD 1080p (2.0 Megapixels or higher) with auto-focus and built-in LED lighting optimization
Fingerprint biometric acquisition unit	
	Sensor Type: Optical Resolution: 500 dpi
Matching Speed:	2,000 matches per second
Interface:	USB 2.0
Operating Temperature:	-10°C to +50°C

The enrolment workstation shall support simultaneous enrollment of credentials, face image, and fingerprint biometric templates within a single operator workflow.

C2: CBK - Official

Enrolment RFID reader

Card/tag types	The reader shall support enrolment, reading, and encoding of contactless smart cards, RFID proximity cards, key fobs, and RFID tags
Supported technologies	13.56 MHz ISO 14443 Type A/B, MIFARE Classic, MIFARE Plus, MIFARE DESFire EV1/EV2/EV3, NFC- compatible credentials
Read/write capability	Full read/write support for all supported card/tag types
Interfaces	USB 2.0 / 3.0 or Ethernet (TCP/IP), with driver support for Windows 11
Software compatibility	Integration with ACS software and cardholder management applications via native drivers, SDK, or API
Indicators	LED status indicators, audible buzzer for feedback
Security features	Secure communication with host system, AES encrypted credential handling where supported, secure key management support, firmware integrity protection / secure boot
Compliance	CE, FCC, RoHS, ISO standards for RFID devices

Contactless smart card

Format	Comply with ISO/IEC 7810, format ID-1
Dimensions	85.60 mm x 53.98 mm, Thickness: 0.76 mm
Material	PVC or polycarbonate
Communication protocol	13.56 MHz

C2: CBK - Official

Reading range	5 - 10 cm
Processor	16-bit to 32-bit RISC microcontroller
Encryption	Minimum 128 bit or 3DES
Life cycle	At least 5 years
Operating temperature	-10 to 50˚C
Relative humidity	0% to 95%

Door alarm

Detection method	Magnetic reed switches, contact sensor, or electronic trigger integrated with door frame and door leaf
Alarm output	Built-in siren, minimum 85–100 dB at 1 meter
Dealy time	Programmable, at least 4 modes
Audible alarm duration	Programmable, 30 seconds to continuous until reset
Tamper protection	Anti-tamper switch or circuit to detect device removal or wiring cut
Visual indicator	Required, Red light
Relay	C/NO/NC 30V
Mounting type	Surface-mounted on door or frame
Material & finish	High-strength ABS or polycarbonate housing; color options: white or red
Reset	Mechanical key
Operating voltage	12–24 VDC
Operating temperature	-10 to 50˚C

C2: CBK - Official

Relative humidity	0% to 95%
Compliance	CE, RoHS, EN 50131 or equivalent security standard

INTRUSION DETECTION SYSTEM

General

At each site, the Intrusion Detection System (IDS) shall consist of two separate subsystems:

a. An IDS based on volumetric intrusion detection sensors installed in various rooms and protected areas throughout the site.

b. An IDS based on seismic and vibration detection sensors installed in secure rooms, vaults, safes, or strong rooms.

All IDS field devices, controllers, communication modules, and associated equipment installed in indoor environments shall comply with EN 50131 Grade 3 certification requirements or equivalent international standard.

The IDS shall support centralized integration with the PSIM platform. The system shall support both local site management and centralized monitoring and management from the MSC and SMSC according to user authorization levels.

The IDS architecture shall support distributed operation, allowing each site to continue autonomous operation in the event of communication loss with the MSC, SMSC, or PSIM platform.

The IDS shall support partitioning of protected areas into independent zones, groups, and arming areas.

The IDS shall support event logging, alarm history, audit trail functionality, and time synchronization using the site NTP infrastructure.

Communication between IDS controllers, workstations, servers, and integrated systems shall support encrypted communication channels.

Communication between control panels, keypads, expansion modules, and intelligent field devices shall be encrypted and continuously supervised against substitution and spoofing attempts.

C2: CBK - Official

Integration with the PSIM

The integration with the PSIM software shall support the following:

a. Real-time transmission of events, alarms, and system status information to the PSIM software.

b. Integration with video management systems (VMS) for automatic video display, recording, and playback associated with alarms and events.

c. Bi-directional communication, allowing commands and control actions to be initiated from the PSIM platform including:

d. Alarm acknowledgment.

e. Arming and disarming of sensors and zones.

f. Neutralizing/bypass of sensors and zones.

g. Setting time windows

h. Generation of reports

The PSIM platform shall support execution of the following IDS control commands according to operator authorization:

a. Alarm acknowledgment.

b. Arming and disarming of areas, partitions, sensors, and zones.

c. Bypass/neutralization of sensors and zones.

d. Scheduling and configuration of time windows and arming schedules.

e. Report generation and event history retrieval.

From the PSIM platform it will be possible to display the following indications received from the IDS:

a. Alarm condition.

b. Normal/reset condition.

c. Bypass/neutralized condition.

C2: CBK - Official

d. Tamper alarm.

e. Sensor fault.

f. Low battery indication.

g. Communication failure between sensors and controllers.

h. Controller communication loss.

i. Controller cabinet tamper.

j. Power supply fault.

k. Controller fault or hardware failure.

l. AC power loss and restoration.

m. Arming/disarming status.

C2: CBK - Official

Control panel

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Onboard zones	8 (minimum)
Max number of zones	Up to 520 zones Without any changes to existing hardware or software, except for the addition of expansion modules
Partitions / zones	At least 32 The system shall allow setting sensitivity for each zone (minimum zone open time required to trigger an alarm) The system shall allow automatic zones reset after several alarm cycles; the setting shall be programmable individually for each zone
Number of keypads	At least 16
Number of keyfobes	At least 8
Wired sirens	The control panel shall include 2 dedicated siren outputs on the main board and shall support up to 20 outputs via zone/output expansion modules The two siren outputs shall be isolated so that a fault (e.g., short circuit) on one output does not affect the other
User codes	500 Minimum

	The system memory shall store at least 2,000 recent events, in Non-volatile memory including at a minimum the following events: System arming and disarming Zone alarms Tamper events System faults
	Entry into technician/service menu Incorrect code entry Remote access via control software Setting of system clock and date Performing detector walk tests The system memory shall store the events in non-volatile memory that is independent of power supply and cannot be erased Every system arming and disarming shall be recorded with the username as defined in the system All alarm events shall be recorded with the name of the zone as defined in the system The memory shall display events in chronological order and by event type
	The system shall support KNOCKING ZONE functionality (a zone can be programmed so that an alarm is triggered only if the zone is activated more than once within a defined time period) The system shall support CROSSING ZONE functionality (a condition can be programmed between zones so that an alarm is triggered only if a pair of zones is activated within a defined time period; the alarm is triggered from both zones simultaneously)

	The system shall not trigger an alarm for at least 60 seconds and up to a maximum of 120 seconds after full power restoration (detector warm-up period) The system shall allow a zone to be defined as a "test zone" – when the zone is activated, there shall be indication on the keypad and in the memory, but no reports or sirens shall be triggered
Remote monitoring communication	The system shall provide reporting to a central monitoring station via multiple communication channels: Telephone lines (PSTN/RTB). Radio communication. Cellular network (supporting two SIM cards with automatic switching in case of cellular network failure). Ethernet network using TCP/IP protocol. Cellular channel usage shall be configurable as one of the following: Backup for the telephone line. Primary channel.

	For TCP/IP reporting using SIA protocol, the system shall provide encryption according to protocol requirements. The system shall allow reporting to six private phone numbers. The system shall be capable of reporting to two different monitoring stations, each with a different account number and communication protocol. Reporting shall be configurable at the zone level for both stations. The system shall detect a telephone line fault/disconnection immediately (according to programmable timing) and report it to the monitoring station as well as provide visual and audible indicators on the keypad. Detection and reporting of the fault shall occur continuously, regardless of system state (armed or disarmed).
	The system shall detect communication failures to the monitoring station and report via the available communication channels, while also providing visual and audible indication on the keypad.
Diagnostic	The system shall allow zone testing – "walk test" – to verify the proper operation of all zones. The system shall allow activation of a buzzer on any device connected to the BUS to facilitate rapid identification of its physical location on site.

Protection	The system shall include multiple thermal fuses to protect peripheral devices (detectors, sirens, keypads). The control panel shall include a fuse to prevent uncontrolled current supply from the battery to the board. The system shall provide short/open-circuit detection for all zones, enabling visual and audible indication on the keypad and reporting to the monitoring station, regardless of system state (armed or disarmed). The system shall include an option to inhibit system activation in the event of a fault. The detectors power outputs shall be protected against short-circuits and the control panel shall report any short- circuit on the detector supply voltage, regardless of system state (armed or disarmed).
Programming	There shall be a separation between user codes and the alarm system installer/technician codes.
Zone programming	The system shall include the following options for configuring each zone: Entry delay Exit delay Conditional entry-following zone Instant zone

	Siren-activating zone 24-hour zone Night mode active zone Bell zone (keypad buzzer activation upon any zone opening while the system is disarmed) Automatically reset zone (after 3 alarms on the same arming) End-of-line resistor (EOL) configuration, including adjustable resistor values Selectable zone input type: Normally Closed (N.C.) or Normally Open (N.O.) Assigning zones to specific partitions/areas. Setting zone type (e.g., intrusion, tamper, fire, auxiliary). Configuring zone sensitivity (minimum open time to trigger an alarm). Programming special zone functions such as KNOCKING ZONE and CROSSING ZONE. Enabling or disabling automatic zone reset after a number of alarm cycles. Configuring “Test Zone” mode for walk testing and functional verification. Assigning zones to specific sirens, outputs, and reporting channels. Setting zone-specific reporting parameters to monitoring stations. The system shall allow copying the configuration of one zone to another zone or to a group of zones, and from one group of zones to another group, using the keypad.
Arming / disarming	The system shall allow automatic arming at a pre-defined time.

	The system shall provide visual and audible warning of an upcoming automatic arming. The system shall support active automatic arming, whereby any partition in which zones have not been activated within a pre-defined period will be automatically armed. The system shall allow specifying zones that cannot be disarmed by users. Temporary zone disarming shall be canceled if the system is not armed within a pre-defined time period. The system shall allow restricting user disarming rights according to pre-defined schedules, with each user receiving an individual configuration. The system shall provide visual and audible indication of system arming and disarming via the keypad, sirens, and mobile application. Operation of the system shall not be possible without changing the default codes to new codes. Entering an incorrect code multiple times on the keypad or via the application shall trigger keypad lockout for a programmable duration, local alert via sirens and keypad, and reporting to the monitoring station and application. The number of attempts, lockout duration, and responses shall be configurable.
	The system shall support multiple arming modes, including: Full/Stay Arming Night/Partial Arming Instant Arming Automatic Arming (pre-scheduled or active mode).
Cyber security	TLS 1.2 or higher encrypted communications. Role-based user authentication and authorization.

	Secure firmware update mechanism with digital signature validation. Protection against unauthorized configuration changes. Audit logging of configuration modifications and operator actions. Support for strong password policies and account lockout mechanisms. Secure remote access via VPN or encrypted tunnels only.
Communication redundancy	The system shall support automatic communication failover between available communication channels (Ethernet, Cellular, PSTN, Radio) without operator intervention. The control panel shall continuously supervise all communication paths and generate alarms upon communication degradation or failure.
Time synchronization	The system shall support synchronization with enterprise NTP servers to ensure accurate timestamping of all alarms, events, and audit logs.
Health monitoring	The system shall continuously monitor: • Battery health. • AC power status. • Communication module status. • Peripheral device connectivity. • Detector power consumption abnormalities.
Backup power supply	Required. Battery for 36 hours
GSM/GPRS module	Required option
ISDN	Required option
Operating temperature	-10°C to 55°C
Relative humidity	75% non-condensing
Enclosure	From metal

Internal 8 zones expansion module

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Number of zones	At least 8
Type	Wired
Card status LED	Two LEDs to indicate the card status and communication with the control panel
End-of-line (EOL) tamper	Required
Power supply	Required as part of the unit (built-in or attached)
Tamper switch	On-board tamper switch reported to panel
Outputs	At least 4, programmable
Operating temperature	-10°C to 55°C

External 32 zones expansion module

Shall meet the same technical and functional requirements as the 8-zone expander but provide 16 fully supervised wired zones.

Keypad

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Type	Wired
Display	LCD/ OLED, 32 alphanumeric backlit display

C2: CBK - Official

Tamper protection	Required, front and rear
Functional features	Using the keypad the following operations can be performed: System arming using a code consisting of a 6- 8-digit combination, with no limitation on the number of combinations. General disarming or disarming of a specific zone or multiple zones. Reset. Parameter configuration/modification. Browsing the system memory. Technician code modification. Quick arming option by pressing a single key. Activation of a duress (panic) code simultaneously with system operation. Viewing all zones simultaneously.
Communication	The keypad communication with the control panel shall be encrypted and continuously supervised against communication loss, tampering, substitution, or bus manipulation attempts
Diagnostics	The keypad shall support local diagnostic indications for communication status, power status, bus faults, and tamper conditions.
Keypad lockout	The keypad shall support configurable lockout after multiple invalid code attempts, including local audible indication and reporting to the monitoring station
Display options	The keypad unit shall provide visual indication of the following system states: System disarmed. System armed.
	System in alarm. System in fault condition, including detection of open or short circuits on zone lines and power supplies. Event history display.

Indicators	System Armed System Disarmed Alarm Fault / Trouble
	LED indicators brightness shall be configurable for day/night operation
Housing material	ABS plastic
Operating temperature	-10°C to 50°C
Relative humidity	Up to 90% non-condensing

External alarm strobe & siren

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Type	Integrated audible siren and visual strobe
Sound output	Minimum sound pressure level: ≥110 dB @ 1 meter Multiple selectable alarm tones (continuous / pulsed) Frequency range: 300 Hz – 3 kHz
Visual indicator	High-intensity LED strobe Light output: ≥15–30 cd (or equivalent lumen rating) Flash rate: 60–90 flashes per minute Color - Red
	Flash rate – 60 - 90 flashes per minute
Tamper protection	Required, front and rear
Operating voltage	12 VDC / 24 VDC
Mounting	Wall-mounted

Enclosure material	ABS / Polycarbonate
IP rating	IP65
Operating temperature	-10°C to 50°C
Relative humidity	Up to 90% non-condensing

DT Wall mounted detector

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Type	Wall mounted
Sensors	K-Band Microwave + Dual Element PIR
Coverage	15 meters with a horizontal field of view of 90 degrees
White light immunity	Required
Sensitivity	Adjustable
Radio Frequency (RF) Immunity	Compliance with EN 50130-4 standard
Built-in End-of-Line (EOL) Resistors	Required
Tamper	Rear and cover
Anti mask	Required
Test mode	Walk Test mode with LED indication of test results. Option to disable the LED after the test
Operating voltage	9 - 16 VDC
Mounting	Wall-mounted
Enclosure material	ABS / Polycarbonate

C2: CBK - Official

Operating temperature	-10°C to 55°C
Relative humidity	Up to 90% non-condensing

Ceiling detector, up to 4 meters

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Type	Ceiling mounted
Max installation height	4 meters
Sensors	Microwave + passive PIR
Coverage	18 meters, 360 degrees
Pulse count	Selectable (1, 2, or 3 pulses)
White light immunity	Required
Sensitivity	Adjustable
Radio Frequency (RF) Immunity	Compliance with EN 50130-4 standard
Built-in End-of-Line (EOL) Resistors	Required
Tamper	Rear and cover
Anti mask	Required
Test mode	Walk Test mode with LED indication of test results. Option to disable the LED after the test
Operating voltage	9 - 24 VDC
Enclosure material	ABS / Polycarbonate
Operating temperature	-10°C to 55°C

C2: CBK - Official

Relative humidity	Up to 90% non-condensing

Ceiling detector, up to 8 meters

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Type	Ceiling mounted
Max installation height	8 meters
Sensors	K-Band Microwave + passive PIR
Coverage	12 meters, 360 degrees
Pulse count	Selectable (1, 2, or 3 pulses)
White light immunity	Required
Sensitivity	Adjustable
Radio Frequency (RF) Immunity	Compliance with EN 50130-4 standard
Built-in End-of-Line (EOL) Resistors	Required
Tamper	Rear and cover
Anti mask	Required
Test mode	Walk Test mode with LED indication of test results. Option to disable the LED after the test
Operating voltage	9 - 24 VDC
Enclosure material	ABS / Polycarbonate
Operating temperature	-10°C to 55°C
Relative humidity	Up to 90% non-condensing

Seismic detector

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Installation	Ceiling or wall mounted
Detection range	Minimum 5 meters radius on reinforced concrete surfaces
Sabotage protection	Pry-off and cover Switch Low voltage alarm Temperature alarm Internal functional alarm
Attack types	- Hammering - Chiseling - Drilling - Diamond drilling
	- Hydraulic attacks - Oxy-acetylene torches
Drilling shield	Required
Integrated temperature alarm	Required (85 C threshold)
Remote test	Required
Sensitivity	Adjustable, at least 4 levels by DIP Switches, optional for remote adjustment

C2: CBK - Official

Radio Frequency (RF) Immunity	Compliance with EN 50130-4 standard
Diagnostic LED	Required
Built-in End-of-Line (EOL) Resistors	Required
Tamper	Rear and cover
Protection	The detector shall include protection against substitution, bypass, short-circuit, open-circuit, and tamper attempts.
Installation tool	Required, Noise and alarm indicator
Alarm algorithm	Required
Operating voltage	9 - 24 VDC
IP rating	IP40
Operating temperature	-10°C to 70°C
Relative humidity	Up to 90%, non-condensing

C2: CBK - Official

Panic alarm switch, wired

Compliance standard	EN 50131 or equivalent
Security grade	Grade 3
Environmental class	Class II (Indoor)
Operating principle	Manual activation, push button
Reset method	Key reset or tool reset
Built-in End-of-Line (EOL)	Required
Tamper	Required
IP rating	IP 40
Operating voltage	12V to 30V DC
Housing material	Flame-retardant ABS/PC
Operating temperature	-10°C to 55°C
Relative humidity	Up to 90% non-condensing

Magnetic door position switch

Compliance standard	EN 50131-2-6 Grade 3 or equivalent
Installation method	Surface mount
Chassis material	ABS
End-of-line resistors	Required
Gap distance	Up to 3/8 in
Circuit type	N/O and N/C
IP rating	IP 65

C2: CBK - Official

Operating temperature	-10° to 50° C
Relative humidity	0% to 95%

Heavy duty magnet

Compliance standard	EN50131-2-6 Grade 3
Installation method	Surface mount
Material	Aluminum / ABS
Armored cable	Required
Gap distance	10 mm
Tamper	Required
Voltage range	12Vdc
Operating temperature	-10° to 60° C
Relative humidity	0% to 95%

Active IR beam, 15 / 50 / 100 meter, Outdoor

Compliance standard	EN 50131 or equivalent
Detection range	30 / 50 / 100 meter
Number of beams	4 x Synchronized beams
Number of channels	4 x Selectable beam channels to prevent crosstalk
Response time	50msec. to 700msec. variable
Sensitivity adjacent	Automatically increased in bad weather to contend with fog, heavy rain, frost or snow

C2: CBK - Official

External light compensation	Required, against sunlight, automobile headlights, fluorescent light or mercury light
beam transmission strength	2 levels
Beam alignment	Audible signal
Tamper	Required, including top cover
IP rating	IP65
Operating voltage	12V to 30V DC
Enclosure material	Polycarbonate
Operating temperature	-10°C to 55°C
Relative humidity	Up to 90% non-condensing
Price of the unit is for a transceiver and a receiver	

C2: CBK - Official

Dual technologies detector, Outdoor

Compliance standard	EN 50131 or equivalent
Detection channels	2 Microwave and 2 PIR
Coverage range	Adjustable, up to 15 m
Microwave anti-collision	Required
Pet immunity	Selectable / up to 20 kg
Environmental immunity	High immunity to sunlight, rain, wind, vegetation movement, and temperature changes
Tamper protection	Front and rear tamper switch
Anti mask	Required
IP rating	IP 65
Operating voltage	12V to 30V DC
Enclosure material	Polycarbonate
Operating temperature	-10°C to 55°C
Relative humidity	Up to 90% non-condensing

C2: CBK - Official

Curtain detector

Compliance standards	EN 50131-2-2 or equivalent
Security grade	Grade 3
Detection technology	Dual element PIR, K-band microwave
Coverage range	Adjustable, up to 12 m
Anti mask	Required
Tamper protection	Wall tamper switch
Sunlight immunity	Required
Sensitivity adjustment	Required, Adjustable
End-of-Line	Required, supervised
LED indication	Multi-color LED for alarm, masking, fault, and walk test
IP rating	IP 65
Operating voltage	12V to 16 VDC
Enclosure material	Polycarbonate
Operating temperature	-10°C to 55°C
Relative humidity	Up to 90% non-condensing

C2: CBK - Official

Laser detector, Grade 3

Compliance standards	EN 50131-2-2 or equivalent
Security grade	Grade 3
Detection technology	Infrared laser scanning (LiDAR)
Laser protection class	Class 1 (eye-safe)
Coverage range	Adjustable, up to 20 m × 20 m, 95° field of view
Multiple detection areas	Required, adjustable
Sensitivity adjustment	Required, Adjustable
Anti mask	Required
Tamper protection	Wall tamper switch
IP rating	IP 65
Operating voltage	12V to 30 VDC
Operating temperature	-10°C to 55°C
Relative humidity	Up to 90% non-condensing

PUBLIC ADDRESS SYSTEM

General

The Public Address (PA) system shall provide live paging, prerecorded announcements, emergency notifications, and routine information broadcasting throughout all designated areas.

