KDEAP KENYA DIGITAL ECONOMY ACCELERATION PROJECT

ICT Authority

THE WORLD BANK

Government of Kenya

Request for Proposals

Information Systems

(Two-Envelope Bidding Process- Without Prequalification)

Procurement of:

Supply, Delivery, Integration, Support, Capacity Building and Maintenance Support of Hardware, Analysts Computer, SOC-Security Software and Technology tools, Support for ICTA's Government Security Operation Centre (GOVSOC)

Purchaser: **The Information and Communications Technology Authority**

Project: **Kenya Digital Economy Acceleration Project**

Contract title**: Supply, Delivery, Integration, Support, Capacity Building and Maintenance Support of Hardware, Analyst Compute, Security Software and Technology Tools, Support for ICTA's Government Security Operations Center**

Country: **Kenya**

Loan No. **7289-KE and 7290-KE**

RFP No: **KE-ICTA-571743-NC-RFP**

Issued on: **17th November 2026**

Vision

Tranforming Lives Using ICT

Mission

To champion and harness ICT to enable efficient and effective access in the delivery of public service for the public office and public service.

Official Use Only



Specific Procurement Notice – Request for Proposals without Prequalification

Request for Proposal Information Systems

(Design, Supply and Installation)

(Two-Envelope Bidding Process-Without Prequalification)

Purchaser: **The Information and Communications Technology Authority**

Project: **Kenya Digital Economy Acceleration Project**

Contract title: **Supply, Delivery, Integration, Support, Capacity Building and Maintenance Support of Hardware, Analyst Compute, SOC-Security Software and Technology Tools, Support for ICTA's Government Security Operations Center**

Country: **Kenya**

Loan No. **7289-KE and 7290-KE**

RFP No: **KE-ICTA-571743-NC-RFP**

Issued on: **17th November 2026**

1. The Government of Kenya has received financing from the World Bank toward the cost of the Kenya Digital Economy Acceleration Project, and intends to apply part of the proceeds toward payments under the contract for **Supply, Delivery, Integration, Support, Capacity Building and Maintenance Support of Hardware, Analyst Compute, Security Software and Technology Tools, Support for ICTA's Government Security Operations Center**. For this contract, the Borrower shall process the payments using the Direct Payment disbursement method, as defined in the World Bank's Disbursement Guidelines for Investment Project Financing, except for those payments, which the contract provides to be made through letter of credit.

2. The Information and Communications Technology Authority (ICT Authority) now invites sealed Proposals from eligible Proposers for **Supply, Delivery, Integration, Support, Capacity Building and Maintenance Support of Hardware, Analyst Compute, SOC-Security Software and Technology Tools, Support for ICTA's Government Security Operations Center, to be installed on 23rd Floor, Telposta Towers, along Kenyatta Avenue, Nairobi, Kenya, within thirty-five (35) weeks from the Effective Date of the Contract to Operational Acceptance of the complete System, followed by a five (5) year support and maintenance period.**

3. The procurement process will be conducted through international competitive procurement using Request for Proposals (RFP) as specified in the World Bank's "Procurement

Regulations for IPF Borrowers" **First Published in July 2016, Revised Fifth Edition, September 2023** ("Procurement Regulations"), and is open to all eligible Proposers as defined in the Procurement Regulations.

4. Proposals will be evaluated in accordance with the evaluation process set out in the bidding documents. The following weightings shall apply for Rated Criteria (including technical and non-price factors): 80% and the Financial Proposal: 20%

5. Interested eligible Proposers may obtain further information from ICTA, Deputy Director Supply chain management / procurement@ict.go.ke and inspect the request for proposal document during office hours 0900 to 1600 hours East African Time (EAT) at the address given below.

6. The bidding document in English may also be downloaded free of charge by interested eligible Bidders from the ICTA's website https://www.icta.go.ke/tenders or Public Procurement Information Portal website https://www.tenders.go.ke Bidders who download the bidding documents are invited to notify the purchaser by e-mail with full contact details if they intended to participate, as this will facilitate issuance of notifications by the Purchaser during the procurement process, to all bidders where necessary.

7. Proposals must be delivered to the address below on or before **10:00am EAT on 7th January 2027.** Electronic procurement **will not** be permitted. Late Proposals will be rejected. The outer Proposal envelopes marked "ORIGINAL PROPOSAL", and the inner envelopes marked "TECHNICAL PART" will be publicly opened in the presence of the Proposers' designated representatives and anyone who chooses to attend, at the address below on **10:00am EAT on 7th January 2027**. All envelopes marked "FINANCIAL PART" shall remain unopened and will be held in safe custody of the Purchaser until the public opening of Financial Parts.

8. The Proposals must be accompanied by a **Proposal Security (unconditional bank guarantee)** of **KES. 10 Million (Kenya Shillings Ten Million Only) Or Equivalent In a Freely Convertible Currency.**

9. Attention is drawn to the Procurement Regulations requiring the Borrower to disclose information on the successful Proposer's beneficial ownership, as part of the Contract Award Notice, using the Beneficial Ownership Disclosure Form as included in the request for proposal document.

10. The address (es) referred to above is (are):

Jessy K. Maruti
Chief Executive Officer
The Information and Communications Technology Authority
12th Floor, Telposta Towers, Along Kenyatta Avenue
P.O. Box 27150-00100
NAIROBI, KENYA
info@ict.go.ke/procurement@ict.go.ke

Table of Contents

Section I - Instructions to Proposers (ITP).....5
Section II - Proposal Data Sheet (PDS).....46
Section III - Evaluation and Qualification Criteria (After Prequalification) 57
Section III - Evaluation and Qualification Criteria (Without Prequalification) 56
Section IV - Proposal Forms 87
Section V - Eligible Countries.....135
Section VI - Fraud and Corruption.....137
Section VII - Requirements of the Information System 140
Section VIII - General Conditions of Contract 270
Section IX - Special Conditions of Contract.....357
Section X - Contract Forms 376

PART 1 – REQUEST FOR PROPOSALS PROCEDURES

SECTION I - INSTRUCTIONS TO PROPOSERS (ITP)

Contents

A. General....7

1. Scope of Proposal....7
2. Source of Funds....8
3. Fraud and Corruption....8
4. Eligible Proposers....9
5. Eligible Goods and Services....12

B. Contents of the Request for Proposals Document....12

6. Sections of the Request for Proposals Document....12
7. Clarification of Request for Proposals Document, Site Visit, Pre-Proposal Meeting 14
8. Amendment of Request for Proposals Document....15

C. Preparation of Proposals....15

9. Cost of Proposals....15
10. Language of Proposal....15
11. Documents Comprising the Proposal....15
12. Letters of Proposal and Price Schedules....17
13. Alternative Proposals....18
14. Documents Establishing the Eligibility of the Information System....18
15. Documents Establishing the Eligibility and Qualifications of the Proposer....18
16. Documents Establishing Conformity of the Information System....19
17. Proposal Prices....21
18. Currencies of Proposal and Payment....23
19. Period of Validity of Proposals....23
20. Proposal Security....24
21. Format and Signing of Proposal....26

D. Submission of Proposals....26

22. Submission, Sealing and Marking of Proposals....26
23. Deadline for Submission of Proposals....28
24. Late Proposals....28
25. Withdrawal, Substitution, and Modification of Proposals....28

E. Public Opening of Technical Parts of Proposals....29

26. Public Opening of Technical Parts of Proposals....29

F. Evaluation of Proposals- General Provisions....30

27. Confidentiality....30
28. Clarification of Proposals....31
29. Deviations, Reservations, and Omissions....31

G. Evaluation of Technical Part of Proposals 32

30. ... Determination of Responsiveness 32
31. ... Eligibility and Qualifications of the Proposer 32
32. ... Detailed Evaluation of Technical Part 33

H. Notification of Evaluation of Technical Parts and Public Opening of Financial Parts33

33. ... Notification of Evaluation of Technical Parts and Public Opening of Financial Parts33

I. Evaluation of Financial Part of Proposals 36

34. ... Adjustments for Non-material Noconformities 36
35. ... Correction of Arithmetic Errors 36
36. ... Evaluation of Proposals Financial Part 37
37. ... Abnormally Low Proposals 38
38. ... Unbalanced or Front Loaded Proposals 38

J. Evaluation of Combined Technical and Financial Parts, Most Advantageous Proposal And Notification of Intention To Award 39

39. ... Evaluation of combined Technical and Financial Parts, Most Advantageous Proposal 39
40. ... Purchaser's Right to Accept Any Proposal, and to Reject Any or All Proposals 40
41. ... Standstill Period 41
42. ... Notification of Intention to Award 41

K. Award of Contract 41

43. ... Award Criteria 41
44. ... Purchaser's Right to Vary Quantities at Time of Award 41
45. ... Notification of Award 42
46. ... Debriefing by the Purchaser 42
47. ... Signing of Contract 43
48. ... Performance Security 44
49. ... Adjudicator 44
50. ... Procurement Related Complaint 45

Section I - Instructions to Proposers

A. GENERAL

1. Scope of Proposal

1.1. The Purchaser, as indicated in the PDS, or its duly authorized Purchasing Agent if so specified in the PDS (interchangeably referred to as "the Purchaser" issues this request for proposals document for the supply and installation of the Information System as specified in Section VII, Purchaser's Requirements. The name, identification and details of this RFP are specified in the PDS.