The system architecture shall be IP-based and scalable, allowing future expansion without replacement of existing infrastructure.

C2: CBK - Official

The Public Address (PA) system shall be fully IP-based, with all audio distribution, control, monitoring, and management functions operating over the IP network.

The system shall be based on network-enabled horn speakers and ceiling/internal speakers with built-in Class D amplifiers and DSP functionality. Centralized amplifiers shall not be required.

The system shall be scalable and support the addition of at least 200 network speakers and multiple master stations without degradation in performance.

System configuration, monitoring, and management shall be performed via the PSIM platform and/or VMS system where applicable.

The system shall be fully integrated into the PSIM platform for centralized monitoring, control, and event-driven announcements.

All communications between system components shall support TLS 1.2 or higher encryption and authenticated device communications.

The system shall include a physical desk-mounted master control console for local operation.

Integration with the PSIM

The system integration with PSIM shall support at minimum:

a. Real-time visualization of PA devices on MAP/GIS interface.

b. Monitoring of device status, including fault, offline, and communication loss conditions.

c. Control of announcement zones and volume levels.

d. Initiation of live and pre-recorded announcements from PSIM.

e. Event-triggered audio broadcasting based on security events.

C2: CBK - Official

PA master station console

Functional requirements	• The master station shall support: • Live voice announcements • Pre-recorded message broadcasting • Zone/group selection and control • Volume control per zone • Speaker status monitoring and fault indication • Event-triggered announcements
Management parameters	Zone definition and grouping Message library management Button configuration and assignment Priority levels for announcements Pre-announcement chime settings
Screen	5” full colour touchscreen, 800 x 480 pixels
Zones	At least 8 configurable zones
Material	Brushed aluminium or PVC
Gooseneck microphone	Included
Operating temperature	-5°C to +55°C
Relative humidity	15% to 90% non-condensing
Certification	CE marking or equivalent internationally recognized standards (EN, IEC)

C2: CBK - Official

Network horn speaker

Amplifier	Built-in 7W Class D amplifier
Max sound pressure level	>121 dB
Frequency response	280 Hz - 12.5kHz
Test tone	Required, built-in
Supported protocols	IPv4/IPv6 support, SIP, RTP, RTCP, HTTP/HTTPS, TLS encryption, SNMP v1/v2c/v3, NTP, DHCP, DNS, IGMP (multicast support), SSH for secure management
Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log
VoIP	Support for SIP for integration with VoIP systems, peer to peer or integrated with SIP/PBX.
Casing	Impact-resistant aluminium
Power	PoE IEEE 802.3af/802.3at Type1 Class 3
Connectors	RJ 45 10 BASE-T/100 BASE – TX PoE
IP rating	IP 66
Operating temperature	-5°C to 50°C
Relative humidity	10% to 85%
Certification	EN 55032, EN 55024, EN 50121-4 or equivalent international standards (UL/IEC acceptable)

C2: CBK - Official

Network ceiling speaker

Amplifier	Built-in 6W Class D amplifier
Max sound pressure level	95 dB
Frequency response	45 Hz – 20 kHz
Test tone	Required, built-in
Supported protocols	IPv4/IPv6, SIP, RTP/RTCP, HTTP/HTTPS, TLS encryption, SNMP v1/v2c/v3, NTP, DHCP, DNS,IGMP multicast support
Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log
VoIP	Support for SIP for integration with VoIP systems, peer to peer or integrated with SIP/PBX.
Casing	Steel
Power	PoE IEEE 802.3af/at (Class 3 or higher)
Connectors	RJ 45 10BASE-T/100 BASE-TX PoE
I/O	One input and one output
IP rating	IP 54
Operating temperature	-5°C to 55°C
Relative humidity	10% to 90% non-condensing
Certification	EN 55032, EN 55024, EN 50121-4 or equivalent international standards

C2: CBK - Official

INTERCOM SYSTEM

General

The intercom system shall be fully IP-based, with all audio, video, control, and management functions operating over the IP network.

The system shall be scalable and support simultaneous operation of at least 20 concurrent SIP sessions without degradation.

System configuration, monitoring, and management shall be performed via the PSIM platform and/or VMS system where applicable.

The intercom system shall be fully integrated into the PSIM platform for centralized monitoring and operational control.

The system shall include a physical desk-mounted master control console for local operation.

The intercom system shall support open SIP standards and interoperability with third- party SIP PBX systems.

Performance

Call setup time - ≤ 2 seconds

Audio latency - ≤ 300 ms end-to-end.

Integration with the PSIM

The system integration with PSIM shall support at minimum:

a. Real-time device visualization on MAP/GIS interface.

b. Device status monitoring, including fault, offline, and communication loss conditions.

c. Remote operation of intercom door units via PSIM interface.

d. Event logging and alarm generation within PSIM.

Intercom master station console

C2: CBK - Official

Communication protocol	SIP
Capacity	16 lines with up to 16 SIP accounts
Display	8” full colour touchscreen, 1280x800 pixels, IPS LCD
Camera	Tiltable 2 mega-pixel CMOS camera, 1080P@30fps
Camera privacy shutter	Required
Video frame rate	Up to 30 fps
Microphone	Dual-mic, speakerphone with noise reduction and echo cancellation
Construction materials	Stainless steel or aluminium
Security	User and administrator level passwords, SHA-256 or higher based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1x media access control, anti-hacking secure boot
Protocols	SIP, RTP/RTCP, TCP/IP, HTTPS, DNS, DHCP, NTP TLS, 802.1X, SRTP, IPv6 supported
Network interface	2 x RJ45 (Ethernet) 10/100/1000 Mbps with integrated PoE/PoE+
Power supply	PoE IEEE 802.3af/802.3at Class 4
IP rating	IP54
Impact rating	IK06
Operating temperature	-5°C to 40°C
Relative humidity	15% to 90%
Certification	CE marking or equivalent internationally recognized standards (EN, IEC)

C2: CBK - Official

Video intercom door unit

Video	
Camera resolution	Minimum 2 MP (Full HD 1080p)
Compression	H.264, H.265, Motion JPEG
Sensitivity	0.1 lux (color mode), 0 lux in IR illumination mode
Frame rate	25 FPS
Field of view	Horizontal field of view: minimum 130° Vertical field of view: minimum 90°
ONVIF	Required
Audio	
Maximum sound pressure level (at 0.5 meter)	106 dB
Frequency range	200 Hz – 7000 Hz
Internal speaker	10 W class D
Audio technology	Full open duplex, switched open duplex
Audio features	Acoustic Echo Cancellation (AEC), Automatic volume control (AVC), Automatic gain control
General	
SIP protocol	Supported
Call button	Backlit, LED
Speaker & microphone	Included, integrated
Construction materials	Stainless steel or Aluminum or Polycarbonate
Supervision functions	Keep alive test, tone test

C2: CBK - Official

Ethernet connector	1 x RJ-45
Security	IEEE 802.1X, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), X.509 Certificate PKI, host- based firewall
Installation	Options for wall or flush mounting
Power supply	PoE+ Class 4 (Type 2)
IP rating	IP 66
Impact rating	IK10
Operating temperature	-5°C to 65°C
Relative humidity	15% to 90%
Certification	CE marking or equivalent internationally recognized standards (EN, IEC)

Intercom pole

The intercom pole shall be designed for outdoor installation and mechanical stability.	
Pole height	2.0 meters from finished ground level
Intercom units	2 units mounted on the pole
Unit mounting heights	Lower Unit: 1.3 m Upper Unit: 1.8 m
Pole material	Stainless steel grade 304 or higher for corrosion resistance.
Pole finish	UV-resistant powder coating in RAL color as approved by the Client
Pole diameter	Minimum 100 mm with structural reinforcement as required

C2: CBK - Official

Base / Foundation	Minimum 300 × 300 × 500 mm or as per geotechnical requirements
Cable routing	Internal via protected conduit (minimum 25 mm diameter) with waterproof sealing
Installation	The installation shall ensure vertical alignment within ±2° tolerance and proper grounding in accordance with electrical safety standards

LICENSE PLATE RECOGNITION SYSTEM

General

In accordance with the Client's current access policy, vehicle access to the sites shall be authorized manually by security guards, and automatic access shall not be permitted.

The LPR system shall capture and record vehicle number plates, store the data securely, and provide functionality for review and debriefing.

The system is required to also support the following operational methods:

a. Access to the site will be manually controlled by the guards via the gate control console. The LPR camera will identify the vehicle number and will send positive notification to the guard workstation.

b. Access to the site will be automatic; the gate elements will open automatically upon vehicle identification by the LPR camera. The system will send positive notification to the guard workstation.

c. Controlled exit from the site/barrier.

d. Automatic exit from the site/barrier.

System architecture

The system shall be based on centralized architecture where the main servers and data base are located at the corporate Main Security Center. Management (MSC) at the local sites shall be via Client workstations.

C2: CBK - Official

Data from the sites shall be synchronized and monitored from the MSC for centralized reporting, analysis, and configuration.

The solution may be implemented as a standalone LPR application, a module integrated within a VMS platform, or a PSIM-integrated LPR module, provided that all functional and performance requirements specified herein are fully met. If the Contractor chooses to provide a solution based on a dedicated LPR product requiring dedicated application servers, the cost of all required software licenses and servers shall be included as part of the LPR channel cost.

System management shall be performed via the PSIM/VMS platform for operational functions. Administrative and advanced configuration functions may be performed via the LPR/VMS management software provided by the Contractor. Web-based management interfaces shall not be used as the primary management method.

The central server shall be capable of aggregating data from all local workstations and LPR cameras across multiple sites. It shall provide centralized reporting, analytics, and alerts, enabling the MSC to monitor the entire network of cameras and vehicles.

From both the local sites and the MSC it will be possible to:

a. Define rules for specific vehicles.

b. Create whitelist.

c. Create blacklist.

d. Add vehicle to database.

e. Remove vehicle from database.

f. Update vehicle status.

g. Allocate time windows and restrictions.

h. Generate reports.

Functional requirements

The LPR system is required to recognize all valid license plates approved by the Ministry of Transport, including plates with numbers and letters such as diplomatic or foreign plates, as well as the ability to recognize military and police numbers.

C2: CBK - Official

The LPR system shall be scalable, supporting the addition of an unlimited number of sites, servers, and LPR cameras.

The solution may support edge-based processing, server-based processing, or a hybrid architecture, provided all performance requirements are achieved.

The system is required to detect vehicles with at least a ≥98% probability (at a driving speed of up to 30 km/h) under manufacturer-recommended installation conditions.

The system is required to enable recognition of more than ≥96% of readable vehicle license plates (at a driving speed of up to 30 km/h) under manufacturer-recommended installation conditions.

The system will allow recognition in both day and night conditions, as well as under changing weather conditions.

The detection time from trigger activation to decoding will not exceed 1.0 second.

The time from trigger activation to barrier opening (and/or receiving positive manual opening approval from the guard) will not exceed 1.5 seconds.

C2: CBK - Official

The system must be able to store images and decode data even in offline mode. The system shall continue to perform vehicle detection and license plate recognition during temporary communication interruptions between field devices and the management server, through edge processing, local buffering, or equivalent mechanisms.

The system will include all the necessary computing systems, controllers, and switches required for its full operation.

The system shall include a report generation module with multiple filtering options.

Vehicle triggering shall be achieved through inductive loops, camera-based vehicle detection, radar sensors, or equivalent technologies. Inductive loops are preferred.

The system shall support forensic vehicle search based on:

a. License plate.

b. Partial plate.

c. Date and time range.

d. Site and lane.

The system shall be integrated with the UVSS, ACS and PSIM.

System main components

The system will consist of:

a. Inductive loops (for vehicle detection and triggering).

b. LPR camera.

c. LPR software.

d. Database.

e. Central server including synchronization server.

f. Client workstation at the MSC and local sites (Can be part of VMS Client). g. Card/controller for integration with barriers.

C2: CBK - Official

Integration with the PSIM

The integration with the PSIM software shall support the following:

a. Adding authorized vehicle to the site.

b. Allocation of schedule (timeframe) to vehicles.

c. Deleting vehicle from the site.

d. Display of system faults and alerts.

e. Generation of reports.

Cyber security

The LPR platform shall support:

a. Role-based access control.
b. Multi-factor authentication.
c. Audit trail.
d. Active Directory / LDAP integration.
e. TLS 1.2 or higher.
f. Encrypted database communication.
g. Secure backup and restore.

C2: CBK - Official

LPR software

Language	The software shall be in English
Database	Microsoft SQL or equivalent
Capacity	Capability to manage 5,000 vehicles or more
Vehicle groups	Minimum of 10 vehicle groups
Number of main parking lots	Minimum of 30 main parking lots (sites)
Number of entry and exit lanes	Minimum of 30 entry lanes Minimum of 30 exit lanes
Software functions	Create and manage sites, gates, lanes, and LPR camera locations. Add, edit, suspend, and delete authorized vehicles. Manage vehicle information including license plate number, vehicle category, company, driver name, contact details, and associated documentation. Create and manage whitelist and blacklist databases. Support import and export of vehicle databases in standard formats (CSV, XLSX, XML, or equivalent). Assign vehicles to one or more sites, gates, or access zones. Define vehicle access schedules, time windows, and validity periods.

C2: CBK - Official

	Configure vehicle-specific entry and exit permissions. Configure rules for temporary, permanent, contractor, employee, visitor, emergency, and service vehicles. Register visitor vehicles and assign temporary access permissions. Record the details of the person authorizing or creating vehicle access permissions. Generate real-time alerts for unauthorized vehicles, blacklisted vehicles, expired authorizations, and abnormal access events. Support manual approval workflows for vehicle access where required. Search and retrieve vehicle records using multiple criteria including license plate number, driver name, company, vehicle group, site, gate, date, and time. Generate operational and audit reports including authorized vehicles, unauthorized vehicles, blacklist events, vehicle movements, access violations, communication failures, and system events. authorized vehicles, unauthorized vehicles, blacklist events, vehicle movements, access violations, communication failures, and system events.
	Maintain a complete audit trail of all vehicle database modifications, access permission changes, and operator actions. Support synchronization of vehicle databases between local and central management servers

C2: CBK - Official

	Support integration with ACS, PSIM, UVSS, barriers, gates, and third-party security systems through standard APIs and integration interfaces. Support bulk enrolment, modification, and deletion of vehicle records
Camera's capacity	The system will be able to control at least 30 LPR cameras
Search criteria	The system will support a variety of search criteria such as vehicle number, driver's name, specific parking lot, time, date, company, and more
Report generation	The system will support the generation of various reports with multiple filters, including, but not limited: Entries and exits to a parking lot (site) by day, week and month. Filtered by name or group Blacklists Displaying parking duration Vehicles entry without being in database. Fault Report Abnormal barrier Openings 10 additional reports as defined by the Client Reports shall be exported in XLS format and PDF format. Reports shall be generated based on filters for parking lot or the entire system
Permissions	Ability to set permissions/limitations for each vehicle or user
System alerts	The system will generate alerts for at least the following events: Open barrier that remains open for more than 120 seconds.

C2: CBK - Official

	Loss of communication between the LPR camera and the control unit. Faulty LPR camera. A vehicle is parked in the lot and has not exited within the defined time frame. Vehicle on the blacklist. Vehicle not found in the database. The alerts will be received at the PSIM client station

LPR server

All requirements are recommendation; the Contractor shall provide a server that meets the LPR manufacturer's specified hardware and software requirements. The server hardware and software shall ensure uninterrupted operation under maximum load without any performance degradation according to system capacity, functional requirements and manufacturer recommendations The Contractor may propose a system that can be fully managed through the PSIM, eliminating the need for a dedicated Server.	
Brand	Dell or HP or approved equivalent
Operating system	Windows Server 2019 / 2022 or Linux (Ubuntu LTS or equivalent)
CPU	Intel Xeon Silver or equivalent
RAM	32 GB of RAM (minimum 6 GB dedicated to SQL Server)
Storage	Dedicated RAID5 storage with 4 enterprise grade disks or better
Power supply	220VAC
Operation temperature	0 – 35 C
Relative humidity	80% (non-condensing)

C2: CBK - Official

LPR client workstation

All requirements are minimum requirements. The Contractor shall provide a workstation that meets the LPR manufacturer's specified hardware and software requirements. The workstation hardware and software shall ensure uninterrupted operation under maximum load without any performance degradation. The Contractor may propose a system that can be fully managed through the PSIM, eliminating the need for a dedicated Client workstation.	
Manufacturer	Dell or HP or approved equivalent
Processor	Quad-core 3.0 GHz or higher (Intel i5/i7 or AMD equivalent)
RAM	16 GByte
Storage	500 Gb SSD or better
Network interface	1 Gbps Ethernet (minimum)
Audio	32-bit sound card and speakers
Graphics accelerator	Dedicated or integrated GPU supporting Full HD video display and hardware acceleration
Security	Role-based login, encrypted connection to LPR server (TLS/HTTPS), antivirus/endpoint protection
	USA; FCC Class A EU countries: EN 55022 Class A Japan: VCCI Class A
Electromagnetic immunity	Generic Immunity EU countries: EN50082-1
Operating temperature	10 °C – 35°C
Humidity	20% to 80% (non-condensing)
Input voltage	90 V AC to 264 V AC
Operating system	Latest windows edition

C2: CBK - Official

General	The workstation will be provided with all required hardware including computer, monitor, keypad and mouse

LPR camera

Image sensor	1/2.8” progressive scan CMOS
Lens	Motorized varifocal lens suitable for the required capture distance and lane width
Resolution	1920x1080 (Min)
Frame rate	Up to 60 fps in all resolutions (WDR off)
Minimum focus distance	0.5 meter
IR	Required, range - 30 meters
Minimum illumination	Color:0.1lux, 0 Lux with IR illumination on
WDR	120 DB
Shutter speed	1/66500s to 2s
Video compression	H.264, H.265, JPEG
Pan/Tilt/Zoom	Digital zoom capabilities
Protocols	IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS 2, TLS 2 , QoS Layer 3 DiffServ, SFTP, SMTP, mDNS (Bonjour), SNMP v1/v2c/v3 (MIB II), DNS/DNSv6, DDNS, NTP, PTP, NTS, RTSP, RTP, SRTP/ RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCPv4/ v6, ARP, SSH, LLDP, CDP, ONVIF Profile G/S/T support
Security	Signed OS, brute force delay protection, digest authentication and Secure authentication via TLS 1.2 /

C2: CBK - Official

	1.3, HTTPS, certificate-based authentication, role-based access control, password protection
ONVIF	The camera shall support ONVIF Profile S,T and M.
IP rating	IP 66
Impact rating	IK 10
Power supply	PoE) IEEE 802.3af/802.3at Type 1 Class 3
Operating temperature	-40°C to 50 °C
Operating humidity	10–100% RH (non-condensing)

LPR camera pole

Pole Height	1.0 meters from finished ground level
LPR units	1 unit mounted on the pole
Pole construction and material	Square section, 80×80 mm, Mild steel or Stainless steel (304 grade for corrosion resistance)
Pole finish	Powder-coated (UV-resistant), RAL color
Base / Foundation	Base plate with anchor bolts for secure installation; suitable for concrete foundation or floor mounting. Base plate ≥ 8 mm thick.
Cable Routing	Internal conduit, minimum 25 mm diameter, protected from water ingress
Installation	Vertical alignment ±2°, all wiring terminated in accessible junction box, grounded per safety code

C2: CBK - Official

UNDER VEHICLE SCANNING SYSTEM

General

The Undercarriage Vehicle Scanning System (UVSS) shall be installed at the designated vehicle entry points, as specified in the Bill of Quantities (BOQ).