1.2. Unless otherwise stated, throughout this request for proposals document definitions and interpretations shall be as prescribed in the Section VIII, General Conditions of Contract.

Throughout this request for proposals document:

(a) the term "in writing" means communicated in written form (e.g. by mail, e-mail, fax, including if specified in the PDS, distributed or received through the electronic-procurement system used by the Purchaser) 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 Borrower. It excludes the Borrower's official public holidays.

(d) "ES" means environmental and social (including Sexual Exploitation and Abuse (SEA), and Sexual Harassment (SH));

(e) "Sexual Exploitation and Abuse" "(SEA)" means the following:

Sexual Exploitation is defined as any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another;

Sexual Abuse is defined as the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions.

(f) "Sexual Harassment" "(SH)" is defined as unwelcome sexual advances, requests for sexual favors, and other verbal

or physical conduct of a sexual nature by the Supplier's Personnel with other Supplier's Personnel or Purchaser's Personnel.

(g) "Supplier's Personnel" is as defined in GCC Clause 1.1; and

(h) "Purchaser's Personnel" is as defined in GCC Clause 1.1.

A non-exhaustive list of (i) behaviors which constitute SEA and (ii) behaviors which constitute SH is attached to the Code of Conduct form in Section IV

2. Source of Funds

2.1. The Borrower or Recipient (hereinafter called "Borrower") indicated in the PDS has applied for or received financing (hereinafter called "funds") from the International Bank for Reconstruction and Development or the International Development Association (hereinafter called "the Bank") in an amount specified in the PDS toward the project named in the PDS. The Borrower intends to apply a portion of the funds to eligible payments under the contract(s) for which this request for proposals document is issued.

2.2. Payments by the Bank will be made only at the request of the Borrower and upon approval by the Bank in accordance with the terms and conditions of the Loan (or other financing) Agreement between the Borrower and the Bank (hereinafter called the Loan Agreement), and will be subject in all respects to the terms and conditions of that Loan (or other financing) Agreement. The Loan (or other financing) Agreement prohibits a withdrawal from the loan account for the purpose of any payment to persons or entities, or for any import of equipment, materials or any other goods, if such payment or import is prohibited by a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations. No party other than the Borrower shall derive any rights from the Loan (or other financing) Agreement or have any claim to the funds.

3. Fraud and Corruption

3.1. The Bank requires compliance with the Bank's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in Section VI.

3.2. In further pursuance of this policy, Proposers shall permit and shall cause their agents (where declared or not), subcontractors, subconsultants, service providers, suppliers, and personnel, to permit the Bank to inspect all accounts, records and other documents relating to any initial selection process,

prequalification process, bid submission, proposal submission and contract performance (in the case of award), and to have them audited by auditors appointed by the Bank.

4. Eligible Proposers

4.1. A Proposer may be a firm that is a private entity, a state-owned enterprise or institution subject to ITP 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 into such an agreement supported by a letter of intent. 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 procurement process and, in the event the JV is awarded the Contract, during contract execution. Unless specified in the PDS, there is no limit on the number of members in a JV.

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

(a) directly or indirectly controls, is controlled by or is under common control with another Proposer; or

(b) receives or has received any direct or indirect subsidy from another Proposer; or

(c) has the same legal representative as another Proposer; or

(d) has a relationship with another Proposer, directly or through common third parties, that puts it in a position to influence the Proposal of another Proposer, or influence the decisions of the Purchaser regarding this procurement 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 Proposal; or

(f) or any of its affiliates has been hired (or is proposed to be hired) by the Purchaser or Borrower 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

Official Use Only

project specified in the PDS ITP 2.1 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 Borrower (or of the project implementing agency, or of a recipient of a part of the loan) who: (i) are directly or indirectly involved in the preparation of the request for proposals document or specifications of the Contract, and/or the Proposal 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 Bank throughout the procurement process and execution of the Contract.

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

4.4. A Proposer may have the nationality of any country, subject to the restrictions pursuant to ITP 4.8. A Proposer shall be deemed to have the nationality of a country if the Proposer 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 may be. 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.

Official Use Only

4.5. A Proposer that has been sanctioned by the Bank, pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework as described in Section VI paragraph 2.2 d., shall be ineligible to be initially selected for, prequalified for, bid for, propose for, or be awarded a Bank-financed contract or benefit from a Bank-financed contract, financially or otherwise, during such period of time as the Bank shall have determined. The list of debarred firms and individuals is available at the electronic address specified in the PDS.

4.6. Proposers that are state-owned enterprises or institutions in the Purchaser's Country may be eligible to compete and be awarded a Contract(s) only if they can establish, in a manner acceptable to the Bank, that they (i) are legally and financially autonomous (ii) operate under commercial law, and (iii) are not under supervision of the Purchaser.

4.7. A Proposer shall not be under suspension from bidding or submitting proposals by the Purchaser as the result of the operation of a Bid–Securing Declaration or Proposal-Securing Declaration.

4.8. Firms and individuals may be ineligible if so indicated in Section V and (a) as a matter of law or official regulations, the Borrower's country prohibits commercial relations with that country, provided that the Bank is satisfied that such exclusion does not preclude effective competition for the supply of goods or the contracting of works or services required; 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, the Borrower's country 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. This request for proposal process is open for all eligible Proposers, unless otherwise specified in ITP 15.2.

4.10. A Proposer shall provide such documentary evidence of eligibility satisfactory to the Purchaser, as the Purchaser shall reasonably request.

4.11. A firm that is under a sanction of debarment by the Borrower from being awarded a contract is eligible to participate in this procurement, unless the Bank, at the Borrower's request, is satisfied that the debarment; (a) relates to fraud or corruption,

and (b) followed a judicial or administrative proceeding that afforded the firm adequate due process.

5. Eligible Goods and Services

5.1. The Information Systems to be supplied under the Contract and financed by the Bank may have their origin in any country in accordance with Section V, Eligible Countries.

5.2. For the purposes of this request for proposals document, the term "Information System" means all:

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

(b) 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 Proposer and as specified in the Contract.

5.3. For purposes of ITP 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.

B. CONTENTS OF THE REQUEST FOR PROPOSALS DOCUMENT

6. Sections of the Request for Proposals Document

6.1. The request for proposals document consists of Parts 1, 2, and 3, which include all the sections indicated below, and should be read in conjunction with any Addenda issued in accordance with ITP 8:

PART 1 - Request for Proposals Procedures

Section I - Instructions to Proposers (ITP)

Section II - Proposal Data Sheet (PDS)

Section III - Evaluation and Qualification Criteria

Section IV - Proposal Forms

Section V - Eligible Countries

Section VI - Fraud and Corruption

PART 2 - Purchaser's Requirements

Section VII - Requirements of the IS, including:

- Technical Requirements
- Implementation Schedule
- System Inventory Tables
- Background and Informational Materials

PART 3 - Contract

Section VIII - General Conditions of Contract

Section IX -Special Conditions of Contract

Section X - Contract Forms

6.2. The Specific Procurement Notice – Request for Proposals (RFP) issued by the Purchaser is not part of this request for proposals document.

6.3. Unless obtained directly from the Purchaser, the Purchaser is not responsible for the completeness of the document, responses to requests for clarification, the Minutes of the pre-Proposal meeting (if any), or Addenda to the request for proposals document in accordance with ITP 8. In case of any contradiction, documents obtained directly from the Purchaser shall prevail.

6.4. The Proposer is expected to examine all instructions, forms, terms, and specifications in the request for proposals document and to furnish with its Proposal all information or documentation as is required by the request for proposals document.

Official Use Only

7. Clarification of Request for Proposals Document, Site Visit, Pre-Proposal Meeting

7.1. A Proposer requiring any clarification of the request for proposals document shall contact the Purchaser in writing at the Purchaser's address specified in the PDS or raise its enquiries during the pre-Proposal meeting if provided for in accordance with ITP 7.4. The Purchaser will respond in writing to any request for clarification, provided that such request is received prior to the deadline for submission of Proposals within a period specified in the PDS. The Purchaser's shall forward copies of its response to all Proposers who have acquired the request for proposals document in accordance with ITP 6.3, including a description of the inquiry but without identifying its source. If so specified in the PDS, the Purchaser shall also promptly publish its response at the web page identified in the PDS. Should the Purchaser deem it necessary to amend the request for proposals document as a result of a request for clarification, it shall do so following the procedure under ITP 8 and ITP 23.2.

7.2. The Proposer may wish to visit and examine the site where the Information System is to be installed and its surroundings and obtain for itself on its own responsibility all information that may be necessary for preparing the Proposal and entering into a contract. The costs of visiting the site shall be at the Proposer's own expense.

7.3. The Proposer and any of its personnel or agents will be granted permission by the Purchaser to enter upon its premises and lands for the purpose of such visit, but only upon the express condition that the Proposer, its personnel, and agents will release and indemnify the Purchaser and its personnel and agents from and against all liability in respect thereof, and will be responsible for death or personal injury, loss of or damage to property, and any other loss, damage, costs, and expenses incurred as a result of the inspection.

7.4. The Proposer's designated representative is invited to attend a pre-Proposal meeting and/or a site visit, if provided for in the PDS. The purpose of the meeting will be to clarify issues and to answer questions on any matter that may be raised at that stage.

7.5. The Proposer is requested, as far as possible, to submit any questions in writing, to reach the Purchaser not later than two Working (2) weeks before the meeting.

7.6. Minutes of the pre-Proposal meeting, including the text of the questions raised without identifying the source, and the responses given, together with any responses prepared after the meeting, will be transmitted promptly to all Proposers who have acquired the request for proposals document in accordance with ITP 6.3. Any

modification to the request for proposals document that may become necessary as a result of the pre-Proposal meeting shall be made by the Purchaser exclusively through the issue of an Addendum pursuant to ITP 8 and not through the minutes of the pre-Proposal meeting.

7.7. Nonattendance at the pre-Proposal meeting will not be a cause for disqualification of a Proposer.

8. Amendment of Request for Proposals Document

8.1. At any time prior to the deadline for submission of Proposals, the Purchaser may amend the request for proposals document by issuing addenda.

8.2. Any addendum issued shall be part of the request for proposals document and shall be communicated in writing to all who have obtained the request for proposals document from the Purchaser in accordance with ITP 6.3. The Purchaser shall also promptly publish the addendum on the Purchaser's web page in accordance with ITP 7.1.

8.3. To give prospective Proposers reasonable time in which to take an addendum into account in preparing their Proposals, the Purchaser may, at its discretion, extend the deadline for the submission of Proposals, pursuant to ITP 23.2.

C. PREPARATION OF PROPOSALS

9. Cost of Proposals

9.1. The Proposer shall bear all costs associated with the preparation and submission of its Proposal, and the Purchaser shall not be responsible or liable for those costs, regardless of the conduct or outcome of the Request for Proposals process.

10. Language of Proposal

10.1. The Proposal, as well as all correspondence and documents relating to the Proposal exchanged by the Proposer and the Purchaser, shall be written in the language specified in the PDS. Supporting documents and printed literature that are part of the Proposal may be in another language provided they are accompanied by an accurate translation of the relevant passages in the language specified in the PDS, in which case, for purposes of interpretation of the Proposal, such translation shall govern.

11. Documents Comprising the Proposal

11.1. The Proposal shall comprise two Parts, namely the Technical Part and the Financial Part. These two Parts shall be submitted simultaneously in two separate sealed envelopes (two-envelope procurement process). One envelope shall contain only information relating to the Technical Part and the other, only information relating to the Financial Part. These two envelopes

shall be enclosed in a separate sealed outer envelope marked "Original Proposal'.

11.2. The Technical Part shall contain the following:

(a) **Letter of Proposal**-Technical Part, prepared in accordance with ITP 12;

(b) **Proposal Security or Proposal-Securing Declaration** in accordance with ITP 20;

(c) **Alternative Proposal**- Technical Part**:** if permissible, in accordance with ITP 13, the Technical Part of any Alternative Proposal;

(d) **Authorization:** written confirmation authorizing the signatory of the Proposal to commit the Proposer, in accordance with ITP 21.3;

(e) **Eligibility of Information System:** documentary evidence established in accordance with ITP 14.1 that the Information System offered by the Proposer in its Proposal or in any alternative Proposal, if permitted, are eligible;

(f) **Proposer's Eligibility and qualifications:** documentary evidence in accordance with ITP 15 establishing the Proposer's eligibility and qualifications to perform the contract if its Proposal is accepted;

(g) **Conformity:** documentary evidence established in accordance with ITP 16 that the Information System offered by the Proposer conform to the **request for proposals** document;

(h) **Subcontractors:** list of subcontractors, in accordance with ITP 16.4;

(i) **Intellectual Property**: a list of: Intellectual Property as defined in GCC Clause 15;

(i) all Software included in the Proposal, assigning each item to one of the software categories defined in GCC Clause 1.1 (c):

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

b. Standard and Custom Software;

(ii) all Custom Materials, as defined in GCC Clause 1.1 (c), included in the Proposal;

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

(j) any other document required **in the PDS.**

11.3. **The Financial Part shall contain the following:**

(a) Letter of Proposal – Financial Part: prepared in accordance with ITP 12 and ITP 17;

(b) Schedule: Price Schedules completed in accordance with ITP 12 and ITP 17;

(c) Alternative Proposal - Financial Part: if permissible in accordance with ITP 13, the Financial Part of any Alternative Proposal; and

(d) any other document required in the PDS.

11.4. The Technical Part shall not include any information related to the Proposal price. Where material financial information related to the Proposal price is contained in the Technical Part the Proposal shall be declared non-responsive.

11.5. In addition to the requirements under ITP 11.2, Proposals submitted by a JV shall include in the Technical Part 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 letter of intent to execute a Joint Venture Agreement in the event of a successful Proposal shall be signed by all members and submitted with the Proposal, together with a copy of the proposed Agreement indicating at least the parts of the Information System to be executed by the respective members.

11.6. The Proposer shall furnish in the Letter of Proposal - Financial Part information on commissions and gratuities, if any, paid or to be paid to agents or any other party relating to this procurement process.

12. Letters of Proposal and Price Schedules

12.1. The Letter of Proposal - Technical Part, Letter of Proposal-Financial Part and Price Schedules shall be prepared using the relevant forms furnished in Section IV, Proposal Forms. The forms must be completed without any alterations to the text, and no

Official Use Only

substitutes shall be accepted except as provided under ITP 21.3. All blank spaces shall be filled in with the information requested.

13. Alternative Proposals

13.1. The PDS indicates whether alternative Proposals are allowed. If they are allowed, the PDS will also indicate whether they are permitted in accordance with ITP 13.3, or invited in accordance with ITP 13.2 and/or ITP 13.4.

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

13.3. Except as provided under ITP 13.4 below, Proposers wishing to offer technical alternatives to the Purchaser's requirements as described in the request for proposals document must also provide: (i) a price at which they are prepared to offer an Information System meeting the Purchaser's requirements; and (ii) all information necessary for a complete evaluation of the alternatives by the Purchaser, 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 Proposer with the Most Advantageous Proposal conforming to the basic technical requirements shall be considered by the Purchaser.

13.4. When Proposers are invited in the PDS to submit alternative technical solutions for specified parts of the system, such parts shall be described in Section VII, Purchaser's Requirements. Technical alternatives that comply with the performance and technical criteria specified for the Information System shall be considered by the Purchaser on their own merits, pursuant to ITP 32.

14. Documents Establishing the Eligibility of the Information System

14.1. To establish the eligibility of the Information System in accordance with ITP 5, Proposers shall complete the country of origin declarations in the Price Schedule Forms, included in Section IV, Proposal Forms.

15. Documents Establishing the Eligibility and Qualifications of the Proposer

15.1. To establish its eligibility and qualifications to perform the Contract in accordance with Section III, Evaluation and Qualification Criteria, the Proposer shall provide the information requested in the corresponding information sheets included in Section IV, Proposal Forms.

15.2. In the event that prequalification of potential Proposers has been undertaken as stated in the PDS, only Proposals from prequalified

Official Use Only

Proposers shall be considered for award of Contract. These qualified Proposers should submit with their Proposals any information updating their original prequalification applications or, alternatively, confirm in their Proposals that the originally submitted prequalification information remains essentially correct as of the date of Proposal submission.

15.3. Any change in the structure or formation of a Proposer after being prequalified and invited to submit Proposals, if applicable, (including, in the case of a JV, any change in the structure or formation of any member and also including any change in any specialized subcontractor whose qualifications were considered to prequalify the Applicant) shall be subject to the written approval of the Purchaser prior to the deadline for submission of Proposals. Such approval shall be denied if (i) a Proposer proposes to associate with a disqualified Proposer or in case of a disqualified joint venture, any of its members; (ii) as a consequence of the change, the Proposer no longer substantially meets the qualification criteria; or (iii) in the opinion of the Purchaser, the change may result in a substantial reduction in competition. Any such change should be submitted to the Purchaser not later than fourteen (14) days after the date of the notice for RFP sent to the prequalified Proposers.