The system shall provide high-resolution imaging, automatic anomaly detection, image comparison, and operator-assisted inspection.

Images of the vehicle undercarriage shall be displayed to the operator via a dedicated PC workstation responsible for image processing and display.

There shall be two operational modes:

a. Manual undercarriage scanning for vehicles undergoing inspection for the first time.

b. Automatic comparison of the undercarriage against stored reference images.

To support Operational Mode B, the UVSS shall be integrated with License Plate Recognition (LPR) cameras for vehicle identification.

The UVSS system is not required to integrate with other ISS components, except for the LPR system.

Functional requirements

The system shall provide automatic detection of foreign objects, suspicious items, and anomalies attached to or present on the vehicle underside.

The system shall perform real-time image acquisition, processing, and stitching to generate a continuous, high-resolution panoramic image of the complete vehicle undercarriage.

The UVSS scanning unit shall feature a fixed configuration suitable for surface- mounted or flush-mounted installation within the roadway, according to the approved design and site conditions.

C2: CBK - Official

Detected anomalies shall be automatically highlighted and clearly indicated to the operator for further inspection using visual markers and overlays.

The system shall allow manual operator review, including zoom, pan, image enhancement, and comparison with reference or historical images for the same vehicle.

The system shall accommodate variations in vehicle height, ground clearance (low or high ground clearance), or length of the vehicle undercarriage and shall be capable of inspecting vehicles of varying sizes and configurations, within the system's rated load and width specifications.

The system shall be capable of scanning and inspecting vehicles at speeds ranging from 0 km/h to 30 km/h while maintaining compliant image quality and detection performance. The maximum operational scan speed shall be configurable, and operation at higher speeds shall not degrade image continuity or detection performance.

The system shall produce clear, undistorted, and seamless composite images of the vehicle undercarriage, including when vehicles stop, move slowly, or exhibit non- uniform motion over the scanning unit. Image quality and stitching accuracy shall be maintained regardless of stoppage, non-uniform motion, or slow vehicle movement over the scanner.

The UVSS shall provide functionality to magnify composite images, both current and historical, to facilitate detailed inspection of any portion of the vehicle underside.

The UVSS shall be capable of dynamically and automatically adjusting the brightness and contrast of composite images to ensure optimal image quality under varying external lighting conditions, including direct sunlight, shade, and low-light environments.

The UVSS shall provide real-time simultaneous display of all relevant data, including composite images of the vehicle underside, vehicle frontal images, and license plate information. All data shall appear on the operator workstation monitor with minimal latency to allow instant situational awareness and decision-making.

The operator shall be able to view and compare reference and live images, search and mark suspicious zones, and allow or deny the subsequent movement of a vehicle - all within a single GUI.
The UVSS applications and operating software shall be based on Windows or Linux platforms. It shall provide a user-friendly graphical user interface (GUI), allow multiple users with role-based access to log into the system, and include a robust search facility for rapid retrieval of stored data.

The system shall retain images for 30 days.

Technical specifications

C2: CBK - Official

All technical specifications listed below represent minimum mandatory requirements. The Contractor shall provide a UVSS solution fully compliant with all functional and operational requirements specified in this document	
Camera technology	The UVSS may utilize area-scan, line-scan, or hybrid imaging technology, provided that the system fully complies with all specified functional, operational, and image quality requirements, including operation under stop-and-go traffic conditions and temporary vehicle stoppage over the scanning unit.
Image resolution	The UVSS shall generate a composite undercarriage image with a minimum effective resolution of ≥ 8 megapixels per vehicle (stitched composite equivalent)
Pixel density	The system shall provide a minimum spatial resolution (pixel density) of: • ≤ 1.5 mm per pixel (minimum requirement) across the full undercarriage area • ≤ 1.0 mm per pixel (high-security target performance) • Pixel density shall be maintained uniformly across: • Vehicle centerline • Wheel tracks • Edge regions and extremities The system shall not use digital upscaling or interpolation to artificially meet resolution requirements.
	The imaging system shall maintain consistent resolution regardless of vehicle speed variation within the specified operational range (0–30 km/h).

C2: CBK - Official

Scan time per vehicle	The system shall render the complete composite undercarriage image on the GUI within 3 seconds after image acquisition is completed, regardless of whether the vehicle is moving or stationary over the scanning unit
Minimum pause between scans	The system shall support consecutive vehicle scans with a maximum interval of 3 seconds between vehicles
Speed range	Operational vehicle speed range: 0 km/h to 30 km/h. The system shall support stop-and-go vehicle movement and complete vehicle stop above the scanning unit without image corruption.
Minimum vehicle ground clearance	The system shall support inspection of vehicles with a minimum ground clearance of 100 mm
Illumination	Integrated illumination suitable for day, night, and low- light operation and shall automatically compensate for varying environmental conditions
Illumination lifetime	≥ 50,000 hours at nominal operating condition
Maximum axle load	Minimum supported axle load: 30 tons per axle
Communication protocols	10/100/1000 Mbps Ethernet
Availability	The UVSS shall achieve a minimum system availability of ≥ 99.5% uptime on a monthly basis
MTBF	Not less than 20,000 operational hours
MTTR	Not exceed 4 hours for critical components under normal maintenance conditions

C2: CBK - Official

Automatic fault detection	The system shall include automatic fault detection and real-time health monitoring for all critical subsystems, including: • Cameras • Illumination units • Processing unit • Network connectivity
IP rating	IP68, Minimum
Housing and top plate	Housing and roadway top plate shall be constructed of heavy-duty corrosion-resistant steel and/or aluminum suitable for outdoor roadway installation
Finishing	Protective anti-corrosion finishing suitable for outdoor installation and harsh environmental conditions
Operation temperature	-10°C to +70°C
Power supply	110–240 VAC, 50/60 Hz
Protection	The system shall include: • Surge protection • Lightning protection • Grounding (according to local standards)
Standards	CE, IEC 60204-1:2016

Detection performance

The UVSS shall provide automatic detection of foreign objects, anomalies, and suspicious modifications on the vehicle undercarriage using image processing and/or AI-based analysis.

C2: CBK - Official

The system shall achieve a minimum anomaly detection rate of ≥ 95% under controlled test conditions, including but not limited to:

a. Attached objects of metallic and non-metallic materials.
b. Objects with minimum detectable size of 100 mm × 100 mm or equivalent surface area.
c. Objects mounted on flat and curved undercarriage surfaces.

The false alarm rate shall not exceed 5% under normal operational conditions.

The system shall be capable of detecting anomalies under varying environmental conditions, including:

a. Daylight, direct sunlight, and shadowed conditions
b. Night-time operation using IR illumination
c. Light rain and dust conditions

Detection shall remain effective for vehicles moving at speeds from 0 km/h to 30 km/h, including during temporary stoppage over the scanning unit.

Detected anomalies shall be automatically highlighted on the composite undercarriage image using visual indicators (e.g., bounding boxes, color overlays, or markers).

The system shall provide operator verification tools allowing confirmation, rejection, or classification of detected anomalies.

The UVSS shall support logging of all detected events, including:
a. Timestamp.
b. Vehicle identification (linked via LPR system where available).
c. Captured images.
d. Operator actions.

Cyber security

The UVSS shall implement role-based access control (RBAC) with at least the following user roles:
a. Administrator
b. Operator
c. Supervisor

All user authentication shall enforce strong password policies and account lockout after repeated failed login attempts.

All communication between UVSS components, workstation, and external systems shall be encrypted using industry-standard secure protocols (e.g., TLS 1.2 or higher).

C2: CBK - Official

The system shall maintain immutable audit logs for all user actions, including:

a. Login/logout events.
b. Image reviews and modifications.
c. Alarm acknowledgements.
d. System configuration changes.

Audit logs shall be protected against unauthorized modification and shall be exportable for forensic analysis.

The system shall support secure time synchronization using NTP or equivalent.

Server / workstation

The server specifications are minimum Requirements; the Contractor shall provide a server that meets the UVSS manufacturer's specified hardware and software requirements. The hardware and software shall ensure uninterrupted operation under maximum load without any performance degradation according to system capacity, functional requirements and manufacturer recommendations	
CPU	Intel Xeon Silver / Gold (8–16 cores)
RAM	32 GB
Storage (Archive)	6 TB configured in a hardware RAID-5/6
Storage (OS+DB)	1 TB SSD
Network	Dual Gigabit or 10 GbE
GPU	Dedicated GPU according to manufacturer recommendations
Operating system	Windows Server 2022 Standard (64-bit) or latest stable release
DB	Microsoft SQL server standard
Operation temperature	-10 + 40 C
Operating humidity	10–85% RH (non-condensing)

C2: CBK - Official

RADAR

General

The Contractor shall provide, install, test, and commission a radar-based intrusion detection system for perimeter and area surveillance applications.

The radar system shall be suitable for medium-range and long-range perimeter protection applications.

The radar system shall provide automatic detection, tracking, and classification of moving targets within the protected area.

The system shall provide continuous operation on a 24/7 basis and shall be suitable for deployment in critical infrastructure and security applications.

The radar system shall support integration with third-party VMS, PSIM, GIS and Command-and-Control platforms.

The system shall support future expansion through the addition of radar sensors without requiring replacement of existing infrastructure.

The radar system shall be fully integrated with the PSIM platform.

Performance requirements

The radar shall automatically detect, track, and classify moving targets.

The radar shall provide continuous target tracking within its coverage area.

The radar system shall support automatic cueing of PTZ cameras for alarm verification and target tracking. Human detection range shall be not less than 250 meters.

Vehicle detection range shall be not less than 500 meters.

Where applicable, the radar shall detect and track small watercraft.

The radar shall provide horizontal coverage of at least 90°.

The radar shall detect and track targets moving at speeds ranging from 0.1 m/s to 30 m/s.

The radar shall provide a minimum refresh rate of 2 Hz.

C2: CBK - Official

The radar shall support simultaneous tracking of at least 100 targets.

The radar shall provide target location information including:

a. Range.

b. Azimuth.

c. Speed.

d. Track history.

The radar shall provide automatic target classification including, at minimum:

a. Human.

b. Vehicle.

c. Two-Wheeled Vehicle.

d. Animal.

e. Unknown

The radar shall provide a probability of detection (Pd) of at least 95% within the specified detection range.

The radar shall support detection zones, exclusion zones, and masking zones.

The radar shall provide target confidence or quality indication for each detected target.

The radar shall maintain target tracking during temporary target obscuration whenever technically feasible.

The radar shall support configurable detection sensitivity and alarm thresholds.

17.2.18. The radar shall support configurable alarm verification delays to reduce nuisance alarms.

The radar shall include filtering mechanisms to reduce nuisance alarms caused by:

a. Rain.

b. Wind.

c. Vegetation movement.

d. Ground clutter.

e. Environmental reflections.

The radar shall support automatic classification and filtering of nuisance targets including vegetation movement, birds, and small animals. The radar shall provide volumetric detection coverage from ground level up to a minimum height of 4 meters.

C2: CBK - Official

The manufacturer shall provide documented detection coverage envelopes indicating detection width as a function of range.

The radar shall provide continuous coverage throughout its specified detection area without coverage gaps within the published detection envelope.

The radar system shall support 24/7 continuous operation without degradation of detection performance.

Technical requirements

The radar shall utilize solid-state technology and shall not rely on mechanically rotating antennas.

The radar shall be based on FMCW, phased-array, MIMO, or equivalent modern radar technology.

The radar shall operate in frequency bands approved by the applicable regulatory authority.

Communication between the radar and the management platform shall be IP-based.

The radar shall support Ethernet communications.

Power may be provided by:

a. PoE.

b. PoE+.

c. DC Power.

d. Manufacturer-standard power supply.

The radar shall support operation in harsh environmental conditions including rain, fog, dust, snow, and high humidity.

The radar shall support remote firmware upgrades over the network.

The radar shall support automatic recovery following power interruptions.

The radar shall support network time synchronization using NTP.

The radar shall provide diagnostic and health monitoring information including operational status, communication status, and fault indications.

Range measurement accuracy shall be better than ±0.5 meter.

C2: CBK - Official

Angular accuracy shall be better than ±1°.

The radar shall include an integrated GPS receiver and electronic compass, or provide equivalent means for automatic geographic positioning and orientation.

The radar shall be supplied with all mounting brackets and accessories required for wall and pole installation.

The mounting arrangement shall permit azimuth and elevation adjustment.

The radar shall comply with IP67 or better environmental protection rating.

The radar enclosure shall comply with IK10 impact resistance rating or equivalent.

The operating temperature range shall be at least -20°C to +60°C.

Radar management software

The radar management software shall display all detected targets on a geographical map.

The system shall support creation of user-defined detection zones, exclusion zones, masking zones, and alarm zones.

The system shall support alarm generation based on:

a. Target type.
b. Speed.
c. Direction.
d. Dwell time.
e. Zone crossing.
f. Target confidence level.

The system shall support multiple user-configurable operational profiles.

The system shall support automatic PTZ camera positioning based on radar target coordinates.

The system shall provide target tracking history and forensic playback capabilities.

The system shall maintain a historical database of alarms, tracks, and events.

The system shall allow replay of recorded tracks and alarms on the geographic map.

C2: CBK - Official

The system shall support user-defined alarm priorities.

The system shall support exporting alarm and event data for investigation and reporting purposes.

The system shall provide system health monitoring for all connected radar sensors.

The system shall support fusion of multiple radar sensors into a unified operational display.

The system shall consolidate detections from overlapping radar coverage areas into a single operational picture.

The system shall maintain continuous tracking of targets moving between adjacent radar coverage areas.

The system shall support target prioritization based on configurable threat levels, alarm zones, or proximity criteria.

The system shall provide alarm and event forwarding to external systems.

Integration and cybersecurity

The system shall support open APIs and SDKs for third-party integration.

Thesystem shall support integration with VMS and PSIM platforms through standard industry protocols and APIs.
The system shall support secure network protocols including HTTPS, TLS 1.3, and 803.1X authentication."

The system shall support encrypted communications between radar sensors and management servers.

The system shall support HTTPS-based management interfaces.

User authentication and role-based permissions shall be supported.

The system shall support role-based user management with configurable permissions.

The system shall maintain audit logs for user logins, configuration changes, user activities, alarms, and system events.
The system shall support deployment in redundant server configurations, including failover architectures where required by the project.

The system shall support database replication and automatic recovery following server failures.

The radar shall operate only in frequency bands approved by the applicable national regulatory authority.

C2: CBK - Official

LIDAR RADAR

LiDAR system performance parameters

Detection Range: 2m–450m (nominal conditions).
Field of View (FOV): 120° Horizontal x 24° Vertical.
Angular Resolution (max): 0.1° Horizontal x 0.05° Vertical.
Frame Rate: 10 FPS.
Points per Second: 5.76 million.
Range Resolution: 1 cm.

Zone configuration requirements

Each field unit shall support:

a. Minimum 1–64 configurable detection zones.
b. 2D polygon definition (ground map).
c. 3D height envelope (minimum/maximum height) per zone.
b. Support for Exclusion Zones to suppress alerts from static known objects.
c. Tracking capacity of at least 200 simultaneous objects (tracks) per unit, including object-event correlation.

Laser characteristics

Wavelength: 905nm.
Laser Safety Class: Class 1 (Eye-Safe), compliant with IEC 60825-1 and FDA.
Scanned Lines within FOV: 480.

Coverage geometry

Range (m)	Horizontal coverage (m)	Vertical coverage (m)
2	6.50	0.85
450	1,550	180

GIS Interface

Map-based display of units and zones.

C2: CBK - Official

Timeline-based historical navigation.

AI capabilities

The system shall support object classification (human, vehicle, animal, unknown).

The system shall support false alarm filtering (vegetation, vibration, rain).

The system shall support static object detection in sterile zones.

The system shall support 3D visualization and analytics rendering.

CCTV Cameras integration

Integration via ONVIF video streaming.

Control of PTZ cameras via ONVIF or vendor API.

Time synchronization via NTP/PTP.

Scalability

The management software shall be able to manage minimum 20 field units.

The system shall support remote configuration deployment.

Display and management

From the system interface it will be possible to:

a. View live Events Screen with classification, priority, timestamp, unit ID, zone ID, and status.

b. View live PTZ video window with synchronized 3D point-cloud overlay.

b. To manage the following actions: verify, close, escalate, assign, annotate, export report.

c. To configure automatic PTZ slew-to-cue functionality and continuous 24/7 recording.

d. To define Role-Based Access Control (RBAC).

C2: CBK - Official

e. To manage Zone configuration.

f. To set alarm rules, time schedules, sensitivity thresholds.

g. To monitor connectivity, temperature, power consumption, sensor availability, fog index.

h. To generate and export reports to PDF/CSV with full audit trail.

C2: CBK - Official

Cyber security

The system shall support

a. Strong device identity validation.
b. Protection against impersonation attacks.
b. Prevention of unauthorized endpoint access.
c. Zero-trust network compatibility.

DATA COMMUNICATION SYSTEM

Industrial 8 RJ45 ports + 2G SFP Managed PoE Switch

Number of ports	8 x 10/100/1000 Base TX ports 2 x Gigabit RJ-45/ SFP combo RS-232 connector: RJ-45 type
Relay output	Dry Relay output: 1A / DC 24V
Power forwarding capability	30W/IEEE 802.3at
System memory	32M Bytes flash ROM, 256M Bytes DDR3 SDRAM
Diagnostic indicators	RJ 45 ports, SFP ports, power, system, alarm relay, PoE
Security	Port based network access control, RADIUS, MAB, TACACS+, IP address security to prevent unauthorized access, Local or remote Server with authentication, Receipt E-mail accounts with mail server authentication, Port security to assign authorized MAC to specific port
Installation	DIN-Rail mounting
Operating temperature	-40 to + 75o C
Operating humidity	0% ~ 95%, non-condensing

Industrial 16 RJ45 ports + 4G SFP Managed PoE Switch

The same requirements for 8 RG45 ports 2 SFP ports but for 16 RG45 ports+ 4 SFP ports.

C2: CBK - Official

Access switch, Managed layer 2/3, 24 ports

Ports	24 10/100/1000 ports
Switching architecture	Non-blocking architecture
Switching capacity	128 Gbps. Min
Processor and memory	Enterprise-grade multi-core processor with sufficient memory resources to support full switching, routing, QoS, security, and management functions without performance degradation
Throughput	95.2 Mpps
V-LAN support	Required
MAC address table	Minimum 16K MAC entries
POE budget	370 W Class 4 PoE/PoE+
	Access control list (ACL) RADIUS Terminal Access Controller Access-Control System (TACACS+) MAC-based client authentication DHCP snooping DAI IP-MAC-port binding Port isolation
Logging	Syslog support
Monitoring tools	Port statistics, bandwidth monitoring, CPU/memory monitoring
Fan	Hot-swappable, redundant fan trays included (N+1) redundancy)

C2: CBK - Official

Power supplies	2x100-240VAC power supplies (Hot-swappable)
Operating voltage	100 VAC–240 VAC -48 VDC to –60 VDC
Management	IMC; Smart MC, command-line interface; web browser; SNMP manager, Support IPv4 and IPv6 dual-stack networking and management capabilities
Operating temperature	-5° - 45°C
Operating humidity	10 to 90% (noncondensing)
Certifications	CE, FCC, RoHS, UL listed or equivalent

Layer 3, Managed core switch

Layer 3	The switch shall support full Layer-3 routing including OSPF, BGP, VRRP, Static Routing and IPv6.
Ports	24 × SFP+ plus additional 4 × QSFP+/SFP28 uplinks
Switching architecture	Non-blocking architecture
Switching capacity	850 Gbps. Min
Stacking / Redundancy	VSF stacking with cross-chassis link resilience
Multicast support	The switch shall support IGMP Snooping and Layer-3 multicast routing including PIM-SM.
QoS	The switch shall support advanced QoS including DSCP, traffic prioritization and queue scheduling
Jumbo frames	Support jumbo frames of at least 9,000 bytes

C2: CBK - Official

Packet Buffer	The switch must include an intelligent, dynamically allocated packet buffer memory of at least 8 MB to mitigate micro-bursts caused by advanced camera video analytics and motion-triggered event streams.
Processor and memory	Multi-core CPU, ≥ 4–16 GB DRAM
Forwarding Rate	At least 400 Mpps
V-LAN support	Required
MAC address table	≥ 64K entries
Security	Access control list (ACL) RADIUS Terminal Access Controller Access-Control System (TACACS+) MAC-based client authentication DHCP snooping DAI IP-MAC-port binding Port isolation
Logging	Syslog support
Monitoring tools	Port statistics, bandwidth monitoring, CPU/memory monitoring
Fan	Hot-swappable, redundant fan trays included (N+1) redundancy)
Power supplies	2x100-240VAC internal power supplies (Hot- wappable)
Operating voltage	100 VAC–240 VAC -48 VDC to –60 VDC
Management	IMC; Smart MC, command-line interface; web browser; SNMP manager

C2: CBK - Official

Operating temperature	-5° - 45°C
Operating humidity	10 to 90% (noncondensing)
Certifications	CE, FCC, RoHS, UL listed or equivalent

Optical patch panel

Form factor	19-inch standard rack-mount panels, 1U
Material	Cold-rolled steel, aluminium, or alu-zinc alloy. Powder- coated finish
Capacity	24 ports
Connectors type	LC or SC
Fiber type	Single Mode (OS1/OS2) and/or Multimode (OM3 / OM4)
Splice trays	Required, modular, removable
Fiber management	Internal fiber routing guides
Minimum bend radius	Compliant with ITU-T and TIA standards
Cable Entry	Cable entry from rear, side, bottom with integrated strain relief mechanisms to maintain minimum fiber bend radiusFront cable management rings/guides shall be provided.
Labelling	Fiber, port, and splice tray
Grounding	The panel shall include grounding/bonding points compliant with telecommunications grounding standards.
Operating temperature	-20°C to +60°C
Compliance standards	IEC 61754, TIA/EIA-568, ISO/IEC 11801 or equivalent

C2: CBK - Official

Flammability rate	UL 94 or equivalent

Patch panels shall be supplied fully populated with adapters and accessories unless otherwise specified.

Copper patch panel

Form factor	19-inch standard rack-mount panels, 1U
Material	Cold-rolled steel, aluminum, or alu-zinc alloy. Powder- coated finish
Capacity	24 ports
Connectors type	RJ45
Cable category support	CAT 6A / CAT 7
PoE support	Compatible with IEEE 802.3af/at/bt PoE
Labelling	Cable and port
Grounding/bonding	Required
Operating temperature	-20°C to +40°C
Compliance standards	ANSI/TIA-568.2-D and ISO/IEC 11801 Class EA.
Flammability rate	UL 94 or equivalent

Single mode fiber optic cable – 12 cores

Fiber category	OS1 or OS2 (depending on whether for indoor use or outdoor use) The patch panel shall support OS2 single- mode and OM3/OM4 multimode fiber infrastructures.
Operating wavelengths	1310 nm / 1550 nm

C2: CBK - Official

Tensile strength	500 N to 1000 N
Bend radius	According to manufacturer specs
UV resistance	Required
Marking	The cable outer jacket shall be provided with white embossed printing. The marking shall clearly and legibly include the manufacturer's name, manufacturer part number, batch/lot number, manufacturing date, and continuous sequential meter marking along the entire cable length
Water blocking	Gel-filled or Dry water-blocking
Operating temperature	−40°C to +70°C
Compliance standards	ITU-T G.652.D, IEC 60793, IEC 60794, EC 60332-1 / IEC 60332-3 (if LSZH)

Single mode fiber optic cable – 24 cores

The same requirements as for single mode fiber optic cable with 12 cores.

C2: CBK - Official

CAT 7 data cable

Compliance standard	ISO/IEC 11801 Class F, IEC 61156-5
Conductor size	23 AWG
Pair construction	Individually shielded twisted pairs
Shielding	Aluminum foil per pair
Jacket material	LSZH (Low Smoke Zero Halogen)
Fire performance	IEC 60332-1, IEC 60754, IEC 61034
Operating temperature	-20°C to +60°C

CAT 6A data cable

Compliance standard	ANSI/TIA-568.2-D, ISO/IEC 11801 Class EA, EN 50173, IEC 61156, and IEEE 802.3
Conductor size	Minimum 23 AWG solid copper
Pair construction	Four (4) twisted pairs
Pair separation	Internal separator or equivalent technology to reduce alien crosstalk
Jacket material	LSZH (Low Smoke Zero Halogen)
Fire performance	IEC 60332-1, IEC 60754, IEC 61034
Marking	Permanently marked with manufacturer name, category rating, length markings, and compliance standards
Operating temperature	-20°C to +60°C

C2: CBK - Official

44U Equipment rack

Type	Equipment rack for 19” installation
Cabinet frame	Heavy-duty steel frame, Electrostatic powder-coated finish
Front door	Made of tempered safety glass or perforated metal design, Mounted on reinforced hinges, fully removable
Rear door	With perforations to enhance airflow and heat dissipation, fully removable
Accessories	The cabinet shall be supplied with all accessories required for the installation of electronic equipment, including mounting rails, trays, and shelves. All unused spaces within the cabinet shall be covered with blank (blind) panels to ensure proper airflow management and a clean installation
Fixed shelves	Included, minimum of four (4) units
Side panels	Removable
Lock	Lockable front and rear doors
Fans	Minimum 4-fan roof-mounted ventilation unit with thermostat control
Thermostat	Required, Included
Documentation box	Required, Included
Cable tray	Vertical and horizontal cabling trays mounted for cables installation

C2: CBK - Official

Electrical outlets	Includes 12 local-standard power outlets power strip designed for installation in a 19″ rack frame. Equipped with a 16 A circuit breaker (G-type) and indicator LED Supplied with a pendant cable up to 15 m in length terminated with a 16 A CEE plug
LED illumination	Required, Included
Tamper switch	Required, Included
I/O Output	Dry-contact alarm outputs for cabinet intrusion, temperature alarm, and power failure indication.
“blind “panels	Will be installed in empty spaces between equipment
Wheels	Equipped with four (4) caster wheels with locking mechanism to secure the cabinet in place
Cables entry	From top or bottom of rack
IP level	IP 20
Standard	Compliant with ANSI/EIA RS-310-D
ACS reader	Cabinet door shall include provision for installation of an access control reader and electronic locking mechanism

C2: CBK - Official

22U Equipment cabinet

The same specifications and requirements as the 44U rack shall apply, adapted for a 22U rack.

15U Equipment cabinet

Type	Wall mounted, 19” installation
Dimensions	Width: Standard 600 mm Depth: Minimum 600 mm
Structure	Steel frame construction
Front door	Front door shall be solid metal or perforated metal construction with lockable mechanism.
Side panels	Removable
Fan & thermostat	Thermostatically controlled ventilation fan unit shall be included
Documentation box	Required, Included
Cable tray	Vertical and horizontal cabling trays mounted for cables installation
Electrical outlets	Rack-mounted power strip. Up to 6 outlets in one unit. Additional outlets required will be installed in a separate unit
LED illumination	Required, Included
Tamper switch	Required, Included
I/O Output	Dry-contact alarm outputs for cabinet intrusion, temperature alarm, and power failure indication.

C2: CBK - Official

Cables entry	From top or bottom of rack
Fixed shelves	Included, minimum of two (2) units
IP level	IP 20
Mounting accessories	Cabinet shall include all wall mounting accessories and hardware.
Standard	Compliant with ANSI/EIA RS-310-D
ACS reader	Cabinet door shall include provision for installation of an access control reader and electronic locking mechanism

6U Equipment cabinet

The same specifications and requirements as the 15U communication cabinet shall apply, adapted for a 6U communication cabinet.

Outdoor communication cabinet

Type	Outdoor communication cabinet, designed for ground installation
Cabinet material	Reinforced polyester
Front door	Solid (opaque) door with lockable mechanism
UV-resistant	Cabinet material shall be UV-resistant and suitable for prolonged outdoor exposure
Fan & Thermostat	Thermostatically controlled ventilation fan unit shall be included
Environmental protection	Waterproof, dustproof, and moisture-resistant

C2: CBK - Official

Circuit breakers	The cabinet will include main breaker and distribution boards for electrical sockets
Grounding	Required. According to local regulation
LED illumination	Included
Tamper switch	Included
I/O Output	Dry-contact alarm outputs shall be provided for intrusion, temperature alarm, humidity alarm, and power failure indication.
Surge protection	Surge protection devices (SPD) shall be provided for AC power and communication interfaces in accordance with IEC 61643.
Cables entry	From top or bottom of cabinet. All cable entries protected against rodents, dust and water
Accessories	The cabinet will be supplied with all required all necessary accessories for the installation of electronic equipment, including mounting rails, trays, cable ducts, power strip (pdu) and shelves The height of the cabinet will be determined based on the required equipment capacity, with an additional 30% reserve for future expansion.
Overvoltage / Lightning protection	Required, included in the price of the cabinet
Grounding	The cabinet shall be properly grounded according to electrical code regulations
Protection standard	IP 65 or better

C2: CBK - Official

Concrete base	The cabinet shall be installed on a levelled concrete base, elevated approximately 20 cm above ground level Base preparation is the responsibility of the Contractor Cost of the base shall be included in the overall price of the cabinet

DIN rail UPS for outdoor communication cabinet

Installation method	DIN rail mounting
Backup time	As per BOQ
Volt-Amps rating	850 VA / 510 W
Voltage	230V (±20%)
Frequency	50 Hz ± 10%
Output voltage	230V ± 5%
Overload protection	105% of nominal load for 20 seconds 120% of nominal load for 10 seconds 130% of nominal load for 3 seconds
Battery	Sealed, maintenance-free lead-acid battery
Short circuit protection	UPS output cut off immediately
Indications	Battery Backup Status Weak Battery Alert Overload Condition
Operating temperature	0°C to +50°C
Humidity	1-95%, non-condensing
Standards	CE, EN62040-1, EN62040-2 or equivalent North America

C2: CBK - Official

UPS for indoor communication cabinet

Operating mode	Line Interactive
Backup time	As per quantity specifications (dependent on load, battery condition, and model selected)
VA ratings	600, 1000, 1500
Frequency detection	Automatic frequency sensing (50-60Hz ±10%)
Input voltage	115V / 230V +/- 25% all line input, 50 or 60 Hz +/-10% (auto sensing)
Output voltage	Simulated sine wave at 230V +/-5%, 50 or 60 Hz +/-1Hz
Overload & short circuit protection	420 joules, Breaker, or fuse for overload & short circuit protection UPS automatic power off if overload exceeds 110% of nominal at 60 seconds and 130% at 3 seconds. UPS output cut off immediately or input circuit breaker protection
Battery type	Gel, Sealed, maintenance- free, UL compliance, MSDS
Alarms and indicators	Backup mode, Weak battery, Overload (Audible beep for status alerts)
Operating temperature	0°C to +50°C
Humidity	1-95%, non-condensing
Standards	CE, EN62040-1, EN62040-2 or equivalent North America

UPS 10 kVA

C2: CBK - Official

Technology	Online double-conversion
Control	Microprocessor-controlled
Phase	Single phase with ground
Capacity	10,000 VA / 9000 W
Generator compatibility	Supported
Converter mode	Frequency converter
Nominal input voltage	208 / 220 / 230 / 240 VAC
Output voltage	208 / 220 / 230 / 240 VAC
AC to Battery mode transfer time	Zero
Inverter to Bypass transfer time	Zero
Protections	Overload, overheating, short circuit, deep discharge, battery overcharging
Indicators	Load level, Battery level, AC mode, Battery mode, Bypass mode, Fault
Audio alarm	Required
Battery	12 V / 9 Ah, AGM (maintenance-free lead)
Operating temperature	0°C to +40°C
Humidity	0-95%, non-condensing
Standards	IEC EN 62040-1, IEC EN 62040-2, IEC EN 62040-3 or equivalent North America standard

KVM extender

C2: CBK - Official

Input interface	HDMI
Output interface	HDMI
Resolution (max.)	1920 x 1200 @ 60 Hz, Full HD (1080 p) or 4 K (up to 2048 x 1152)
Distance (max.)	140 m, 6a cable
Keyboard / Mouse	USB HID (support of keyboard/ mouse with additional module USB 2.0 transparent)
Power supply	International power supply unit (90-240V Input)
Mounting accessories	19” Rackmount
Operating temperature	0 to +50 C
Operating humidity	0 to 90% (no condensing)

Industrial controller (Data acquisition and control module)

I/O type	6 Digital Inputs (DI) + 6 Relay Outputs
DI input type	Dry contact / Wet contact
Communication interface	Ethernet 10/100Base-T(X)
Supported protocols	Modbus/TCP, TCP/IP, UDP, HTTP, DHCP, SNMP, MQTT, ICMP, ARP
Connectors	1 × RJ-45, plug-in screw terminal blocks
Mounting	DIN-rail, wall, or stack mounting
Power supply	10 – 30 VDC
Operating temperature	-10 to +70 C
Operating humidity	0 to 90% (no condensing)

C2: CBK - Official

Rodent repellent system

Device type	Ultrasonic / electromagnetic rodent repeller
Installation type	Plug-in wall outlet
Coverage area	Up to 100 m² open area
Ultrasonic technology	High-intensity ultrasonic sound waves
Electromagnetic feature	Digitally processed electromagnetic waves through internal wall wiring
Frequency operation	Multi-frequency ultrasonic emission (changes periodically to prevent rodent adaptation)
Power supply	85–135 V AC, 50–60 Hz
Operating temperature	0 to +35 C
Operating humidity	0 to 90% (no condensing)
Compliance	CE, FCC, RoHS or equivalent

Environmental monitoring system

Function	Server room environmental monitoring system
Monitoring capabilities	Temperature, humidity, flood, door status
Temperature accuracy	Up to ±0.25 °C
Alerts	Required, SMS, SNMP, HTTP
Data logging	Required, Historical data with graphs
Sensor capacity	Up to 12 sensors
Optional sensors	Flood, door switch, airflow, smoke

C2: CBK - Official

Power supply	85–135 V AC, 50–60 Hz
Operating temperature	0 to +35 C
Operating humidity	0 to 90% (no condensing)
Compliance	CE, FCC, RoHS or equivalent

COMMUNICATION & ELECTRICITY INFRASTRUCTURE

General

All containment systems, conduits, ducts, cable trays, manholes and associated accessories shall be supplied, installed, tested and commissioned as a complete system.

The Contractor shall provide all accessories, supports, brackets, couplers, reducers, bends, pull boxes, warning tapes, identification labels and other components required for a complete installation, whether specifically mentioned or not.

Metal cable tray 60×120 mm

Compliance standard	IEC 61537, EN 50085 or equivalent
Material	Steel, Hot dip galvanized
Installation method	Wall-mounted, suspended, or supported by brackets
Wall thickness	At least 1.0 mm
Fire retardancy	UL 94-V0 or equivalent
Cover and internal divider	Required. Price included in unit price
Accessories	Including all required covers, couplers, bends, tees, brackets, mounting hardware and all other accessories required for complete installation

C2: CBK - Official

Grounding	All metallic trays shall be bonded and grounded in accordance with IEC 60364 and local electrical regulations

HDPE communication conduit, 50 / 75 mm

Compliance standard	UL 651A or equivalent
Material	High-density polyethylene (HDPE), PE100 or PE80 grade
Inner lining	Co-extruded silicone coating for a low coefficient of friction
Wall thickness	4.6 mm
Mechanical strength	High resistance to soil pressure and traffic loads
Chemical resistance	Resistant to oils, acids, alkalis, and most industrial chemicals
Accessories	Provided with all required end fittings, couplers, and mounting clamps and all other accessories required for complete installation
Joining methods	Mechanical couplers, Electrofusion, or Butt Fusion
Cable pulling cord	Included, factory-installed pre-inserted pulling line, 8 mm
Sealing	All conduit entries shall be sealed against water, dust, rodents and insects

Flexible corrugated (flexible) conduit – 32 / 50 / 75 mm

C2: CBK - Official

Compliance standard	IEC 61386-24, EN 61386 (Flexible conduit), RoHS compliant
Material	High-density polyethylene (HDPE) or PVC, flame- retardant, UV-resistant
Internal diameter	Internal diameter shall correspond to the specified nominal conduit size
Mechanical strength	Impact-resistant, crush-resistant per IEC 61386 / EN 61386-24 (flexible conduits)
Chemical resistance	Resistant to oils, acids, alkalis, and most industrial chemicals
Accessories	Provided with all required end fittings, couplers, and mounting clamps and all other accessories required for complete installation
Cable pulling cord	Included, Polyester, Nylon, or Polypropylene, 6-8 mm
Sealing	All conduit entries shall be sealed against water, dust, rodents and insects

PVC duct, 60 / 120 mm

Compliance standard	EC 61386 / BS EN 50085 or equivalent
Material	Rigid PVC, Flame retardant, UV Resistant
Installation method	Wall-mounted or suspended with brackets
Wall thickness	2.0 – 3.0 mm
Fire retardancy	UL 94-V0 or equivalent
Accessories	Including all required covers, bends, tees, reducers, couplers and all other accessories required for complete installation

C2: CBK - Official

Rigid PVC Conduit, 16 / 20 / 25 mm

Compliance standard	IEC 61386-21 (Rigid PVC conduit), EN 61386, RoHS compliant
Material	PVC-U (Unplasticized Rigid PVC), flame-retardant, UV- resistant
Wall thickness	1.5 mm – 3 mm
Mechanical strength	Impact-resistant, crush-resistant per IEC 61386 / EN 61386
Fire Retardancy	Complies with UL94-V0, IEC 60332-1, or equivalent
Accessories	Provided with all required junction boxes, elbows, couplers, end caps, mounting brackets and all other accessories required for complete installation

C2: CBK - Official

Pliable conduit 16 / 20 / 25 mm

Compliance standard	IEC 61386-22 / IS 61386-22
Material	Flame-retardant PVC or Polypropylene
Inner surface	Smooth or low-friction to assist cable pulling
Fire Retardancy	Self-extinguishing / UL 94 V-0 or equivalent
Accessories	Provided with all required PVC couplers, conduit clips, end caps and all other accessories required for complete installation

Manhole, 60cm

Material	Polypropylene (PP), HDPE, reinforced concrete, or composite
Internal diameter	550–600 mm
Number of inlets	1 main inlet + up to 3 side inlets
Adjustable shaft height	Up to 2 m using extensions
Load class (cover)	B125 (12.5 t) or Load Class C250 (as appropriate)
Drainage	The bottom of the manhole shall be provided with a gravel drainage layer not less than 100 mm thick.
Marking	Manhole cover shall be permanently marked: "COMMUNICATION"
Standard compliance	BS EN 13598-2 / EN 1610 or equivalent

C2: CBK - Official

MAIN SECURITY CENTER

General

The Contractor is required for designing, building, and equipping a state-of-the-art Main Security Center (MSC) capable of managing both routine and emergency security operations.