16. Documents Establishing Conformity of the Information System

16.1. Pursuant to ITP 11.2 (g), the Proposer shall furnish, as part of its Proposal, documents establishing the conformity to the request for proposals documents of the Information System that the Proposer proposes to design, supply and install under the Contract.

16.2. The documentary evidence of conformity of the Information System to the request for proposals documents including:

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

(b) written confirmation that the Proposer accepts responsibility for the successful integration and inter-operability of all

components of the Information System as required by the request for proposals documents;

(c) an item-by-item commentary on the Purchaser's Technical Requirements, demonstrating the substantial responsiveness of the Information System offered to those requirements. In demonstrating responsiveness, the Proposer should use the Technical Responsiveness Checklist (or Checklist Format) in the Sample Proposal Forms (Section IV). The commentary shall include explicit cross-references to the relevant pages in the supporting materials included in the Proposal. Whenever a discrepancy arises between the item-by-item commentary and any catalogs, technical specifications, or other preprinted materials submitted with the Proposal, 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 PDS ITP 17.2 requires Proposers to propose.

16.3. References to brand names or model numbers or national or proprietary standards designated by the Purchaser in the request for proposals documents are intended to be descriptive and not restrictive. Except as specified in the PDS for specific items or standards, the Proposer may substitute alternative brand/model names or standards in its Proposal, provided that it demonstrates to the Purchaser'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.

16.4. For major items of the Information System as listed by the Purchaser in Section III, Evaluation and Qualification Criteria, which the Proposer intends to purchase or subcontract, the Proposer shall give details of the name and nationality of the proposed subcontractors, including manufacturers, for each of those items. In addition, the Proposer shall include in its Proposal information establishing compliance with the requirements specified by the Purchaser 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.

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

Official Use Only

17. Proposal Prices

17.1. 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 Proposer to fulfill the requirements of the Information System, must be priced separately and summarized in the corresponding cost tables in the Sample Proposal Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below.

17.2. Unless otherwise specified in the PDS, the Proposer must also propose 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 tables in the Sample Proposal Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below:

(a) if specified **in the PDS,** the Proposer must also propose 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 Proposer'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.

17.3. 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. Proposers may be required to provide a breakdown of any composite or lump-sum items included in the Cost Tables

17.4. The price of items that the Proposer has left blank in the cost tables provided in the Sample Proposal 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 Proposal and, provided that the Proposal is substantially

Official Use Only

responsive, an adjustment to the Proposal price will be made during Proposal evaluation in accordance with ITP 34.1.

17.5. 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 PDS, as follows:

(a) Goods supplied from outside the Purchaser's country:

Unless otherwise specified **in the PDS**, the prices shall be quoted on a CIP (named place of destination) basis, exclusive of all taxes, stamps, duties, levies, and fees imposed in the Purchaser's country. 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 Proposer shall be free to use transportation through carriers registered in any eligible countries. Similarly, the Proposer may obtain insurance services from any eligible source country;

(b) Locally supplied Goods:

Unit prices of Goods offered from within the Purchaser's Country, shall be quoted on an EXW (ex factory, ex works, ex warehouse 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;

(c) Inland transportation.

17.6. Unless otherwise stated in the PDS, 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 ITP 17.5, whether the Goods are to be supplied locally or from outside the Purchaser's country, except when these costs are already included in the price of the Goods, as is, e.g., the case, when ITP 17.5 (a) specifies CIP, and the named places of destination are the Project Sites.

17.7. 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 the Purchaser's country on/to the price of the Services invoiced to the Purchaser, if the Contract is awarded.

Official Use Only

17.8. Unless otherwise specified in the PDS, 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 Purchaser or its staff, or by third parties, must be included in the price only to the extent such obligations are made explicit in these request for proposals documents (as, e.g., a requirement for the Proposer to include the travel and subsistence costs of trainees).

17.9. Unless otherwise specified in the PDS, prices quoted by the Proposer shall be fixed during the Proposer's performance of the Contract and not subject to increases on any account. Proposals submitted that are subject to price adjustment will be rejected.

18. Currencies of Proposal and Payment

18.1. The currency(ies) of the Proposal and currencies of payment shall be the same. The Proposer shall quote in the currency of the Purchaser's Country the portion of the Proposal price that corresponds to expenditures incurred in the currency of the Purchaser's Country, unless otherwise specified in the PDS.

18.2. The Proposer may express the Proposal price in any currency. If the Proposer wishes to be paid in a combination of amounts in different currencies, it may quote its price accordingly but shall use no more than three foreign currencies in addition to the currency of the Purchaser's Country.

19. Period of Validity of Proposals

19.1. Proposals shall remain valid until the date specified in the PDS or any extended date if amended by the Purchaser in accordance with ITP 8. A Proposal that is not valid until the date specified in the PDS, or any extended date if amended by the Purchaser in accordance with ITP 8, shall be rejected by the Purchaser as nonresponsive.

19.2. In exceptional circumstances, prior to the date of expiry of the Proposal validity, the Purchaser may request Proposers to extend the date of validity until a specified date. The request and the responses shall be made in writing. If a Proposal Security is requested in accordance with ITP 20, it shall also be extended for twenty-eight days (28) beyond the deadline of the extended validity period. A Proposer may refuse the request without forfeiting its Proposal Security. A Proposer granting the request shall not be required or permitted to modify its Proposal, except as provided in ITP 19.3.

19.3. If the award is delayed by a period exceeding fifty-six (56) days beyond the expiry of the initial Proposal validity specified in

accordance with ITP 19.1, the Contract price shall be determined as follows:

(a) in case of fixed price contracts, the contract price shall be the Proposal price adjusted by a factor or factors specified **in the PDS**;

(b) in the case of an adjustable price contracts, no adjustments shall be made;

(c) in any case, Proposal evaluation shall be based on the Proposal Price without taking into consideration the applicable correction from those indicated above.

20. Proposal Security

20.1. The Proposer shall furnish as part of the Technical Part of its Security as specified in the PDS, in original form and, in the case of a Proposal Security, in the amount and currency specified in the PDS.

20.2. A Proposal-Security shall use the form included in Section IV, Proposal Forms.

20.3. If a Proposal Security is specified pursuant to ITP 20.1, the Proposal security shall be a demand guarantee in any of the following forms at the Proposer's option:

(a) an unconditional guarantee issued by a non-bank financial institution (such as an insurance, bonding or surety company);

(b) an irrevocable letter of credit;

(c) a cashier's or certified check; or

(d) another security indicated **in the PDS,**

from a reputable source from an eligible country. If an unconditional guarantee is issued by a non-bank financial institution located outside the Purchaser's Country the issuing non-bank financial institution shall have a correspondent financial institution located in the Purchaser's Country to make it enforceable unless the Purchaser has agreed in writing, prior to Proposal submission, that a correspondent financial institution is not required. In the case of a bank guarantee, the Proposal Security shall be submitted either using the Proposal Security Form included in Section IV, Proposal Forms or in another substantially similar format approved by the Purchaser prior to Proposal submission. In either case, the form must include the complete name of the Proposer. The Proposal Security shall be valid for twenty-eight (28) days beyond the original date of expiry of the Proposal validity, or beyond any extended date if requested under ITP 19.2.

20.4. If a Proposal Security is specified pursuant to ITP 20.1, any Proposal not accompanied by a substantially responsive Proposal Security shall be rejected by the Purchaser as non-responsive.

20.5. If a Proposal Security is specified pursuant to ITP 20.1, the Proposal Security of unsuccessful Proposers shall be returned as promptly as possible upon the successful Proposer's furnishing of the Performance Security pursuant to ITP 48.

20.6. The Proposal Security of the successful Proposer shall be returned as promptly as possible once the successful Proposer has signed the Contract and furnished the required Performance Security.

20.7. The Proposal Security may be forfeited:

(a) if a Proposer withdraws its Proposal prior to the expiry date of Proposal validity specified by the Proposer on the Letter of Proposal or any extended date provided by the Proposer; or

(b) if the successful Proposer fails to**:**

(i) sign the Contract in accordance with ITP 47; or

(ii) furnish a performance security in accordance with ITP 48.

20.8. The Proposal Security of a JV shall be in the name of the JV that submits the Proposal. If the JV has not been legally constituted into a legally enforceable JV at the time of submission of Proposals, the Proposal Security shall be in the names of all future members as named in the letter of intent referred to in ITP 4.1 and ITP 11.5.

20.9. If a Proposal Security is not required in the PDS, and;

(a) if a Proposer withdraws its Proposal prior to the expiry date of the Proposal validity specified by the Proposer on the Letter of Proposal, or any extended date provided by the Proposer; or

(b) if the successful Proposer fails to: sign the Contract in accordance with ITP 47; or furnish a Performance Security in accordance with ITP 48;

the Purchaser may, if provided for **in the PDS**, declare the Proposer disqualified to be awarded a contract by the Purchaser for a period of time as stated **in the PDS**.