The MSC will be equipped with hardware and PSIM software to receive, analyze, and display routine and emergency events, while monitoring various security subsystems."

The MSC will include fully equipped operator tables, workstations, small monitors, and large display screens.

The Client will provide the space for the MSC in an envelope condition. The Contractor will be responsible for all construction work needed to prepare the space for the installation of electronic systems.

MSC components

The MSC will consist of the following components:

a. Operations Center (OC).
b. Crises Management Room (CMR).
b. Supervisor / Duty officer room.
c. Technical Equipment Room (TER).
d. Operators' rest area.

Operation centre (OC)

The operations room will serve as the primary location for monitoring and managing the ISS. It will support the following functions:

a. Operator control desks.
b. Video Wall.
c. Communication equipment (radios and landline telephones).
d. Service cabinets and desks

The room shall be equipped with specialized lighting fixtures to prevent glare on the monitors and to provide an optimal working environment for perators. The room shall be air-conditioned.

Each workstation shall be equipped with advanced PSIM software and three 24" personal monitors, designated for:

C2: CBK - Official

a. Video viewing.

b. Events monitoring and management.

c. Map display.

The 3D rendering below illustrates the conceptual design of the Operation Center.

FIGURE 12 - CONCEPTUAL 3D RENDERING OF THE OPERATION CENTER

C2: CBK - Official

Crisis Management Room (CMR).

The CMR shall be used by Client management staff during serious emergency events that require senior emergency team to convene and make decisions based on the visual data and information provided by the Operation Center.

The CMR shall be equipped with all necessary communication and control facilities to receive selected information from the various security centers.

The Contractor shall provide complete equipment for the multimedia room, including:

a. Executive conference table for 12 participants.

b. 12 comfortable armchairs.

c. 50" video wall monitors, mounted on a wall or suspended from the ceiling.

d. Electricity and communication outlets in the table and on the walls.

e. Other necessary equipment as required.

A dedicated workstation, equipped with PSIM software, shall be installed in the CMR and operated, when required, by a skilled operator to deliver selected visual images and data from the OC to the emergency team.

C2: CBK - Official

FIGURE 13 - CONCEPTUAL LAYOUT OF THE CMR

Supervisor / Duty officer room

The room will include operator console, PSIM workstation and communication devices.

The room will be air-conditioned.

C2: CBK - Official

Technical equipment room

The MSC equipment room shall include space for at least two (2) 19" racks, covering an area of approximately 7 sqm.

The equipment room's air conditioning (AC) system shall operate continuously, 24/7, using two independent AC units for redundancy, with automatic switchover. These units shall be independent from any other AC systems installed in the facility.

The ambient temperature in the equipment room shall not exceed 24°C.

The AC system in the equipment room shall not include any water-based components.

The required AC capacity (BTU) shall be calculated based on the actual equipment load plus an additional 50% reserve.

The room shall include a raised technical floor.

The room shall be supplied from a dedicated double-pole circuit breaker (a separate electrical circuit for the room).

The room shall be equipped with communication and electrical infrastructure to support the security systems. Power outlets shall be connected to the essential power supply. CEE sockets shall be provided for the server cabinets.

The room shall have no windows. The entrance door shall be a access controlled metal security door (e.g., multi-bolt type) with a 3-star security rating.

Operators' rest area

The Operators' rest area shall include:

a. Fully equipped Kitchenet with cabinets, sink, refrigerator, microwave, dining table, chairs.

b. Toilets.

MSC construction

The Contractor shall establish a professional team, led by an architect and including all required engineers (construction, electrical, acoustic, and others as needed), to design and construct the MSC complex in accordance with this specification.

C2: CBK - Official

The design team shall include local designers to ensure that the design and construction comply with all applicable local laws and regulations.

The MSC design shall be presented to the Client for approval, and the presentation must include 3D renderings. The Contractor may proceed with the works only after receiving the Client's formal approval

In accordance with the approved design, the Contractor shall carry out the required construction, which shall include, but not be limited to, the following works and materials:

a. Construction of plaster walls.

b. Construction of glass partitions.

b. Construction of main complex door and internal doors.

c. Wherever necessary close some of the windows.

d. Construction of double floor and acoustic ceiling.

e. Construction of Main Electrical boards, electrical outlets, grounding and lighting.

f. Construction of data communication access points.

g. Adjustment or replacement of the existing lighting to the needs of the control center

h. Installation of complete air conditioning system.

i. Supply of control desks as specified in this specification.

j. Supply of chairs for the operators as specified in this specification.

k. And other works and materials until full completion of the required MSC according to the attached drawings and specifications.

C2: CBK - Official

The 3D rendering and drawing below present a conceptual view of the MSC.

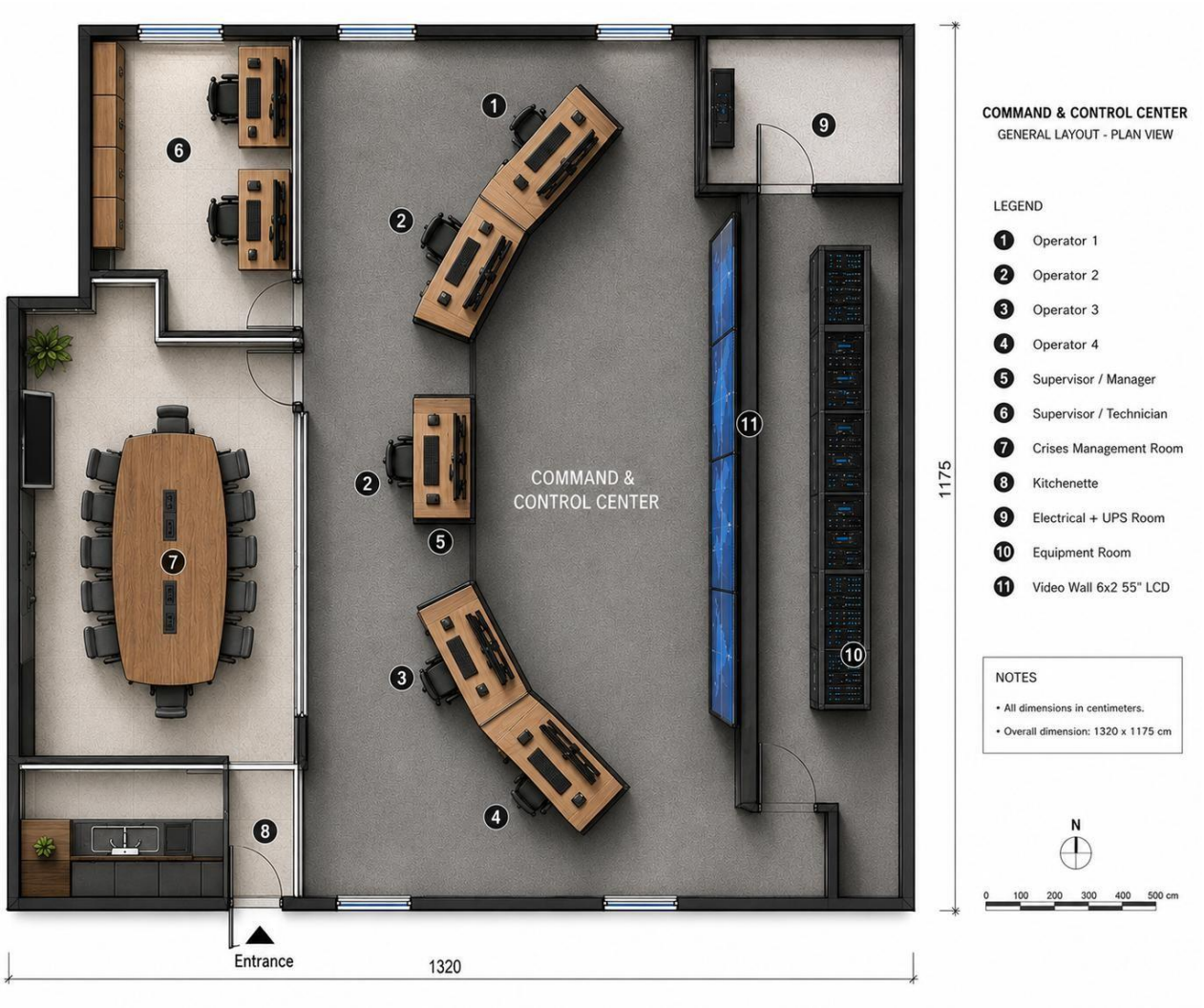

FIGURE 14 - CONCEPTUAL LAYOUT OF THE MSC

C2: CBK - Official

FIGURE 15 - MSC COMPLEX TOP VIEW

Control console module (control desk)

General	The control room console module shall be a purpose-built product engineered for control room applications.
Construction	Modular design with a heavy duty steel frame painted in epoxy powder coating, removable steel panels. The desk surface shall be made of HPL or HPL COMPACT material, 25–40 mm thick, resistant to wear, liquids, and scratches.
Work surface	The work surface corners shall be rounded to prevent injuries. 5 cm-deep edge strip shall be installed on the front of the work surface, made of materials such as rubber or plastic, to protect the work surface from impact.

	The work surface shall include a cable pass-through slot for routing cables from the storage compartment to the work surface. A concealed pop-up desk panel shall be installed on each side of the work surface. The panel shall open with a push mechanism and include three electrical outlets. The panel shall feature a satin aluminium finish.
Maximum load	The module shall be designed to support a load of up to 100 kg.
Fire safety	All materials used in the command module shall be made of fire- retardant materials compliant with UL94.
Length	Minimum length of 1.8 meters. Modules shall be capable of attaching to adjacent modules to create a unified workstation.
Width	800 – 900 mm
Finish materials	The control desk shall be finished in a color, shade, and texture determined by the client according to the control centre's color palette. The desk shall include a nameplate illuminated with LEDs to display the client's name.

Monitors brackets	Arms for monitors shall be provided (3 monitors, 24" each – compatible with monitors supplied by the awarded contractor). The arms shall be designed to accommodate internal cable management. The arms shall be mounted on a rail attached to the work surface, allowing adjustment of distance, height, tilt, and angle. Required load capacity: up to 5 kg per monitor.
Equipment compartment	The desk shall be designed with an equipment compartment for computers and other peripheral equipment. The front of the workstation shall have hinged doors with recessed handles or a door angle that allows easy opening. The doors shall include locks to secure the storage compartment. The rear of the equipment compartment shall be closed by a removable maintenance panel or hinged doors. The panel/doors
	shall feature recessed handles and ventilation openings of at least 15 cm in height and 30 cm in length. Opening the doors shall activate LED lighting inside the equipment compartment, providing sufficient illumination to work within the compartment.
Electricity & communication outlets	Integrated into the desk according to equipment quantities, with a minimum of six electrical outlets, six communication ports, and two telephones.
Cables management	Cables shall enter the desk module from the floor through specialized fixtures that prevent the entry of insects, or via the desk module profile. Cable distribution within the desk shall be managed using horizontal and vertical cable trays.

Thermostat & fan	Required, low noise fans will be located at the back of the desk (away from operators) Ventilation system shall be sized to dissipate the heat generated by installed equipment under continuous operation.
Drawers	Required (at least 3)
Pricing of the Control console module	The price for the command desk, as indicated in the bill of quantities, shall include: Detailed design of the desk. Assembly at the factory, client approval, disassembly, transportation, and installation at the facility. Cutting of raised floors/ceilings, restoration with suitable tiles, and returning the raised floor/ceiling to its original condition. Installation of channels for low-voltage and electrical system cabling. Connection between adjacent desks, including closure of gaps with appropriate panels. All other works and equipment required for the completion and full operational functionality of the desk to the client's complete satisfaction.

C2: CBK - Official

FIGURE 16 - CONCEPTUAL IMAGE OF CONTROL CONSOLE

SCANNING DEVICES

Walk- Through metal detector

Type	Multi-zone metal detector
Detection zones	Minimum 30 localization zones with visual indication on both side panels
Detection sensitivity	Detection sensitivity shall be independently adjustable per zone and per security program
Programs	Minimum 15 selectable security programs

Structure	Stainless steel or heavy-duty aluminum (Detection heads and support). Plastic / ABS Components for panels. Laminate protection against scratch, aging, weather and wear
Local control unit	Alphanumeric display and keyboard
Visual display	Alphanumeric LCD/LED display with zone indication
Audio	Audible signalling
Passageway size	Width: 760 mm, Hight: 2000 mm, Depth: 530 mm
Access control	3-Level Password and hardware key access protection
Self-test	Self-test diagnostics capabilities
Interfaces	Remote via infrared remote-control unit, BT or ethernet 10/100 base T interface
Reset time	0.3 seconds Max
Throughput capacity	Minimum 50 persons per minute
Security	Multi-level password protection and hardware access key
IP level	IP65
Control unit	IP65, anti-vandal
Interfaces	Ethernet 10/100, Bluetooth or IR remote control capability
Alarm outputs	Relay contact for remote alarm
Diagnostics	Automatic self-test and fault diagnostics

C2: CBK - Official

Electromagnetic/environmental immunity	The WMTD shall be immune to environmental electromagnetic interference and shall not interfere with pacemakers, magnetic media, or nearby electronic equipment
Networking/management	The WMTD shall support remote configuration, alarm monitoring, statistics, diagnostics, and event log retrieval over Ethernet network connection
Power supply	100–240 VAC, 50/60 Hz
Operating temperature	-10°C to +60°C
Relative humidity	0 to 95% (without condensation)
Certification and compliance	CE, FCC, IEC, ICNIRP and ECAC/TSA or equivalent international security standards

Hand-held metal detector

Detection frequency	55 kHz
Audio frequency	2kHz
Indications	Visual and audio alarms
Voltage	3.8 Vdc
Battery operating time	Minimum 40 hours continuous use
Desktop charging station	Included in price of unit
IP rating	IP65
Operating temperature	-20°C to +60°C

C2: CBK - Official

Relative humidity	100%
Certification and compliance	TSA, ECAC, STAC, AENA

Luggage screening system

Tunnel size	620 mm (W) x 420 mm (H)
Conveyor speed	0.20 m/sec continuous conveyor speed
Conveyor Load	100 Kg (Max)
X-ray performance	Steel penetration - 42 mm (Typical)
	Wire resolution - 42 AWG (Typical)
Functional requirements	Multi energy imaging (4 Color), View previous/Next bag, Image archive, Configurable image processing keys, Baggage counter, Date / Time display, Search indicator, Integrated UPS supporting minimum 5–15 minutes, controlled shutdown operation, Multi language support, Automatic continuous self-calibration
Image processing functions	Black and white, Organic / Inorganic stripping, Inverse video, High penetration, Low penetration, Pseudo color- Variable
	edge enhancement, Variable color stripping, Variable gamma, Variable density, Dynamic continuous zoom & panning, Digital zoom up to 64x
Operator training software	Integrated operator training and Threat Image Projection (TIP) software shall be provided.
Diagnostic capability	Built-in automatic diagnostics and fault monitoring with operator notification
Anode voltage	160kV

Network	Support Ethernet connectivity for remote diagnostics, software updates, and image archival
Monitor	21" minimum LED monitor with minimum Full HD resolution
System IP rating	IP20
Control panel IP rating	IP43
System power	220/230 VAC ±10%
Operating temperature	-5°C to 40°C
Relative humidity	5 to 95% non-condensing
Certification and compliance	FDA/CDRH 21 CFR 1020.40, 21 CFR Part 1010, CE marking (Safety & EMC), IEC 61010-2-091, IEC 61326 EMC compliance
Standards	ICAO / IATA

GATES & CONTROLLED PASSAGES

Full height turnstile

Features	Bi-directional
Arms	Three-section rotor positioned at 120° intervals
Throughput capacity	minimum 15 passages per minute under normal operation
Control Possibilities	Manually by a local control panel
	By access control system
Materials	Casework: 304 Grade stainless steel
	Rotor spindle: 304 Grade stainless steel
	Rotor wings: 304 Grade stainless steel

Drive unit	A motorized drive unit for controlled rotation. Brushless DC or AC synchronous motor
Security features	Anti-reverse rotation during transit, Self-centering to reset position, Action lock preventing two passages at one time
Safety features	Visibility unimpeded allowing clear view through rotor, logic voltage 24 VDC, voltage-free contact input for fire alarm fail state, anti-pinching design construction The turnstile shall support motor-assisted controlled rotation with manual emergency operation capability. Upon fire alarm activation or power failure, the turnstile shall automatically switch to fail-safe free passage mode. Emergency mechanical release shall be provided for maintenance and emergency evacuation.
Operational modes	Free access Controlled access Permanently locked
	Emergency
Card reader installation	The unit shall be supplied with a dedicated space for installing card readers, integrated within the frame. Option to install two readers (one facing the entrance direction and one facing the exit direction).
Status lights	Required (green – access granted, red access denied)
Control board location	In the upper section of the device
Cables & conduits	Through the ground
Integration with fire detection system	Required
MCBF	3 million cycles

C2: CBK - Official

Grounding/surge protection	The system shall support grounding and surge protection in accordance with electrical regulations.
IP rating	IP 54
Power supply	230Vac 50Hz
Operating temperature	-5°C to +50°C
Operating humidity	RH 95% (Non – condensing)
Anti-corrosion treatment	Required
Back-up Battery	Supports turnstile motorized drive unit for at least two (2) hours of continuous operation
Conformity with standards	EN 17352, EN 16005, CE, IEC 60204-1
The Contractor shall provide all anchoring, foundation, and civil integration works required for installation.	

Speed gate

Passage width	550 – 650 mm
Cabinet length	1000 - 1300 mm
Glass wing height	1800 mm
Construction	Cabinet from 304 grade stainless steel, wings 12mm toughened glass with rubber safety edge
Opening speed	1 sec (Max)
Throughput capacity	Minimum 30–40 persons per minute
Drive unit	DC brushless motor
MCBF	1,500,000 cycles
Electro-mechanical locking	Required

LED way mode indicator	Required (green – access granted, red access denied)
Card reader	The unit shall be supplied with a dedicated space for installing card readers, either integrated within the frame under a glass cover or mounted on a bracket (for face recognition), with the option to install two readers (one facing the entrance direction and one facing the exit direction).
Audio alarm	Required to indicate unauthorized use to both the security personnel and the user
Presence detection	Required. Cells for the detection of the presence of users
Fail safe mechanical opening	Upon fire alarm activation or power failure, the wings shall automatically open to provide free passage (fail-safe mode).
Tailgating detection	Required
Live passage timeout	Required
Battery back-up	Battery backup shall support automatic fail-safe opening and minimum 30 minutes standby operation.
Integration with fire detection system	Required
Fail safe	Mechanical or with battery failsafe opening.
Safety features	Intrusion, tailgating, Piggybacking, wrong way direction, leave aisle timeout
Control panel	Required, to open wings from gourd / receptionist desk (physical panel made of aluminum)
IP rating	IP 40
Power supply	230Vac 50Hz
Operating temperature	+5°C to + 40°C

C2: CBK - Official

Operating humidity	RH 95% No condensing
Conformity with standards	EN or UL

Wide speed gate

Passage width	800 – 900 mm
Cabinet length	1000 - 1300 mm
Glass wing height	1800 mm
Construction	Cabinet from 304 grade stainless steel, wings 12mm toughened glass with rubber safety edge
Opening speed	1 sec (Max)
Throughput capacity	Minimum 30–40 persons per minute
Drive unit	DC brushless motor
MCBF	1,500,000 cycles
Electro-mechanical locking	Required
LED way mode indicator	Required (green – access granted, red access denied)
Card reader	The unit shall be supplied with a dedicated space for installing card readers, either integrated within the frame under a glass cover or mounted on a bracket (for face recognition), with the option to install two readers (one facing the entrance direction and one facing the exit direction).
Audio alarm	Required to indicate unauthorized use to both the security personnel and the user
Presence detection	Required. Cells for the detection of the presence of users
Fail safe mechanical opening	Upon fire alarm activation or power failure, the wings shall automatically open to provide free passage (fail-safe mode).

C2: CBK - Official

Tailgating detection	Required
Live passage timeout	Required
Battery back-up	Battery backup shall support automatic fail-safe opening and minimum 30 minutes standby operation.
Integration with fire detection system	Required
Fail safe	Mechanical or with battery failsafe opening.
Safety features	Intrusion, tailgating, Piggybacking, wrong way direction, leave aisle timeout
Control panel	Required, to open wings from gourd / receptionist desk (physical panel made of aluminum)
IP rating	IP 40
Power supply	230Vac 50Hz
Operating temperature	+5°C to + 40°C
Operating humidity	RH 95% No condensing
Conformity with standards	EN or UL

Accessible swing gate

The gate shall provide accessible passage for wheelchair users, assisted passage, and equipment transport	
Swing	One-way 90 degree or two-way 180 degree
Passage width	1000 - 1200 mm
Glass wing height	1800 mm
Opening time	Opening time shall not exceed 3 second

Minimum throughput	10 passages per minute
Motion sensor	Infrared safety sensors shall detect user presence and prevent accidental closure
Anti-pinch	The gate shall include anti-pinch and anti-collision safety mechanisms
Integrates with ACS	Required
Construction	Frame made from 304 grade stainless steel, 12 mm tempered safety glass compliant with applicable safety standards
Fail safe mechanical opening	Required
Manual release	Manual emergency release shall be provided
Integration with fire system	Input for voltage free contact for fire system
Control panel	Required, to open the gate from guard / receptionist desk (physical panel made of aluminum)
Power supply	110-240VAC, 50/60Hz
IP rating	IP42
Accessibility standards	ADA, EN 16584, local accessibility regulations
safety standards	CE, EN 16005, IEC 60204-1

Anti-ram raising arm barrier - DOD K 4

Level of protection	Barrier shall be certified to stop a vehicle of at least 6,800 kg at 50 km/h
Barrier type	Raising arm barrier
Arm raising speed	Max 12 seconds for complete opening of the arm (raise position)
Arm length	Up to 6 Meters
Daily cycles	500, Minimum
Safety photocells	Safety photocells and obstacle detection systems shall prevent barrier closure on vehicles or pedestrians.
Manual operation	In case of power failure, manual emergency operation shall be possible
Safety features	Loop detector, led on boom, warning lamp
Integration	Barrier shall support integration with access control, LPR, loop detectors
Boom visibility	LED illumination
Finishing treatment	Zinc coating (inside out) anti–corrosion treatment
Color	Painting system in a color shade according to client requirements
Galvanization	Required, according to EN 1461 or ASTM A123 / A123M
Power supply	380V AC 50HZ - 3X16Amp
MCBF	100,000 cycles
Operation temperature	-5 - 50 C
Impact test standard certification	PAS 68, ASTM F2656-20, IWA 14-1

C2: CBK - Official

Price of the unit shall include all civil work required to install the unit, cement base and safety features Installation and civil foundations shall comply with the manufacturer's certified crash-tested configuration.

Retractable, hydro-electric bollards, K4

Level of protection	Barrier shall be certified to stop a vehicle of at least 6,800 kg at 50 km/h
Drive mechanism	Hydro-electric
Height above ground	700 – 800 mm
Foundation depth	1,300 - 1,600 mm
Finish	304 stainless steel
Safety features	Loop detector, arm barrier
Backup power	A backup power unit is required to allow the lowering of the bollard in case of a power failure
LED	Required, Led strip on top
Raise time	3–5 seconds
Lower time	3–5 seconds
Daily cycles	2500 minimum
Loop detection	The system shall include obstacle detection mechanisms to prevent raising under vehicles or pedestrians.
LED strips	Required

Drainage	The bollard foundation shall include a drainage system to prevent water accumulation within the casing.
Power supply	208-240 VAC, 3-Phase
MCBF	1,500,000 cycles
IP rating	IP 66
Operation temperature	-5 - 55 C
Safety compliance	EN ISO 13849:2015 or equivalent
Impact test standard certification	PAS 68, ASTM F2656-20, IWA 14-1
Bollard price shall include all civil work required to install the unit, cement base and safety features	

Arm barrier

Arm length	2.5 – 6 meters
Opening speed	Between 1.5 to 4 seconds. Adjustable. The arm drive system will include speed control and deceleration.
Cycles	Up to 10,000 cycles per day (according to manufacturer specifications)
Housing construction	Folded and welded sheet steel, from 2 to 6 mm thick, protected by cataphoresis and two coats of structured paint
Arm material	Aluminum or reinforced plastic, includes a skirt
Arm color	Varnished white with red reflecting stripes and end-sealing
Arm position	Right or left

C2: CBK - Official

Manual release	Manual release mechanism shall permit barrier operation during power failure
Safety	Photo-electric cell. The barrier shall automatically stop and reverse movement upon obstacle detection.
Loop detector integration	The system shall support loop detector integration
Reflective markings and LED illumination	Boom arm shall include reflective markings and LED illumination
MCBF	10,000,000 cycles
Indications	Open or closed, State of the presence detectors, Command for master-slave barriers (movement of one barrier controlled by the other barrier)
Access panels	Side door giving access to the mechanism, with security lock
IP rating	IP 44
Environmental protection	Internal mechanical elements treated by electro-galvanization
Motor	Electromechanical drive system suitable for intensive-duty operation
Surge protection	Surge protection shall be provided for power and control interfaces
Power supply	Single phase 230VAC, 50/60Hz + Ground
Operating temperature	-20 and +50°C
Relative humidity	95% non-condensing
Certification	The barrier shall comply with applicable CE and EN safety standards for powered vehicle barriers.

C2: CBK - Official

Price shall include all required anchoring, civil works, and installation accessories

Cantilever sliding gate

Height	2.5 meters
Length	According to lane length. Up to 6 meters
	Cantilever design (no ground track). Gate frame - made of structural steel, fully welded. Infill – made from solid sheets. The gate shall operate using heavy-duty cantilever roller assemblies designed for industrial use.
Surface treatment and paint	Hot-dip galvanized steel with powder-coated finish, painted in RAL color specified by the Client.
	Electric motor (HEAVY DUTY), minimum 1.5 HP. Includes a speed controller with clutch, which can be disengaged in the event of power failure. Includes friction clutch, drive gears, and rack-and-pinion mechanism.
Opening / closing speed	Gate speed not exceeding 0.4 m/s.
Safety features	The gate shall be equipped with internal and external photocell safety sensors and a flashing warning lamp for gate operation indication. All safety accessories shall be included in the scope of supply and included in the gate price.
Installation and foundation	Price of the Unit includes reinforced concrete pad with anchor bolts; electrical connections for motor, sensors, and control panel; alignment and levelling per manufacturer's instructions.
Wind-load conditions	The gate structure and drive system shall be designed to withstand local wind-load conditions.
Operational cycles	The gate operator shall support intensive-duty operation of at least 300 cycles per day

Emergency manual release	Manual emergency release shall permit gate operation during power failure
Gate price shall include all necessary civil engineering works for site preparation, ground levelling, construction of the gate foundation, and full adaptation of the gate to the fence opening.	

Gate control panel

Construction material	Brushed aluminium
Push buttons	DPDT push buttons. Each controlled element (gate or turnstile) shall be controlled from the Local Control Panel by two pushbuttons: one to open, the other to close the gate/turnstile
Number of push buttons	Quantities according to the number of manually controlled elements
Emergency button	Required. To release all elements in case of a safety emergency situation
LED Illumination	Buttons shall be LED illuminated. The light indication of the push button shall present the status of the gate (open or closed)
The control panel size and design shall be customized according to the customer's requirements.	

Anti-vehicle spikes

Retraction mechanism	Retractable spikes with spring retraction. Ground locking piston
Installation method	Surface-mounted – anchored with chemical anchors
Spike obstacle height	60 mm (height of the obstacle above ground)
Spike thickness	10 mm hardened spikes

Forced entry rated door, 5 minutes

Standard compliance	The door assembly shall provide a minimum forced entry resistance of 5 minutes when tested in accordance with ASTM F3038 or an equivalent resistance level certified to EN 1627 RC4 or higher or equivalent internationally recognized standard
Door type	Single or double-leaf steel or reinforced security door suitable for interior or exterior installation
Door construction	Heavy-gauge steel or reinforced composite panels Internal stiffening and anti-pry reinforcements Welded or bolted frame to prevent bypass
Frame construction	Reinforced steel frame or equivalent, securely anchored to wall or structure Designed to withstand ASTM F3038-14 forced entry tests or equivalent
Locking mechanism	Multi-point locking system with high-security deadbolts and strike plates
Hinges	Heavy-duty hinges with anti-removal pins or security studs
Finish / Surface	Powder-coated, epoxy-coated finish suitable for interior or exterior use
Corrosion resistance	External door assemblies shall be suitable for outdoor environments and provide corrosion resistance equivalent to ISO 12944 Category C3 or higher
Fire-resistance rating	Where required by local regulations, the door assembly shall maintain the required fire-resistance rating without compromising the forced-entry resistance classification
Glazing	Where glazing is incorporated, the glazing shall provide the same forced-entry resistance rating as the door assembly

Access control hardware	The door assembly shall support installation of access control hardware including electric locking devices, door position switches, request-to-exit devices, and access control readers
Accessories	Door seals, anti-pry strips, threshold plates, and mounting hardware included
Installation shall be performed in accordance with the manufacturer's certified installation requirements. The Contractor shall provide all anchoring, reinforcement, adjustment, alignment, and installation works necessary to maintain the certified resistance rating	

Forced entry rated grille, 5 minutes

The same requirements as for forced entry door

ELECTRONIC KEY MANAGEMENT SYSTEMS

Electronic physical keys management cabinet

Application	Secure storage, control, monitoring, and audit of physical keys
	System configuration: The Electronic Key Management System shall be configured by an authorized administrator. All keys shall be assigned unique electronic key tags and registered in the system database. User access rights, authorization levels, and time- based policies shall be defined via the management software.
	User identification and access Authorized users shall authenticate at the key cabinet using an approved identification method such as PIN code, proximity card, smart card, or biometric reader. Authentication may be performed locally or through the central management platform.
	Key authorization and validation Upon successful authentication, the system shall verify the user's authorization to access the requested key, including permissions, availability, and applicable time restrictions (Whether the user is authorized to take a specific key, Time and date restrictions, Key availability and current status).
	Key issuance Once authorization is confirmed, the cabinet door shall unlock and only the assigned key receptor is enabled and illuminated. The user shall remove the key, while all other keys remain secured. The system shall record the transaction automatically (User ID, Key ID, date and time, cabinet used).
	Key return procedure
	Upon completion of use, the key shall be returned to the designated key receptor. The system shall verify the key ID, secure it electronically, and update the transaction record with the return time.

	Monitoring and audit All key transactions are logged with user identity, key ID, date, time, and duration. Authorized personnel can monitor key status in real time and generate audit reports for operational review and compliance purposes.
Keys capacity	Up to 60 keys
Extension capability	Expandable with additional cabinets up to 150 keys
Cabinet type	Wall-mounted
Cabinet material	Powder-coated aluminum or polycarbonate or solid metal
User interface	Integrated touchscreen with graphical user interface
Authentication method	PIN code, proximity card, smart card, biometric (via external reader)
Key retention	Individually locked electronic key receptors
Key identification	Intelligent key tags with unique ID
Visual guidance	Tri-color LED indicators on key positions
Network interface	Ethernet TCP/IP (10/100 Mbps)
Audit & reporting	Full audit trail (user, key, date, time, duration)
User capacity	Supports up to 2,000 users
Alarm outputs	1 Dry-contact relay, Min
Locking options	Locking/non-locking
Battery backup	Required
Power supply	100–240 VAC input, 15 VDC output
Operating temperature	–5 °C to +40 °C
Operating humidity	Up to 95% non-condensing
Compliance	CE / UKCA / FCC / CSA

CYBER SECURITY

Introduction

Cyber Security systems shall be installed on the project's security systems and their IT environment. The Contractor must deliver a holistic, integrated Cyber Security solution for this environment.

The Contractor is responsible end-to-end for the implementation, operation, and maintenance of all cyber security systems.

Cyber security concept

The Cyber security concept is based on the principle of Defense in Depth, implementing multiple security layers at both the network and endpoint levels.

The Contractor shall be fully responsible for integrating security, control, and cyber security systems. This includes aligning all cyber systems to operate on the security IT infrastructure under a unified responsibility for deployment, operation, and maintenance.

All procured products must include full licensing, warranty, and service for at least two years post-handover. After this period, the Contractor shall renew all cyber licenses at their own expense within the maintenance contract framework, at no extra cost.

The Contractor is responsible for executing a detailed Low-Level Design (LLD) based on the existing High-Level Design (HLD). The LLD shall cover all cyber components and their integration with security systems and must be submitted as part of the Critical Design Review (CDR).

All systems must include full licensing for at least two years to cover the entire warranty period.

The Contractor is solely responsible for coordinating all project management and deployment workflows. This responsibility covers both the security systems implementation and their integration with the cyber security systems.

The security Contractor must employ dedicated cyber and IT infrastructure experts to support the project throughout its entire lifecycle—including implementation, integration, testing, handover, service, and maintenance. These experts may be internal staff or subcontractors under the contractor's sole responsibility. All associated costs shall be borne exclusively by the contractor for the duration of the project's establishment and subsequent maintenance periods.

The Contractor must provide all components and supporting IT infrastructure for the Cyber Security solution. This end-to-end scope includes procurement, detailed design, installation, configuration, licensing (and renewals), testing, and end-user training.

The Contractor is required to design a detailed network architecture that meets all performance, redundancy, and survivability metrics for bandwidth, latency, and QoS.

The Contractor shall design and deploy the cyber security systems in strict accordance with industry best practices for each system type. For the avoidance of doubt, the Contractor is solely responsible for optimizing all configurations and system hardening, as well as conducting comprehensive environmental testing to verify the absence of security vulnerabilities.

Procurement processes (Supply Chain Management - SCM)

The Contractor shall procure and supply all equipment in strict accordance with the Client’s detailed instructions and procurement guidelines.

The Contractor shall ensure that all procurement is sourced exclusively from reliable, authorized, and certified vendors.

The Contractor shall implement and maintain a strict control and supervision process for the secure transport and delivery of all equipment to the Client's sites.

Laboratory environment, test field, and integration

The Contractor shall establish and operate a comprehensive staging laboratory environment at their premises to demonstrate all supplied servers, network infrastructure, and cyber security components before site delivery. The Contractor is responsible for executing all necessary configurations, system hardening, and testing within this environment. Prior to field installation, all configurations must be presented to, and approved by, the consultants and the end Client. All costs for setting up and conducting these laboratory demonstrations are fully included in the Contractor's scope of work and must be factored into the initial financial proposal at no additional charge.

Within this staging laboratory environment, the Contractor shall perform full cross- system integration between the cyber security solutions, physical security systems, and control systems. This environment must fully replicate all project networks, servers, and cyber components, ensuring all end-to-end configurations and system interfaces are fully validated prior to on-site transport and installation.

The Contractor must present the complete laboratory environment, including all integrated security for the Client's approval. This presentation shall cover all specific configurations, system settings, and environmental tests executed by the Contractor.

The laboratory environment must be strictly isolated from all other networks. Connection to any external network requires prior written approval from the Client.

All materials, files, or media brought into the laboratory environment must be fully sanitized ("whitened") using a dedicated sanitization system.

Service – Active Directory (AD)

All Windows-based components must fully interface with the Active Directory (AD) server established under this project.

These services will provide the following capabilities:

a. Users and permissions management.

b. DNS services.

c. GPO management and settings.

d. NTP services – all security systems will connect to the NTP service for Windows- based applications and additional applications. The Contractor must design and plan a full and detailed solution based on these principles.

The Contractor is responsible for fully implementing the AD components. All Windows-based servers and endpoints must connect to the AD to receive central security policies and permissions via Group Policy Objects (GPOs). Furthermore, the Contractor shall configure user and group management at the AD level based on Role- Based Access Control (RBAC) principles.

The AD system must be implemented on a dedicated physical or virtual server using a redundant, high-availability configuration.

Management of access permissions will be based on the following principles:

a. Generic user accounts will be defined at different levels according to need and role.

b. Generic account at the controller/operator level – Operator.

c. Personal account for a chief manager (Security Officer) with extended capabilities for defining rules and configuration in the system.

d. ADMIN accounts with maximum permissions for technicians and those with permission at the highest level

The Contractor must fully integrate and operate this environment in strict accordance with the Client's requirements and all defined cyber security controls.

NOC system (Monitoring)

All endpoints will support and be defined accordingly by the Contractor to fully support the established NOC system so that infrastructural and application data can be read from them using relevant protocols SNMP V3, SSH, WMI (WINRM) and likewise will allow sending information in push to the NOC system in relevant protocols (SNMP V3, SYSLOG).

The Contractor shall deploy the monitoring system in full coordination and cooperation with all project stakeholders, ensuring seamless end-to-end operation in strict accordance with the Client's requirements.

Maintenance, security updates and license renewal – SLA

All procured products must include full licensing, warranty, and service for at least two years post-handover. After this period, the Contractor shall renew all cyber licenses at their own expense within the maintenance contract framework, at no extra cost to the Client.

The Contractor is responsible for performing all system updates—including security patches and major version upgrades—for all cyber systems, computing, and network infrastructures in compliance with SLA timelines.

Performance of security updates:

a. The Contractor will perform security updates and version updates for all computing and communication infrastructures and all cyber components.
b. All security updates will be checked in the laboratory environment prior to their installation in the operational environment.
c. Security updates defined as "critical" by the system manufacturer will be implemented in the environment within 14 days at most.
d. Updates at medium, low urgency level – once every half year.
e. In any case, the updates will be performed in coordination with the facility's

f. Security Officer representative and in full coordination with him.
g. The updates will be performed in accordance with the update procedure provided by the client.

Renewal of licenses for all cyber systems for security and the IT environment

a. The Contractor shall execute, exclusively at their own expense, all necessary license renewals across all project components, including but not limited to: physical security systems, cyber security and control solutions, and all underlying IT computing and communication infrastructures.
b. The license renewal will be performed in coordination with the client's representatives.
c. The license renewal will be at the contractor's expense within the framework of service and maintenance payments.
d. The license renewal will be performed before the existing license has ended.

Updates for Endpoint Security (EPS):

a. Likewise, the Contractor commits to perform version updates as required for the EPS system once a quarter within the framework of the service and maintenance contract, and in any case, the Contractor will perform a check prior to the update to verify that the update does not affect the system function.
b. Signature updates of the EPS system will be performed in coordination with the client's representatives.
c. The Contractor will perform an update for the EPS systems at a frequency of once a quarter within the framework of service and maintenance and every time files are brought into the environment.

Data communication protection

The Contractor will provide and design the system components so they can be verified by a Network Access Control (NAC) system through support in the following protocols:

a. SNMP v3.
b. SSH v2.
c. 802.1x.