21. Format and Signing of Proposal

21.1. The Proposer shall prepare one original and copies/sets of the documents comprising the Proposal as described in ITP 11 and Proposer22.

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

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

21.4. In case the Proposer is a JV, the Proposal 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.

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

D. SUBMISSION OF PROPOSALS

22. Submission, Sealing and Marking of Proposals

22.1. The Proposer shall deliver the Proposal in two separate, sealed envelopes (the Technical Part and the Financial Part). These two envelopes shall be enclosed in a separate sealed outer envelope marked "Original PROPOSAL". In addition, the Proposer shall submit copies of the Proposal in the number specified in the PDS.

Copies of the Technical Part shall be placed in a separate sealed envelope marked "COPIES: TECHNICAL PART". Copies of the Financial Part shall be placed in a separate sealed envelope marked "COPIES: FINANCIAL PART". The Proposer shall place both of these envelopes in a separate, sealed outer envelope marked "PROPOSAL COPIES". In the event of any discrepancy between the original and the copies, the original shall prevail.

22.2. If alternative Proposals are permitted in accordance with ITP 14, the alternative Proposals shall be submitted as follows: the original of the alternative Proposal Technical Part shall be placed in a sealed envelope marked "ALTERNATIVE PROPOSAL – TECHNICAL PART" and the Financial Part shall be placed in a sealed envelope marked "ALTERNATIVE PROPOSAL – FINANCIAL PART" and these two separate sealed envelopes then enclosed within a sealed outer envelope marked "ALTERNATIVE PROPOSAL – ORIGINAL", the copies of the alternative Proposal will be placed in separate sealed envelopes marked "ALTERNATIVE PROPOSAL – COPIES OF TECHNICAL PART", and "ALTERNATIVE PROPOSAL – COPIES OF FINANCIAL PART" and enclosed in a separate sealed outer envelope marked "ALTERNATIVE PROPOSAL - COPIES.

22.3. The envelopes marked "ORIGINAL PROPOSAL" and "PROPOSAL COPIES" (and, if appropriate, a third envelope marked "ALTERNATIVE PROPOSAL") shall be enclosed in a separate sealed outer envelope for submission to the Purchaser.

22.4. The inner and outer envelopes shall:

(a) bear the name and address of the Proposer;

(b) be addressed to the Purchaser in accordance with ITP 23.1;

(c) bear the specific identification of this request for proposals process indicated in accordance with ITP 1.1; and

(d) bear a warning not to open before the time and date for Proposal opening.

22.5. If all envelopes are not sealed and marked as required, the Purchaser will assume no responsibility for the misplacement or premature opening of the Proposal.

23. Deadline for Submission of Proposals

23.1. Proposals must be received by the Purchaser at the address and no later than the date and time indicated in the PDS. When so specified in the PDS, Proposers shall have the option of submitting their Proposals electronically. Proposers submitting Proposals electronically shall follow the electronic Proposal submission procedures specified in the PDS.

23.2. The Purchaser may, at its discretion, extend this deadline for submission of Proposals by amending the request for proposals documents in accordance with ITP 8, in which case all rights and obligations of the Purchaser and Proposers will thereafter be subject to the deadline as extended.

24. Late Proposals

24.1. The Purchaser shall not consider any Proposal that arrives after the deadline for submission of Proposals, in accordance with ITP 23. Any Proposal received by the Purchaser after the deadline for submission of Proposals shall be declared late, rejected, and returned unopened to the Proposer.

25. Withdrawal, Substitution, and Modification of Proposals

25.1. A Proposer may withdraw, substitute, or modify its Proposal 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 ITP 21.3, (except that withdrawal notices do not require copies). The corresponding substitution or modification of the Proposal must accompany the respective written notice. All notices must be:

(a) prepared and submitted in accordance with ITP 21 and ITP 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 Purchaser prior to the deadline prescribed for submission of Proposals, in accordance with ITP 23.

25.2. Proposals requested to be withdrawn in accordance with ITP 25.1 shall be returned unopened to the Proposers.

No Proposal may be withdrawn, substituted, or modified in the interval between the deadline for submission of Proposals and the date of expiry of the Proposal validity specified by the Proposer on the Letter of Proposal or any extended date thereof.

E. PUBLIC OPENING OF TECHNICAL PARTS OF PROPOSALS

26. Public Opening of Technical Parts of Proposals

26.1. Except as in the cases specified in ITP 24 and ITP 25.2, the Purchaser shall conduct the Proposal opening in public, in the presence of Proposers` designated representatives and anyone who chooses to attend, and at the address, date and time specified in the PDS. Any specific electronic Proposal opening procedures required if electronic submission of proposals is permitted in accordance with ITP 23.1, shall be as specified in the PDS.

26.2. First, envelopes marked "Withdrawal" shall be opened and read out and the envelope with the corresponding Proposal shall not be opened but returned to the Proposer. No Proposal withdrawal shall be permitted unless the corresponding withdrawal notice contains a valid authorization to request the withdrawal and is read out at Proposal opening.

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

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

26.5. Next, all other envelopes marked "Technical Part" shall be opened one at a time. All envelopes marked "Second Envelope: Financial Part" shall remain sealed and kept by the Purchaser in safe custody until they are opened at a later public opening, following the evaluation of the Technical Part parts of the Proposals. On opening the envelopes marked "Technical Part" the Purchaser shall read out: the name of the Proposer, the presence or the absence of a Proposal Security, or Proposal-Securing Declaration, if required, and whether there is a modification; and Alternative Proposal - Technical Part; and any other details as the Purchaser may consider appropriate.

26.6. Only Technical Parts of Proposals and Alternative Proposal - Technical Parts that are read out at Proposal opening shall be considered further for evaluation. The Letter of Proposal-Technical Part and the separate sealed envelope marked "Second

Envelope: Financial Part" are to be initialed by representatives of the Purchaser attending Proposal opening in the manner specified in the PDS.

26.7. The Purchaser shall neither discuss the merits of any Proposal nor reject any Proposal (except for late Proposals, in accordance with ITP 24.1).

26.8. The Purchaser shall prepare a record of the Proposal opening that shall include, as a minimum:

(a) the name of the Proposer and whether there is a withdrawal, substitution, or modification;

(b) any alternative Proposals; and

(c) the presence or absence of a Proposal Security.

26.9. The Proposers' representatives who are present shall be requested to sign the record. The omission of a Proposer's signature on the record shall not invalidate the contents and effect of the record. A copy of the record shall be distributed to all Proposers.

F. EVALUATION OF PROPOSALS- GENERAL PROVISIONS

27. Confidentiality

27.1. Information relating to the evaluation of the Technical Part shall not be disclosed to Proposers or any other persons not officially concerned with the procurement process until the notification of evaluation of the Technical Part in accordance with ITP 33. Information relating to the evaluation of Financial Part, the evaluation of combined Technical Part and Financial Part, and recommendation of contract award shall not be disclosed to Proposers or any other persons not officially concerned with the RFP process until the Notification of Intention to Award the Contract is transmitted to Proposers in accordance with ITP 42ProposerProposer.

27.2. Any effort by a Proposer to influence the Purchaser in the evaluation of the Proposals or Contract award decisions may result in the rejection of its Proposal.

27.3. Notwithstanding ITP 27.2, from the time of Proposal opening to the time of Contract award, if any Proposer wishes to contact the Purchaser on any matter related to the procurement process, it should do so in writing.

28. Clarification of Proposals

28.1. To assist in the examination, evaluation, and comparison of the Proposals, and qualification of the Proposers, the Purchaser may, at its discretion, ask any Proposer for a clarification of its Proposal. Any clarification submitted by a Proposer that is not in response to a request by the Purchaser shall not be considered. The Purchaser's request for clarification and the response shall be in writing. No change in the prices or substance of the Proposal shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the Purchaser in the evaluation of the Proposals, in accordance with ITP 35.

28.2. If a Proposer does not provide clarifications of its Proposal by the date and time set in the Purchaser's request for clarification, its Proposal may be rejected.

29. Deviations, Reservations, and Omissions

29.1. During the evaluation of Proposals, the following definitions apply:

(a) "Deviation" is a departure from the requirements specified in the request for proposals document;

(b) "Reservation" is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the request for proposals document; and

(c) "Omission" is the failure to submit part or all of the information or documentation required in the request for proposals document.

29.2. Provided that a Proposal is substantially responsive, the Purchaser may waive any nonmaterial nonconformities in the Proposal.