Any other standard secured protocol provided receives approval from the developer's cyber designer and the client's representative.

Network separation principles

The security network shall be a separate network from any other network in the facility.

The network must be divided, according to its complexity and the processes it serves, into zones and sub-networks (segments) based on criteria such as the functional role of the components, user types, their geographical location, affiliation to a certain system, and affiliation to a certain environment.

Traffic filtering and control between the various segments (using Firewalls) must be activated. The authorized protocols, ports, services, and software must be defined – and traffic allowed only for them.

The security network will contain separated VLANs according to the principles of this technical specification:

a. Servers VLAN – which will concentrate the Domain Controller (DC), NOC, and the backup server.
b. PSIM VLAN – which will concentrate the security PSIM system servers.
c. Access control VLAN – which will concentrate the access control system servers.

d. DB VLAN – which will concentrate the Database (DB) servers.
e. ESX & Storage – which will concentrate the central Virtualization (ESX) and Storage servers.
f. Management VLAN – which will concentrate the management interfaces of the virtual environment, the switches management environment, and additional systems requiring management.

It shall be clarified that it is the Contractor responsibility to perform a detailed design at the LLD level and define all the sub-network ranges, segmentation, and micro- segmentation according to the manner and function of the security array and also according to Best Practice.

The Contractor will have to present the detailed design within the framework of the CDR.

The Contractor shall implement Firewall (FW) components to act as the gateway for all VLAN networks. These firewalls must be installed in a high-availability cluster configuration. The Contractor is responsible for seamlessly integrating the FW components with the security environment, ensuring zero negative impact on the performance and functionality of the security systems.

System hardening principles

The Contractor is required to perform strict system hardening on all endpoints, IT components, and network infrastructures. This encompasses all physical security systems, network switches, virtual environments, computers, and servers.

Operating systems and systems under the Microsoft platform (or any other operating system integrated into the solution) will be hardened according to the manufacturer's definitions and in accordance with the best practice defined by the manufacturer.

The Contractor shall submit detailed hardening procedure documents for each component type for the Client's approval. Each document must fully describe the hardening actions to be performed and their execution method. Additionally, the Contractor shall explicitly cite the manufacturer best practices or industry standards used as a baseline, including active webpage links to the original source documentation.

Following the Client's approval of the hardening methodology, the Contractor must implement the hardening configurations across all components. The Contractor is required to factor all necessary manpower and multi-disciplinary labor resources into their initial financial proposal.

Components without manufacturer support (End of Life - EOL, End of Service - EOS) must not be installed.

Users/processes/applications must be prevented from bypassing the Cyber Security systems and connecting directly to central components.

25.10.7. Default accounts must be deleted/neutralized globally.

All system components must be hardened to reduce the attack surface.

Principles of switches hardening and network settings

The Contractor shall perform comprehensive global hardening across all network switches, in strict accordance with the manufacturers' official best practices and the guidelines provided by the Client’s cyber security experts.

As part of this switch hardening process, the Contractor is specifically required to execute the following security configurations for all switch ports:

a. Restricting port access to a maximum of one MAC address per port.
b. Setting the specific MAC of that endpoint device as the only MAC authorized for connection in this Port.
c. Setting the Port as access and not dynamic (will block connection of an additional switch or anything different from an endpoint).
d. Setting "Disable" to a cold port that is not in use. It must be verified that all interfaces not in use will be in a neutralized state.
e. Performing additional settings for hardening and optimization of the network according to best practice.

Principles of computer stations and endpoints hardening

The Contractor shall disable all unused or unnecessary applications, features, and operating system services.

The Contractor shall block all USB ports and external media interfaces across all endpoints, unless explicitly authorized in writing by the Client.
The Contractor shall restrict all endpoints from creating or enabling local privileged (administrator) accounts. All user and access management shall be administered exclusively via the central domain controller

The Contractor shall perform strict hardware-level hardening by disabling all unrequired BIOS/UEFI components—including Wi-Fi and Bluetooth interfaces—and securing the BIOS/UEFI with a strong, complex password.

The Contractor shall disable automatic internet-based update mechanisms on all endpoints. All software updates and patches must be deployed proactively from a designated central patch management server.

The Contractor shall restrict and block the execution of network mapping, discovery, and reconnaissance commands on all endpoint stations.

Central Cyber Incident Management System

The Contractor must provide a central, holistic All-In-One cyber incident management system. This system will monitor the security and building control environments in an Out-of-Band (OOB) configuration.

The solution shall utilize an approved, high-tier specialized security monitoring platform that complies with the detailed technical specifications outlined later in this chapter.

The system will contain all the following capabilities:

a. Environment monitoring and Auto Discovery capabilities.
b. Configuration freeze capabilities.

The system will interface with the central Cyber Control Center to send all indications to the control center.

Lifecycle vulnerability management (CVE) for IoT/OT assets

The Cyber Management System shall deliver continuous, automated vulnerability intelligence for all connected IoT and OT assets, including but not limited to cameras, controllers, radars, and network switches.

The system shall serve as the central repository for identifying known security flaws and vulnerabilities. To ensure operational continuity, this capability must be achieved exclusively through passive monitoring, strictly prohibiting active scanning that could disrupt sensitive OT operations.

Automated CVE correlation:

a. Continuous Monitoring: The system shall maintain a synchronized local database updated against global vulnerability repositories (e.g., NIST National Vulnerability Database - NVD).
b. Passive Identification: The system must automatically correlate the identified Model, Manufacturer, and Firmware version of every asset against current CVE records. This process must be entirely passive to ensure zero impact on the security system's performance and stability.
c. Zero-Day Awareness: The system shall provide immediate alerts when new CVEs are published that affect any component currently active in the project's network.

Risk scoring and categorization (CVSS):

a. Severity Rating: Each identified vulnerability must be presented with its CVSS (Common Vulnerability Scoring System) score, categorizing risks into Critical, High, Medium, and Low.
b. Asset Criticality Mapping: The system shall allow the administrator to define "Critical Assets" (e.g., the Main Radar or the Server Room Access Controller). If a CVE is detected on a critical asset, the alert priority shall be automatically escalated regardless of the base CVSS score.

Remediation and mitigation workflow:

a. Patch Advisory: For every identified CVE, the system must provide a technical summary and, where available, a link to the manufacturer’s firmware update or recommended mitigation steps (e.g., closing specific ports or disabling services).
b. Integrated Response: In the event of a "Critical" CVE (Score 9.0+) detected on a high-risk device, the system shall provide the Security Officer with an immediate option to isolate the device through the NAC/Firewall integration until a patch is applied.

Compliance and reporting

The system shall generate a monthly "Risk Posture Report" listing all unresolved CVEs in the system, sorted by age, severity, and physical location (Switch/Port).

The system must allow the Security Officer to "Acknowledge" or "Mitigate" specific CVE alerts, while maintaining a full audit trail of the decision-making process for compliance purposes.

Sanitization station

Within the framework of the project, the Contractor shall deploy a Stand-Alone data sanitization ("whitening") station to ensure the secure transfer of files into the operational network. Unsecured data transfer into the security network shall be strictly prohibited.

All data sanitization activities shall be coordinated with and authorized by the Client. The Contractor shall submit all files required for sanitization to the Client's Security Officer or designated representatives through a centralized, fully documented process.

Following a successful scanning and testing process, this station shall serve as the exclusive point of entry for all external data entering the secured networks.

The data sanitization process shall be executed exclusively via a dedicated maintenance laptop or a dedicated maintenance storage device, featuring one-to-one identification, both to be provided by the Contractor.

Endpoint security system

The Contractor shall install, operate, and maintain a centrally managed Endpoint Protection (EPS) and EDR/XDR system optimized for closed environments. This solution must include a central management server in the virtual environment and all licenses required to support full defense capabilities. The system must provide a unified interface to block viruses, spyware, and malicious code; perform traffic and behavioral anomaly detection using machine learning; and enforce application whitelisting. Additionally, the Contractor is responsible for deploying Host-based Firewalls (PFW) and Device Control policies across all servers and computers.

During the installation and configuration of all operating systems, the Contractor must implement strict hardening settings using the following system capabilities:

a. Performing configuration and setting for the EPS system in all computer stations and servers and adapting to the server station and the systems installed on the station/server including coordination with the manufacturer of the installed systems to perform all the necessary adjustments and exclusions to allow the software to work without interference.
b. Implementation of a Host-based Firewall (PFW) solution on endpoints through configuration and setting infrastructure of PFW in all endpoints and servers while allowing required traffic only and blocking any other traffic.
c. Implementation of an EDR solution – for discovering exceptional behavior and anomalies and blocking them. The solution will be full and comprehensive and will contain the ability to identify suspicious behaviors, heuristics, and include built-in analysis and diagnostic capabilities.
d. Implementation of the solution will allow implementing an Application Control solution enforcing execution for applications on the computer by defining which applications are authorized to be activated on the station/server – including advanced Whitelisting capabilities that will allow a learning mode. Including the ability to define authorized applications and also including the ability to give temporary flexibility when performing changes by authorized technicians only.
e. The system will include capabilities for learning the existing permitted state, the running systems, the protocols, and the like – and afterwards will allow configuration freeze. All this without harming the security systems' capabilities and allowing maintenance provision. The bidder must perform the configuration while full coordination between all the systems for performing this capability without harming the system function.

Intrusion Detection Systems (IDS)

The Contractor shall procure, install, and deploy a centralized Network Intrusion Detection System (NIDS) designed to continuously monitor and detect network anomalies.

The Contractor shall execute all necessary settings, configurations, and baseline tuning required to optimize the IDS performance and minimize false positive alerts.

NAC System (Network Access Control)

The Contractor shall provide and install a central NAC system as part of the overall Cyber Security package delivered for the project.

Contractor is responsible for the full integration of this system. This includes connecting all endpoints and computing assets to the NAC platform in compliance with these technical specifications.

Hardened technician computers

The Contractor shall procure dedicated technician laptops for the exclusive use of all technicians and system integrators.

These technician laptops shall remain strictly on-site and shall not be utilized for any purpose other than the deployment and maintenance of the project's security systems.

All technician laptops shall undergo comprehensive system hardening in strict accordance with the requirements outlined in this specification.

The Contractor shall install all software, tools, and applications required for the deployment and maintenance phases onto these laptops, encompassing all necessary and valid licenses.
The Contractor’s personnel shall operate in strict compliance with the Client's operational procedures. The use of personal computers, unapproved corporate laptops, or personal USB storage devices is strictly prohibited.

Technical specification – EDR

The Contractor shall supply, install, and maintain a central EPS/EDR system optimized for closed environments. The delivered solution shall include all licensing required to execute the following core security capabilities:

a. Central management interface.
b. Ability to block and neutralize viruses, spyware, and any type of malicious code.
c. Traffic and file identification ability.
d. Capabilities for monitoring unauthorized AD queries and blocking users.
e. Application Isolation capabilities and execution in a protected area in memory while blocking dangerous behaviors.
f. EDR capabilities for recording and identifying behavior and anomalies.
g. Advanced Application Control capabilities, advanced automatic learning capabilities, and Whitelisting capabilities.
h. Device Control capabilities.
i. Host-based Firewall (PFW) capabilities.
j. Virtual patching capabilities for defense against known vulnerabilities.
k. Blocking of unauthorized PowerShell executions.

The Contractor shall install all system components and procure all required licenses in strict accordance with the Client’s and designer's specifications. The delivered solution must be comprehensive, providing full capabilities across identification, protection, detection, response, analysis, and recovery frameworks.

The supplied solution must be fully optimized for disconnected/air-gapped environments and seamlessly adapted to the operational nature of the security systems, network infrastructure, and computing environment.

The Contractor shall deliver and deploy a comprehensive endpoint security suite across all workstations and servers within the security environment. This system must feature unified central management and provide robust protection against malware, advanced threats, and anomalous or malicious network traffic.

The system will be defined to send the reports and alerts to the central cyber management system. The bidder will perform all required system settings for sending reports/logs in any configuration required according to the needs of the central cyber incident collection system.

The system will include a managed device blocking mechanism for USB, CD, and other devices (Device Control).

The system will have capabilities for identifying and neutralizing viruses, worms, spyware, adware, Rootkits, Trojan horses, and additional attack capabilities while minimal dependence on signature updates and reliance on unauthorized behavior, anomalies, and heuristics or using Whitelisting will harden the environment and prevent execution of unknown or unauthorized files.
The system will have the ability to identify suspicious traffic and files based on signature engines.

Performing settings and configuration in the EPS system in all computer stations - Microsoft Windows and Linux-based servers:

a. Performing configuration and setting of all EPS system components in all computer stations and servers and adapting the configuration and required exclusions to applications running on the same computer/server so that there is no harm to the security systems' function running on the same computer/server. The Contractor will perform the configuration according to the Best practice recommendations by the manufacturers of applications existing on the server/workstation. The Contractor will submit a Procedure document describing the manner of defining the component.
b. Implementation of EDR solution – the solution will monitor the server/computer and discover suspicious global actions and will serve as a tool for identifying exceptional behavior and breaches including immediate response, investigation, and treatment of security incidents while minimal dependence on signature updates and reliance on unauthorized behavior, anomalies, and heuristics.
c. Implementation of Device Control solution – allows blocking and managing interfaces in computers and servers.
d. Implementation of Host-based Firewall (PFW) on endpoints – setting and configuration of PFW in all endpoints and servers as part of performing the station hardenings. Including hardening the IP address space to which the station/server is permitted to approach in the security network. The Contractor will submit the hardening configuration setting for the client's approval.

Performing signature update and version update for the EPS system:

a. Within the framework of the warranty and service and maintenance contract, the Contractor commits to performing signature updates for the EPS systems in all computers and stations once a quarter.
b. Likewise, the Contractor commits to performing version updates for the EPS system once every half year, and every time before new files are brought into the environment (for any reason).

Content Disarm and Reconstruction

The Contractor shall supply and install a complete standalone CDR (Content Disarm and Reconstruction) kiosk solution, including all required hardware, software, and licenses. The system must feature an independent kiosk terminal and all necessary peripheral equipment to ensure optimal deployment. The solution shall actively scan all external files to identify and eliminate malicious code prior to their entry into the security environment.

The deployed solution shall enable the secure and verified transfer of digital files and information from external sources into the project environment.

The system must operate in a strictly isolated, air-gapped standalone configuration, with zero network connectivity to the secure ("clean") network. Sanitized files shall be transferred exclusively via approved, dedicated USB drives or serialized, marked CD media directly to the designated entry station within the secure network.

The system will support scanning of at least 5 scan engines.
The system will have format conversion capability.
The system will have the ability to identify suspicious heuristics using the AV engines.

In cases where an executable code package cannot be deconstructed or processed by the CDR system, the Contractor shall obtain an official cryptographic HASH signature (checksum) directly from the software manufacturer to verify the source and integrity of the package. This HASH signature must be validated and matched prior to introducing any files into the network. Following successful integrity verification, the files may be imported and must immediately undergo a comprehensive scan utilizing the central Endpoint Protection (EPS) system.
The system needs to be with the ability to identify hidden threats in documents.

The system will have the ability to identify and block all types of files identified in cases where their extension was changed and does not match the file content: for example, inf, com, bat, exe.
The system will have the ability to identify, scan, and remove METADATA from documents.
The system will have the ability to support blocking files with unknown extensions.
The system will allow defining Blacklist, Whitelist for file types.
Ability to support whitening files in large volumes, scanning 100 Mb of flat files in less than 25 seconds.
Support for checking media over 2 TB according to operating system limitations.
Ability to identify known threats while using Hash comparison without sending content.
Ability to check signatures versus historical signatures and scan the required difference.
The Contractor must include in his proposal all the configuration and integration works required for perfect operation.

Technical specification – Firewall

The Contractor shall procure, install, and configure a Next-Generation Firewall (NGFW) solution to facilitate secure traffic routing between distinct networks, with a dedicated emphasis on deep traffic analysis tailored for production environments.

The NGFW components shall be deployed and configured in a High-Availability (HA) cluster configuration, ensuring full hardware redundancy and seamless failover.

The Contractor shall enable strict traffic filtering and access control between all network segments. Firewall rules must explicitly define authorized protocols, ports, services, and applications, enforcing a default-deny posture where only explicitly approved traffic is permitted.

The facility's communication network is segmented into multiple sub-networks (VLANs). The NGFW components shall monitor, inspect, and control all inter-VLAN traffic, permitting only authorized traffic that strictly complies with the approved security policy.

The Contractor shall provide comprehensive documentation of all firewall security policies and configure automated backups of all policies and system configurations to the central backup server.

The Contractor shall deliver a centralized management system through which all firewall policies, rules, and configurations shall be monitored, managed, and enforced.

Including CPU expansions + at least 16GB RAM + SSD as required for operation for Real-Time systems.

The component will contain a storage volume providing logs saving for at least 3 months.

Including two power supplies for backup.

Installation of the FW in a Cluster configuration.

The Contractor must provide an FW system adapted to the maximum expected traffic volumes while using all the product's defense engines + at least 20% reserve.

Including supply, configuration, and optimization of the NGFW policy and the Intrusion Prevention (IPS) engine.

Including at least two years support and warranty and full warranty and service within the maintenance contract.
Including upgrading the FW to a new model every 5 years without additional payment.

Such as approved high-end NGFW solutions (e.g., equivalent to top-tier enterprise firewalls).
Establishment and configuration of a secure and encrypted VPN connection using the NGFW component.

Configuration and policy optimization of the FW components, policy and security settings:

a. The Contractor will perform all settings fully according to Best practice for all engines at all levels including testing processes, separation between networks, and configuration optimization.
b. Basic definition: "Block by default" which will prevent any traffic except that which will be approved in the policy.
c. Mapping of all IP addresses, VLAN networks, the Ports in use, the protocols, and traffic required for all security systems.
d. Creating Access Control Lists (ACLs) allowing only and solely the traffic required for full activity.
e. Full documentation of the performed settings.
f. Firmware updates of the manufacturer must be performed within the framework of the maintenance contract.

Management software for NGFW components:

a. The system will include at least 100 log backup days.
b. The system will be able to manage up to 5 devices.
c. The system will fully support installation on a virtual environment.

Dedicated analysis and report generation software for NGFW components:

a. Supply, installation, and configuration of central analysis and report generation software installed as a VM.
b. Central Single-console management system.
c. Ability to identify and present threats in a friendly user interface.

Monitoring system for IT infrastructures (NOC)

a. Supply, installation, and configuration of an IT infrastructures monitoring system, including all licenses for managing network devices (switches), servers, traffic, CPU/memory loads, applications, and services.
b. The software will alert any failures and provide a full status picture.
c. History of events/reports saving and report generation.
d. Monitoring systems: Servers, virtual infrastructures, Switches, Databases, and Cyber components (FW etc.).
e. Such as approved high-end network monitoring tools.

Secure Gateway components
a. Central encryption solution providing secured encrypted communication in a Zero trust configuration.
b. Bi-directional communication in real-time with extremely low Latency.

Training and documentation

The Contractor shall deliver comprehensive training for users and management teams.
The Contractor shall provide training booklets and operating instructions for each component.
Documentation:
a. Creation of a facility file and As-Made plans, including architecture plans and configuration freeze.
b. Detailed documentation down to the single component level and connectivity.
c. Renewal of licenses for cyber security systems
Renewal of licenses for all components at the contractor's expense for the entire warranty period (24 months) and the maintenance period.

All systems shall be supplied with a full license for at least two years.

FW components will be upgraded to a new model every 5 years without additional payment.

GENERAL TECHNICAL SPECIFICATIONS

General

This section defines the general technical requirements for the equipment to be supplied and the works to be executed by the Contractor within the framework of this Project.

The list of requirements detailed in this section represents, from the Client’s perspective, the minimum level of compliance required of the systems, equipment, and works, in order to establish a system that meets the Client’s desired standards of quality and performance.

All equipment and materials supplied by the Contractor under the scope of the Project shall be new, original, of high quality, and suitable for the operation of the system under the climatic and environmental conditions at the installation site
Items, components, or works not specifically mentioned in this specification or shown in the drawings, but required by relevant standards, codes, or accepted professional practices, shall be supplied and installed by the Contractor as an integral part of the works, at no additional cost to the Client.

In the event of any conflict between the General Technical Specification and the Specific Technical Specification of a particular system, the Specific Technical Specification shall prevail.

All equipment, systems, and works shall be supplied and installed in accordance with the relevant international and local standards, including, but not limited to, IEC, ISO, UL, and mandatory local standards.
The Contractor shall ensure that all installations are carried out in accordance with the manufacturer's instructions and in compliance with accepted safety practices.

All system components shall be clearly labeled and documented in "As-Built" drawings upon completion of the installation.

The Contractor shall provide certificates of compliance and warranties for all equipment and materials supplied.

Installation of equipment & systems

In all cases, unless explicitly stated otherwise, the installation work shall include all planning, fabrication, and installation activities, including the supply of all required installation accessories, cable routing, wiring, testing, commissioning, and any other actions necessary to bring each equipment item into full and proper operation in accordance with its technical specifications.

All equipment items, materials, installation accessories, and other system components supplied by the Contractor shall comply with the relevant standards and requirements of the local Standards Institute, local Electric Corporation, Ministry of Communications, and Fire & Rescue Authority.

Any damage or alteration caused by the Contractor during the Project to the existing infrastructure (walls, doors, windows, piping, electrical installations, architectural finishes such as paint, plaster, coatings, etc.) shall be immediately repaired by the Contractor at no cost to the Client.

The Contractor shall provide, as part of the installation, all auxiliary accessories - even if not explicitly listed in the specification - that are required for the completion of the Project as defined in the specification.

To avoid any doubt, it is emphasized to the Contractor that the installation of every equipment item, whether explicitly mentioned in this specification or not mentioned but essential for the operation of the required system, shall always include the following activities:

a. Procurement of equipment and systems.
b. Packing, transportation, and delivery of equipment to the site.
b. Physical installation of the equipment: placement and securing of the equipment in position; supply and installation of all mechanical components and reinforcement accessories required - even if not separately listed in this specification - and all other items necessary to complete the mechanical installation works.
c. Electrical installation:

- Supply and installation of all power cables required for the operation of the equipment, from the Client's main electrical panel to all end units of the system. It is the Client's responsibility to provide only the connection point at the electrical panel; all other works shall be the responsibility of the Contractor.

- Supply and installation of all grounding cables, connected at one end to the equipment and at the other end to grounding points or the main grounding rod.

- Execution of all wiring works, including the supply and installation of all interconnection and bridging cables with connectors at their ends, connections between different types of equipment, laying of cables in conduits or fastening to cable trays, bundling, labeling of cable ends, connection and wiring within junction boxes, equipment cabinets,

control desks, and marking of cables - until full integration of all components into a fully operational system.

Mechanical installation:

a. Mechanical works, including installation of piping and cable trays, drilling in concrete walls or gypsum partitions, mechanical reinforcement of equipment to walls, floors, or ceilings, supply and installation of mechanical accessories required for the installation, and any other works not explicitly mentioned in this specification but necessary to complete the installation.

b. Finishing works, including paint touch-ups, repair of any damages, mechanical reinforcements, sealing of holes and cable passages, cleaning, and all other actions required to restore the installation to its original condition.

Future expansion

The system shall support future expansion to an unlimited number of sites and end devices, without requiring changes to its topology or the addition of any software components (excluding the necessary licenses).

Software and licenses

The Contractor shall be obligated to upgrade and update, at no additional cost to the Client, all software versions supplied under the Project throughout the entire warranty period and within the framework of the maintenance contract to be signed with the Contractor.

The Contractor shall not charge any additional fees for renewing licenses for software or hardware items during the warranty period and within the framework of the maintenance contract to be signed with the Contractor.
License costs shall be included in the prices of the software and hardware.

General environmental compliance requirements

Unless otherwise specified in the specific technical specification of an equipment item, the following environmental compliance requirements shall apply to the equipment:

Outdoor equipment	The equipment shall be capable of withstanding wind speeds of at least 100 km/h without degradation of performance or structural damage.
	Operating temperature: The equipment shall operate reliably within a temperature range of –10°C to +55°C.
	Relative humidity: The equipment shall be capable of continuous operation at a relative humidity of up to 95% (non-condensing).
Indoor equipment	Operating temperature: The equipment shall operate reliably within a temperature range of –0°C to +40°C.
	Relative humidity: The equipment shall be capable of continuous operation at a relative humidity of up to 95% (non-condensing).

Electricity

The equipment supplied by the Contractor shall operate from a main power supply of 230 VAC ±10%, 50 Hz ±5%.

The above-mentioned power supply shall be provided to the Contractor from the existing electrical panels of the Client. The Contractor shall, through a qualified electrician under its responsibility, install power supply lines from these panels to the system components. Each power supply line must be approved by the Client.

The installation of the required power supply to the system, connection to the electrical panels, provision of accessories, and all related works shall be carried out by the Contractor in accordance with the rules and procedures defined by the Client. The Client shall provide these rules prior to the installation phase. All work shall be performed exclusively by a certified electrician employed by the Contractor at the Contractor's cost.

The equipment supplied by the Contractor shall operate at the above-defined voltage and/or through AC/DC power supplies provided by the Contractor as an integral part of the equipment, with operating voltages as defined in this specification. The cost of these power supplies shall always be included in the equipment price.

The Contractor shall ensure that all electrical works are executed in full compliance with local laws and regulations, and in accordance with recognized international standards.

Protection

Equipment and systems shall be protected against overvoltage, transient voltages, reverse polarity connections, and electromagnetic interference, as detailed below:

a. Protection against reverse polarity shall be provided by electronic means.
b. The equipment shall withstand transient voltages of 250 V for 50 milliseconds.

Grounding (Earthing)

All outdoor communication cabinets, indoor communication cabinets, and equipment racks shall be properly grounded by the Contractor in accordance with applicable standards.
The resistance of grounding connections to the main grounding point shall not exceed 0.1 Ω.

Reliability and maintainability

The system shall meet the following reliability requirements throughout its entire operational life:
a. MTBF (Mean Time Between Failures) – entire system: at least 10,000 hours.
b. MTBF – individual equipment item: at least 20,000 hours, except for items for which this specification defines a different MTBF.

The required operational life for the complete system and for each individual component shall be at least 7 years. During this period, continuous operational performance shall be ensured without degradation of system performance specifications, provided that maintenance is carried out in accordance with the manufacturer's instructions.

All system components shall be fully interchangeable as Plug-In Units, both as individual parts and as complete assemblies, to meet the specified MTTR (Mean Time To Repair) requirements.

General mechanical requirements

All equipment intended for outdoor installation shall undergo a finishing process that provides corrosion resistance suitable for exposed installation in the site's climate for a minimum of 7 years.

All fasteners and connection materials shall be treated for rust and corrosion protection.
All outdoor equipment shall be weatherproof, with enclosures sealed against moisture, water, dust, and sand, providing protection level of at least IP65.
All external bolts and screws shall be galvanized or made from stainless steel.

Marking and labelling

All equipment installed at the Client's sites shall be labeled and marked in accordance with the Client's instructions, definitions, and procedures.

Every end unit, control unit, and display unit in the system shall be clearly marked in English, clearly indicating its purpose and operation.
Cable labeling shall be carried out as follows:

a. Each cable or conductor shall be individually labeled at both ends with a permanent marking that is resistant to fading or wear, indicating its function and type. Marking may be applied by printing, embossing, engraving, or heat-shrink sleeves.

b. In all cases of wall penetration, cables shall be labeled on both sides of the penetration.

The labeling and marking shall be clear and functional, enabling easy identification of system components in accordance with the drawings and plans.

The quality of labeling shall ensure durability under normal use. Marking and labels shall be resistant to abrasion, gasoline, oils, and external weather conditions.

Galvanization

Wherever galvanization is specified, hot-dip galvanization shall be applied in accordance with EN ISO 1461 or ASTM A123 / A123M, ASTM A153 / A153M or equivalent local standard in country of installation.

Conduits / Piping

26.13.1. A pull string shall be installed inside every conduit, secured at both ends.

For all building or pit penetrations, conduits shall be routed through a properly sized core-drilled hole. The joint between the conduit and the pit/wall shall be sealed with a suitable rubber gasket and polyethylene to prevent ingress of insects.

Connection of conduit sections shall be made using fittings suitable for the type of conduit and intended purpose. Wall-mounted conduits shall be supported with galvanized metal clamps ("straps") at intervals of at least 0.3 m, or as required based on conduit weight. At every conduit corner, a clamp shall be installed 15 cm from the corner in each direction.

Connection of cable tray sections or closure at ends shall be made using appropriate tray connection units. Wall-mounted trays shall be fixed with stainless steel screws and suitable wall plugs at intervals of at least 0.3 m, or according to the tray weight. At every tray corner, screws shall be installed 15 cm from the corner in each direction.

At the entry of conduits into an existing building, a CI4 service box of dimensions 80 × 175 × 225 mm shall be installed on the interior wall. Conduits shall be connected to this box, and cable entry shall be made by drilling a hole through the wall. Conduits shall be enclosed with a 3 mm thick metal cover on the sides and top.

MAINTENANCE SERVICE

General

At the end of the warranty period, the Client shall be entitled to request full maintenance services for the system from the Contractor.

The maintenance services shall cover all components of the system supplied by the contractor, as well as any security equipment or systems installed at the client's site that were supplied by other contractors and remain operational.

During the service contract period, the Contractor shall be responsible for the quality of the work performed and for the quality of all materials and equipment included therein. Without limiting the generality of the foregoing, the Contractor shall be responsible for the proper functioning, integrity, durability, suitability for its intended purpose, performance, output, and quality of the work performed, of the system as a whole, and of each individual component.

Every system inspection or repair during this period shall be accompanied by a report submitted by the Contractor to the Client, detailing all inspections, adjustments, and repairs carried out by the Contractor.

The maintenance required by the Client is global maintenance (TOTAL RISK), meaning a complete set of works and supply of equipment for all system components to ensure continuous and proper operation of the entire system to the full satisfaction of the Client.

Days for performing maintenance works shall be spread over all days of the week except Sundays and holidays, during the standard working hours of the Client.

For the avoidance of doubt, the maintenance required from the Contractor at any stage shall include at least the following tasks:

a. Repair of faults and malfunctions.
b. Supply of replacement equipment, including units and assemblies, electronic cards, spare parts, components, cables, connectors, and consumables.
b. Software maintenance and updates.
c. Continuous reporting to the Client on the execution of maintenance.
d. Preparation and submission to the Client of statistical maintenance reports.
e. Participation in meetings, as required by the Client to discuss various maintenance- related topics.
f. Everything necessary to ensure continuous and proper operation of the system to the full satisfaction of the client.

Maintenance of the system shall include the following services:

a. Preventive maintenance.
b. Repair of faults and malfunctions.
c. Software maintenance and update.

Preventive maintenance

Preventive maintenance shall include the following services:
a. Semi-annual system inspection.
b. Routine system calibration.
c. Preventive maintenance of system components according to the manufacturer's instructions.
d. Cleaning of cameras.
e. Synchronization of clocks for summer or winter time.
f. Review of log files of all systems.
g. Database maintenance (indexes, archives, backups, etc.).

For the avoidance of doubt, all maintenance activities by the Contractor shall be carried out in accordance manufacturer's requirements, which shall govern the preventive maintenance procedures.
Semi-Annual Inspection:

a. Every six months, the Contractor shall perform a comprehensive inspection of all system components. The "semi-annual inspection" shall include the following tasks:
b. Checking communication integrity.
c. Software updates.
d. Verification of operational and functional performance of all software in the system.
e. Repair or replacement of any defective components.
f. General cleaning of equipment from dust and dirt, including cabinets.
g. Adjustment and cleaning camera lenses.
h. Backup of databases, servers, system configurations, and all other critical system information onto physical media, and providing the media to the Client.
i. Any additional actions required to ensure uninterrupted system operation without performance degradation.
j. Inspection dates shall be coordinated with the Client and will be carry out under the Client's supervision.
k. Periodic inspections and their results shall be recorded in special forms agreed upon between the Contractor and the Client.
l. The results of the inspection and corrective measures taken shall be reported to the Client on the forms mentioned above, no later than 7 days after the inspection.
m. A copy of the inspection form shall be left with the facility's chief security officer.

Fault and malfunctions repair

Any system component found to be defective shall be immediately repaired or replaced.
Fault repair shall be performed in accordance with the mandatory response times specified in the Service Level Agreement (SLA).
Any component that fails and is repaired three times within a single maintenance year shall be replaced with a new one.

Software maintenance

As part of software maintenance, the Contractor shall perform the following actions:

a. Immediate and complete correction of any bugs detected during operation in any installed software of the system.
b. Reloading software and system restart in the event of software-related system failure; replacement if necessary.
c. Supply, reloading, and activation of updates and/or new versions of operating systems, infrastructure software, and all software covered by this specification. Operating systems shall be updated at least monthly for critical security updates, and every two months at most for other updates.
d. Replacement of any software that has reached its End-of-Life with equivalent or superior software.
e. Database and/or system configuration changes according to the Client's requirements.
f. Full database maintenance, including indexing and verification of data integrity and correctness.
g. Operating system updates according to the support provided by the developing company.
h. Software testing using diagnostic programs and simulations.
i. Full backup of all systems onto removable media every 6 months.

During the maintenance period, the Contractor shall bear the costs of renewing licenses for any relevant software, if required.
The Contractor shall establish a testing environment at its offices or at the Client site. All software updates or upgrades shall first be performed in the testing environment before deployment to the operational system. The Contractor shall bear all costs for establishing and maintaining the testing environment.

In cases where software failures cause system configuration issues or data loss, the Contractor shall, at its own expense, restore the database and rebuild the system configuration.

During the semi-annual inspection, the Contractor shall scan hard disks, clean corrupted fields, optimize memory, and, with the Client's approval, delete irrelevant information from the system.

With every software change - whether due to bug fixes, Contractor initiative, or Client request - the Contractor shall immediately update the technical documentation of the software held by the Client.

Installation files, licenses of all software installed in the system, database backups, and technical software documentation shall be delivered by the Contractor to the Client.

Response time for service calls

27.5.1. "Response Time" shall mean the elapsed time from the moment the Contractor receives a service notification at its service center, or from the moment the Contractor becomes aware of a system fault, whichever occurs first, until the Contractor's service technician arrives at the facility.

The required response time for a non-critical fault shall be within 48 hours from the receipt of the service call. Non-critical faults shall be repaired during the Client's regular working hours (08:00 – 17:00).
The response time for a critical fault shall be within 9 hours from the receipt of the service call.
A critical fault is defined as one or more of the following:

a. A critical failure or crash of the Physical Security Information Management (PSIM) system.
b. A bug in any of the software installed on a system component.

c. A fault in the CCTV system (20% or more of cameras at the site are inoperable).
d. A fault in the video management system (30% of cameras are not recording).
e. A fault in the intrusion detection system (an entire floor is inoperable or any fault in any detector in the strong rooms).
f. Fault in anti-ram barrier.

Upon arrival at the facility, the Contractor shall continuously address the fault without interruption until the repair is completed, including after regular working hours, to the full satisfaction of the Client.
The Client may, at its sole discretion, extend the response times.

Penalty mechanism

The Contractor shall pay the following penalties for failing to meet the defined SLA:

Fault Type	Penalty
Critical Fault	80,000 Kenyan shilling (charged for every 8 hours of delay)
Non-Critical Fault	40,000 Kenyan shilling (charged for every 12 hours of delay)

Service centre

The Contractor shall operate a service center capable of receiving and managing service calls.
Notification to the service center of a fault shall be considered a binding notification obligating the Contractor to take all necessary measures to rectify the issue as described above.

Equipment and materials for maintenance

The Contractor shall, at its own expense, provide all equipment necessary to perform maintenance services, including complete units and assemblies, electronic cards, spare parts, components, cables, connectors, and consumables such as fuses, bulbs, screws, batteries, accumulators, etc.

For replacements, the Contractor shall only use new equipment from the same manufacturers and models installed in the Client's system. Use of alternative equipment requires prior approval from the Client.

Inventory levels of equipment and components

The Contractor is required to maintain an adequate and sufficient inventory of spare parts at its facility to ensure uninterrupted maintenance, including cameras, servers, computers, electronic cards, repair components, replacement cables, and installation accessories.
The Contractor shall take into consideration quantities necessary to meet the maintenance response times specified in this specification.

Maintenance technical team

Maintenance shall be carried out by a skilled and dedicated team of technicians specifically assigned to maintain the Client's system.
During the maintenance period, the Contractor shall provide, as required, a senior system/electronics engineer familiar with all system components to assist in solving issues that the regular maintenance team cannot resolve.

Computerized monitoring system

System maintenance tracking shall be performed using the Contractor's "computerized monitoring system."
Once a year, or as required by the Client, the Contractor shall provide a statistical fault analysis in various breakdowns, including at least:

a. Total number of faults in the system.
b. Number of faults per specific system item.
c. List of replacement equipment and replacement dates.
d. Average technician response time to the facility.
e. Average fault repair time – Mean Time to Repair (MTTR).
f. Average time between failures – Mean Time Between Failures (MTBF).

System documentation updates

In the event that any repair, maintenance, system renewal, or addition of equipment results in a change in system configuration, composition, quantity of equipment, infrastructure, or installation, the Contractor shall update the technical documentation held by the Client.
Updates to the technical documentation shall be completed no later than 30 days from the date of the change.

The Contractor shall provide the updated documentation in both hard copy and electronic (soft) copy formats.

MEASUREMENT OF QUANTITIES

General

Payments to the Contractor shall be based solely on the actual quantities of equipment installed at the facility. The quantities shall be determined by the Supervisor based on field measurements.

Unit prices

The unit prices in the bill of quantities shall include detailed design, production, supply, installation, connection, wiring, testing, commissioning, warranty, and the value of all works, materials, and expenses.

Without limiting the generality of the foregoing, the unit prices shall also include the following items (a through inclusive), unless explicitly stated otherwise in the executed Contract:

a. All materials (including finished products and auxiliary materials included in the work) and their depreciation.
b. Use of measuring instruments, scaffolding, ladders, tools, engineering equipment, auxiliary equipment, mechanical equipment, transport vehicles, etc.
c. All works required for the execution of the Project as defined in the specifications.

d. Transport of personnel, materials, and tools to and from the facility, including any loading and unloading work required.
e. Storage of materials, tools, instruments, machinery, equipment, etc., and their safekeeping; storage and safekeeping of disassembled equipment and materials on site intended for reinstallation.
f. Removal of all waste generated during the work outside the Client's premises.
g. Full responsibility for works, materials, and equipment located at the Client's site during execution, up to the final handover of the Project to the Client.
h. Taxes, levies, import duties, insurance expenses, social conditions, and any other expenditure related to the execution of the Project.
i. The Contractor's general expenses, direct and indirect.
j. Any other expenses of any type required under the agreement between the Contractor and the Client.
k. System design and full integration among the various systems.
l. Contractor's profit.

Changes and additions to Bill of Quantities

The Client may instruct the Contractor to perform changes to the works, and the Contractor shall carry them out whether or not they appear in the bill of quantities in the Contract.

If a unit price for any item appears in the bill of quantities, it shall be paid according to the bill of quantities.
If a unit price for any item is not included in the bill of quantities, it shall be paid according to the additional works rules set forth in the Contract.

Price analysis based on supplier/manufacturer price lists or the proposal of a single subcontractor shall not be accepted, except with prior special approval of the Client.