Provided that a Proposal is substantially responsive, the Purchaser may request that the Proposer submit the necessary information or documentation, within a reasonable period of time, to rectify nonmaterial nonconformities in the Proposal related to documentation requirements. Requesting information or documentation on such nonconformities shall not be related to any aspect of the price of the Proposal. Failure of the Proposer to comply with the request may result in the rejection of its Proposal.

Official Use Only

G. EVALUATION OF TECHNICAL PART OF PROPOSALS

30. Determination of Responsiveness

30.1. The Purchaser's determination of the Technical Part's responsiveness shall be based on the contents of the Proposal, as specified in ITP 11.

30.2. Preliminary examination of the Technical Part shall be carried out to identify proposals that are incomplete, invalid or substantially nonresponsive to the requirements of the request for proposals documents. A substantially responsive Proposal is one that materially confirms to the requirements of the request for proposals 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 Works specified in the Contract; or

(ii) limit in any substantial way, inconsistent with the request for proposals document, the Purchaser's rights or the Proposer's obligations under the proposed Contract;or

(iii)limit in any substantial way, inconsistent with the request for proposals document, the Purchaser's rights or the Proposer's obligations under the proposed Contract; or

(b) if rectified, would unfairly affect the competitive position of other Proposers presenting substantially responsive Proposals.

30.3. If the Technical Part is not substantially responsive to the requirements of the request for proposals document, it shall be rejected by the Purchaser and may not subsequently be made responsive by correction of the material deviation, reservation, or omission.

31. Eligibility and Qualifications of the Proposer

31.1. The Purchaser shall determine to its satisfaction whether the Proposers that have been assessed to have submitted substantially responsive Proposals are eligible, and either continue to meet (if prequalification applies) or meet (if prequalification has not been carried out), the qualifying criteria specified in Section III, Evaluation and Qualification Criteria.

31.2. The determination shall be based upon an examination of the documentary evidence of the Proposer's eligibility and

qualifications submitted by the Proposer, pursuant to ITP 15. The determination shall not take into consideration the qualifications of other firms such as the Proposer's subsidiaries, parent entities, affiliates, subcontractors (other than Specialized Subcontractors if permitted in the request for proposals document), or any other firm.

31.3. Prior to Contract award, the Purchaser will verify that the successful Proposer (including each member of a JV) is not disqualified by the Bank due to noncompliance with contractual SEA/SH prevention and response obligations. The Purchaser will conduct the same verification for each subcontractor proposed by the successful Proposer. If any proposed subcontractor does not meet the requirement, the Purchaser will require the Proposer to propose a replacement subcontractor.

31.4. Only substantially responsive Proposals submitted by eligible and qualified Proposers shall proceed to the detailed technical evaluation specified in ITP 32.

31.5. The Purchaser's evaluation of Technical Part will be carried out as specified in Section III, Evaluation and Qualification Criteria.

32. Detailed Evaluation of Technical Part

32.1. The scores and weightings to be given to Rated Criteria (including technical and non-price factors and sub factors) are specified in the PDS.

H. NOTIFICATION OF EVALUATION OF TECHNICAL PARTS AND PUBLIC OPENING OF FINANCIAL PARTS

33. Notification of Evaluation of Technical Parts and Public Opening of Financial Parts

33.1. Following the completion of the evaluation of the Technical Parts of the Proposals, the Purchaser shall notify in writing those Proposers whose Proposals were considered substantially non-responsive to the request for proposals document or failed to meet the eligibility and qualification requirements, advising them of the following information:

(a) the grounds on which their Technical Part of Proposal failed to meet the requirements of the request for proposals document;

(b) their envelopes marked "SECOND ENVELOPE: FINANCIAL PART" will be returned to them unopened after the completion of the selection process and the signing of the Contract; and

(c) Option 1: when BAFO or negotiations is not to be applied notify them of the date, time and location of the public opening of the envelopes marked 'Financial Part", or;

Option 2: **when BAFO or negotiations apply as specified in the PDS,** notify them that: (i) the envelopes marked 'Financial Part' will not be opened in public, but in the presence of a probity auditor appointed by the Purchaser, and that (ii) the announcement of the names of the Proposers whose Financial Parts will be opened and the total Proposal prices will be deferred to the time that the Notification of Intention to Award the contract is issued.

33.2. The Purchaser shall, simultaneously, notify in writing those Proposers whose Technical Part have been evaluated as substantially responsive to the request for proposals document and met the eligibility and qualification requirements, advising them of the following information:

33.3. their Proposal has been evaluated as substantially responsive to the request for proposals document and met the eligibility and qualification requirements;

33.4. Option 1: when BAFO or negotiations is not to be applied notify them of the date, time and location of the public opening of the envelopes marked 'Financial Part", or;

Option 2: when BAFO or negotiations apply as specified in the PDS, notify them that: (i) the envelopes marked 'Financial Part' will not be opened in public, but in the presence of a probity auditor appointed by the Purchaser, and that (ii) the announcement of the names of the Proposers whose Financial Parts will be opened and the total Proposal prices will be deferred to the time that the Notification of Intention to Award the contract is issued**.**

33.5. When BAFO or negotiations do not apply as specified in the PDS, the Financial Part of the Proposal shall be opened publicly in the presence of Proposers' designated representatives and anyone who chooses to attend.

33.6. The opening date shall be not less than ten (10) Business Days from the date of notification of the results of the technical evaluation, specified in ITP 33.1 and 33.2. However, if the Purchaser receives a complaint on the results of the technical evaluation within the ten (10) Business Days, the opening date shall be subject to ITP 50.1.

33.7. At this public opening, the Financial Parts will be opened by the Purchaser in the presence of Proposers, or their designated representatives and anyone else who chooses to attend. Proposers who met the eligibility and qualification requirements and whose Proposals were evaluated as substantially responsive will have their envelopes marked "SECOND ENVELOPE: FINANCIAL PART" opened at the second public opening. Each of these envelopes marked "SECOND ENVELOPE: FINANCIAL PART" shall be inspected to confirm that they have remained sealed and unopened. These envelopes shall then be opened by the Purchaser. The Purchaser shall read out the names of each Proposer, the technical score and the total Proposal prices, in this contract, including any discounts and Alternative Proposal - Financial Part, and any other details as the Purchaser may consider appropriate.

33.8. Only envelopes of Financial Part of Proposals, Financial Parts of Alternative Proposals and discounts that are opened and read out at Proposal opening shall be considered further for evaluation. The Letter of Proposal – Financial Part and the Price Schedules are to be initialed by a representative of the Purchaser attending the Proposal opening in the manner specified in the PDS.

33.9. The Purchaser shall neither discuss the merits of any Proposal nor reject any envelopes marked "SECOND ENVELOPE: FINANCIAL PART" at this public opening.

33.10. The Purchaser shall prepare a record of the Financial Part of the Proposal opening that shall include, as a minimum: (a) the name of the Proposer whose Financial Part was opened; (b) the Proposal price, per lot (contract) if applicable, including any discounts; and (c) if applicable, any Alternative Proposal – Financial Part.

33.11. The Proposers whose envelopes marked "SECOND ENVELOPE: FINANCIAL PART" have been opened or their representatives who are present shall be requested to sign the record. The omission of a Proposer's signature on the record shall not invalidate the contents and effect of the record. A copy of the record shall be distributed to all Proposers.

33.12. When, as specified in the PDS, BAFO or negotiations apply the Financial Parts will not be opened in public and will be opened in the presence of a probity auditor appointed by the Purchaser.

33.13. At the opening each of the envelopes marked "Financial Part" shall be inspected to confirm that they have remained sealed and unopened. These envelopes shall then be opened by the Purchaser. The Purchaser shall record the names of each Proposer, and the total Proposal prices and any other details as the Purchaser may consider appropriate. The Letter of Proposal - Financial Part and

the Price Schedules are to be initialed by a representative of the Purchaser attending the opening and by the probity auditor.

33.14. The Purchaser shall prepare a record of the opening of the Financial Part envelopes that shall include, as a minimum:

(a) the name of the Proposers whose Financial Part was opened;

(b) the Proposal prices including any discounts. and

(c) The Probity Auditor's report of the opening of the Financial Part.

33.15. The probity auditor shall sign the record. The contents of the envelopes marked 'Financial Part' and the record of the opening shall be kept in safe custody by the Purchaser and not disclosed to anyone until the time of the transmission of the Notification of Intention to Award the contract.

I. EVALUATION OF FINANCIAL PART OF PROPOSALS

34. Adjustments for Non-material Noconformities

34.1. Provided that a Proposal is substantially responsive, the Purchaser shall rectify quantifiable nonmaterial nonconformities related to the Proposal Price. To this effect, the Proposal Price shall be adjusted, for comparison purposes only, to reflect the price of a missing or non-conforming item or component by adding the average price of the item or component quoted by substantially responsive Proposers. If the price of the item or component cannot be derived from the price of other substantially responsive Proposers, the Purchaser shall use its best estimate.

35. Correction of Arithmetic Errors

35.1. In evaluating the Financial Part of each Proposal, the Purchaser shall correct arithmetical errors on the following basis:

(a) where there are errors between the total of the amounts given under the column for the price breakdown and the amount given under the Total Price, the former shall prevail and the latter will be corrected accordingly;

(b) where there are errors between the total of the amounts of Schedule Nos. 1 to 5 and the amount given in Schedule No. 6 (Grand Summary), the former shall prevail and the latter will be corrected accordingly; 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 subject to (a) and (b) above.

Official Use Only

35.2. Proposers shall be requested to accept correction of arithmetical errors. Failure to accept the correction in accordance with ITP 35.1, shall result in the rejection of the Proposal.

36. Evaluation of Proposals Financial Part

36.1. To evaluate the Financial Part, the Purchaser shall consider the following:

(a) the Proposal price, excluding provisional sums and the provision, if any, for contingencies in the Price Schedules;

(b) price adjustment for correction of arithmetic errors in accordance with ITP 35.1;

(c) price adjustment due to discounts offered in accordance with ITP 26;

(d) price adjustment due to quantifiable nonmaterial nonconformities in accordance with ITP 34.1;

(e) converting the amount resulting from applying (a) to (c) above, if relevant, to a single currency in accordance with ITP 36.2; and

(f) the evaluation factors indicated in the PDS and detailed in Section III, Evaluation and Qualification Criteria.

36.2. For evaluation and comparison purposes, the currency(ies) of the **Proposal** shall be converted into a single currency **as specified in the PDS**.

36.3. No margin of domestic preference shall apply**.**

36.4. If price adjustment is allowed in accordance with ITP 17.7, 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 taken into account in Proposal evaluation.

36.5. The Purchaser will evaluate and compare the Proposals. The evaluation will be performed assuming either that:

Official Use Only

(a) the Contract will be awarded to the Most Advantageous Proposal for the entire Information System; or

(b) if specified **in the PDS**, Contracts will be awarded to the Proposers for each individual Subsystem, or slice defined in the Technical Requirements whose Proposals result in the Most Advantageous Proposal/Proposals for the entire System.

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

37. Abnormally Low Proposals

37.1. An Abnormally Low Proposal is one where the Proposal price in combination with other constituent elements of the Proposal appears unreasonably low to the extent that the Proposal price raises material concerns as to the capability of the Proposer to perform the Contract for the offered Proposal Price.

37.2. In the event of identification of a potentially Abnormally Low Proposal, the Purchaser shall seek written clarifications from the Proposer, including detailed price analyses of its Proposal 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 request for proposals document.

37.3. After evaluation of the price analyses, in the event that the Purchaser determines that the Proposer has failed to demonstrate its capability to perform the Contract for the offered Proposal Price, the Purchaser shall reject the Proposal.

38. Unbalanced or Front Loaded Proposals

38.1. If the Proposal that is evaluated as the lowest evaluated cost is, in the Purchaser's opinion, seriously unbalanced or front loaded the Purchaser may require the Proposer to provide written clarifications. Clarifications may include detailed price analyses to demonstrate the consistency of the Proposal prices with the scope of information systems, installations, proposed methodology, schedule and any other requirements of the request for proposals document.

38.2. After the evaluation of the information and detailed price analyses presented by the Proposer, the Purchaser may:

(a) accept the Proposal; or

(b) if appropriate, require that the total amount of the Performance Security be increased, at the expense of the Proposer, to a level not exceeding twenty percent (20%) of the Contract Price; or

(c) reject the Proposal.

J. Evaluation of Combined Technical and Financial Parts, Most Advantageous Proposal And Notification of Intention To Award

39. Evaluation of combined Technical and Financial Parts, Most Advantageous Proposal

39.1. The Purchaser's evaluation of responsive Proposals will take into account technical factors, in addition to cost factors in accordance with Section III Evaluation and Qualification Criteria. The weight to be assigned for the Technical factors and cost is specified in the PDS. The Purchaser will rank the Proposals based on the evaluated Proposal score (B).

39.2. Best and Final Offer (BAFO): After completion of the combined technical and financial evaluation of proposals, If specified in the PDS, the Purchaser may invite those Proposers to submit their BAFOs. The procedure for submitting BAFOs will be specified in the PDS. BAFO is a final opportunity for Proposers to improve their Proposals without changing the specified business function and performance requirements in accordance with the invitation to Submit Second Stage Combined Technical and Financial Proposals, Proposers are not obliged to submit a BAFO. Where BAFO is used there will be no negotiation after BAFO**.**

39.3. BAFO will apply a two envelope procurement process. The submission of BAFOs, opening of the Technical Parts and Financial Parts and the evaluation of Proposals will follow the procedures described for the Technical, Financial and Combined evaluation above, as appropriate**.**

39.4. The Purchaser shall determine the Most Advantageous Proposal. The Most Advantageous Proposal is the Proposal of the Proposer that meets the Qualification Criteria and whose Proposal has been determined to be substantially responsive to the request for proposals document and is the Proposal with the highest combined technical and financial score.

39.5. If specified in the PDS, the Purchaser may conduct negotiations following the evaluation of the proposals and before the final

contract award. The procedure of the negotiations will be specified in the PDS.

39.6. Negotiations shall be held in the presence of probity auditor appointed by the Purchaser.

39.7. Negotiations may address any aspect of the contract so long as they do not materially change the specified business function and performance requirements.

39.8. The Purchaser may negotiate first with the Proposer that has the Most Advantageous Proposal. If the negotiations are unsuccessful the Purchaser may negotiate with the Proposer that has the next best Most Advantageous Proposal, and so on down the list until a successful negotiated outcome is achieved.

39.9. Unless otherwise specified in the PDS, the Purchaser will NOT carry out tests prior to Contract award, 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 PDS the Purchaser may carry out such tests as detailed in the PDS.

39.10. Proposer.

39.11. Prior to Contract award, the Purchaser may carry out visits or interviews with the Proposer's clients referenced in its Proposal and site inspections.

39.12. The capabilities of the manufacturers and subcontractors proposed by the Proposer that is determined to have offered the Most Advantageous Proposal 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 letter of intent between the parties, as needed. Should a manufacturer or subcontractor be determined to be unacceptable, the Proposal will not be rejected, but the Proposer will be required to substitute an acceptable manufacturer or subcontractor without any change to the Proposal 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.

40. Purchaser's Right to Accept Any Proposal, and to Reject Any or All Proposals

40.1. The Purchaser reserves the right to accept or reject any Proposal, and to annul the procurement process and reject all Proposals at any time prior to contract award, without thereby incurring any liability to Proposers. In case of annulment, all Proposals submitted and specifically, Proposal securities, shall be promptly returned to the Proposers.

41. Standstill Period

41.1. The Contract shall not be awarded earlier than the expiry of the Standstill Period. The Standstill Period shall be ten (10) Business Days unless extended in accordance with ITP 46. The Standstill Period commences the day after the date the Purchaser has transmitted to each Proposer the Notification of Intention to Award the Contract. Where only one Proposal is submitted, or if this contract is in response to an emergency situation recognized by the Bank, the Standstill Period shall not apply.

42. Notification of Intention to Award

42.1. The Purchaser shall send to each Proposer the Notification of Intention to Award the Contract to the successful Proposer. The Notification of Intention to Award shall contain, at a minimum, the following information:

(a) the name and address of the Proposer submitting the successful Proposal;

(b) the Contract price of the successful Proposal;

(c) the total combined score of the successful Proposal;

(d) the names of all Proposers who submitted Proposals, and their Proposal prices as readout and as evaluated prices and technical scores;

(e) a statement of the reason(s) the Proposal (of the unsuccessful Proposer to whom the notification is addressed) was unsuccessful;

(f) the expiry date of the Standstill Period; and

(g) instructions on how to request a debriefing or submit a complaint during the standstill period;

K. AWARD OF CONTRACT

43. Award Criteria

43.1. Subject to ITP 40, the Purchaser shall award the Contract to the successful Proposer. This is the Proposer whose Proposal has been determined to be the Most Advantageous Proposal..

Proposer.

44. Purchaser's Right to Vary Quantities at Time of Award

44.1. The Purchaser reserves the right at the time of Contract award to increase or decrease, by the percentage(s) for items as indicated in the PDS.

45. Notification of Award

45.1. Prior to the date of expiry of the Proposal validity and upon expiry of the Standstill Period, specified in ITP 41.1 or any extension thereof, and, upon satisfactorily addressing any complaint that has been filed within the Standstill Period, the Purchaser shall notify the successful Proposer, in writing, that its Proposal has been accepted. The notification letter (hereinafter and in the Contract Forms called the "Letter of Acceptance") shall specify the sum that the Purchaser will pay the Supplier in consideration of the execution of the Contract (hereinafter and in the Conditions of Contract and Contract Forms called "the Contract Price").

45.2. Within ten (10) Business days after the date of transmission of the Letter of Acceptance, the Purchaser shall publish the Contract Award Notice which shall contain, at a minimum, the following information:

(a) name and address of the Purchaser;

(b) name and reference number of the contract being awarded, and the selection method used;

(c) names of all Proposers that submitted Proposals, and their Proposal prices as read out at Proposal opening, and as evaluated;

(d) name of Proposers whose Proposals were rejected and the reasons for their rejection;

(e) the name of the successful Proposer, the final total contract price, the contract duration and a summary of its scope; and

(f) successful Proposer's Beneficial Ownership Disclosure Form.

45.3. The Contract Award Notice shall be published on the Purchaser's website with free access if available, or in at least one newspaper of national circulation in the Purchaser's Country, or in the official gazette.

45.4. Until a formal contract is prepared and executed, the Notification of Award shall constitute a binding Contract.

46. Debriefing by the Purchaser

46.1. On receipt of the Purchaser's Notification of Intention to Award referred to in ITP 42, an unsuccessful Proposer has three (3) Business Days to make a written request to the Purchaser for a debriefing. The Purchaser shall provide a debriefing to all unsuccessful Proposers whose request is received within this deadline.

46.2. Where a request for debriefing is received within the deadline, the Purchaser shall provide a debriefing within five (5) Business Days, unless the Purchaser decides, for justifiable reasons, to provide the debriefing outside this timeframe. In that case, the standstill period shall automatically be extended until five (5) Business Days after such debriefing is provided. If more than one debriefing is so delayed, the standstill period shall not end earlier than five (5) Business Days after the last debriefing takes place. The Purchaser shall promptly inform, by the quickest means available, all Proposers of the extended standstill period.

46.3. Where a request for debriefing is received by the Purchaser later than the three (3) Business Day deadline, the Purchaser should provide the debriefing as soon as practicable, and normally no later than fifteen (15) Business Days from the date of publication of Public Notice of Award of contract. Requests for debriefing received outside the three (3)-day deadline shall not lead to extension of the standstill period.

46.4. Debriefings of unsuccessful Proposers may be done in writing or verbally. The Proposer shall bear their own costs of attending such a debriefing meeting.

47. Signing of Contract

47.1. The Purchaser shall send to the successful Proposer the Letter of Acceptance including the Contract Agreement, and a request to submit the Beneficial Ownership Disclosure Form providing additional information on its beneficial ownership. The Beneficial Ownership Disclosure Form shall be submitted within eight (8) Business Days of receiving this request.

47.2. The successful Proposer shall sign, date and return to the Purchaser, the Contract Agreement within twenty-eight (28) days of its receipt.

47.3. Notwithstanding ITP 47.2 above, in case signing of the Contract Agreement is prevented by any export restrictions attributable to the Purchaser, to the country of the Purchaser, 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 Proposer shall not be bound by its Proposal, always provided, however, that the Proposer can demonstrate to the satisfaction of the Purchaser and of the Bank that signing of the Contract Agreement has not been prevented by any lack of diligence on the part of the Proposer in completing any formalities, including applying for permits, authorizations and licenses

Official Use Only

necessary for the export of the Information System under the terms of the Contract.

48. Performance Security

48.1. Within twenty-eight (28) days of the receipt of the Letter of Acceptance from the Purchaser, the successful Proposer shall furnish the performance security in accordance with the General Conditions, subject to ITP 38.2 (b), using for that purpose the Performance Security Form included in Section X, Contract Forms, or another form acceptable to the Purchaser. If the Performance Security furnished by the successful Proposer is in the form of a bond, it shall be issued by a bonding or insurance company that has been determined by the successful Proposer to be acceptable to the Purchaser. A foreign institution providing a Performance Security shall have a correspondent financial institution located in the Purchaser's Country.

48.2. Failure of the successful Proposer 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 Proposal Security. In that event the Purchaser may award the Contract to the Proposer offering the next Most Advantageous Proposal.

49. Adjudicator

49.1. Unless the PDS states otherwise, the Purchaser proposes that the person named in the PDS 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 PDS. The proposed hourly fee for the Adjudicator is specified in the PDS. The expenses that would be considered reimbursable to the Adjudicator are also specified in the PDS. If a Proposer does not accept the Adjudicator proposed by the Purchaser, it should state its non-acceptance in its Proposal Form and make a counterproposal of an Adjudicator and an hourly fee, attaching a résumé of the alternative. If the successful Proposer and the Adjudicator nominated in the PDS happen to be from the same country, and this is not the country of the Purchaser too, the Purchaser reserves the right to cancel the Adjudicator nominated in the PDS and propose a new one. If by the day the Contract is signed, the Purchaser and the successful Proposer 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

Official Use Only

Authority is specified there, the Contract will be implemented without an Adjudicator.

50. Procurement Related Complaint

50.1. The procedures for making a Procurement-related Complaint are as specified in the PDS.

SECTION II - PROPOSAL DATA SHEET (PDS)

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

ITP Reference	A. General
ITP 1.1	The reference number of the Request for Proposals is: **KE-ICTA-571743-NC-RFP** The Purchaser is: **The Information and Communications Technology Authority** The name of the RFP is: **Supply, Delivery, Integration, Support, Capacity Building and Maintenance Support of Hardware, Analysts Computer, Security Software and Technology tools, Support for ICTA's Government Security Operation Centre (GOVSOC)** This procurement is a single tender to be awarded as one contract
ITP 1.3 (a)	Electronic Procurement **shall not** be applicable to this procurement.
ITP 2.1	The Borrower is: **The Government of Kenya through the ICT Authority as the procuring entity** Loan or Financing Agreement amount: **USD. 390 Million** The name of the Project is: **Kenya Digital Economy Acceleration Project**
ITP 4.1	Maximum number of members in the JV shall be: **Two (2)**
ITP 4.5	A list of debarred firms and individuals is available on the Bank's external website: http://www.worldbank.org/debarr.
B. Request for proposals Document	
ITP 7.1	For Clarification of Proposal purposes only, the Purchaser's address is: Attention: **Deputy Director, Supply Chain Management** Address: **P.O. Box 27150-00100** Floor/ Room number: **12th Floor, Telposta Towers (ICT Authority offices; the GovSOC installation site is the 23rd Floor, Telposta Towers)** City: **Nairobi** ZIP Code: **Not Applicable**

Official Use Only

	Country: **Kenya** Telephone: **(+254) 20 667 6999** Facsimile number: **Not Applicable** Electronic mail address: **procurement@ict.go.ke** Requests for clarification should be received by the Purchaser no later than: **14 days prior to proposal submission deadline** Web page: **www.icta.go.ke / www.tenders.go.ke**
ITP 7.1	Web page: **www.icta.go.ke and www.tenders.go.ke**
ITP 7.4	A Pre-Proposal meeting will be held virtually on Wednesday, 2nd December 2026 at 10:00 am EAT. The virtual platform details and connection link will be provided to all registered bidders via email by Monday, 30th November 2026, 5:00 pm EAT. Address: **P.O. Box 27150-00100** Floor/ Room number: **12th Floor, Telposta Towers** City: **Nairobi** Country: **Kenya** A site visit conducted by the Purchaser ***shall not be*** organized.
C. Preparation of Proposals	
ITP 10.1	The language of the Proposal is: **English** All correspondence exchange shall be in **English** language. Language for translation of supporting documents and printed literature is **English**
ITP 11.2 (j)	The Proposer shall submit with its Proposal the following additional documents the Technical Part of its Proposal: ***The list of additional documents shall include the following:*** **1. Code of Conduct for Supplier's Personnel (ES)** The Proposer shall submit its Code of Conduct that will apply to the Supplier's Personnel (as defined in GCC Clause 1.1) employed in the execution of the Contract at the Project Site/s to ensure compliance with the Supplier's Environmental and/or Social obligations under the Contract, as applicable. The Proposer shall use for this purpose the Code of Conduct form provided in Section IV. No substantial modifications shall be made to this form, except that the

	Proposer may introduce additional requirements, including as necessary to take into account specific Contract issues/risks. **Management Strategies and Work Implementation Plans (MSIP) to manage the (ES) risks and Mobilization plan** **2. Stakeholder Engagement Plan** *Strategies for continuous stakeholder engagement with system users.* *Consultation processes to address users concerns.* *Feedback mechanisms for users to voice their risks and concerns.* **3. Training and Capacity Building Program** *Regular training sessions on health, safety, and environmental practices.* *Capacity-building initiatives for local workforce development.* *Mentorship programs for employees to improve skills and knowledge.* **4. Monitoring and EvaluationPlan** *Establish performance indicators to assess the effectiveness of all management strategies.* *Regular audits and assessments to ensure compliance with safety and environmental standards.* *Reporting frameworks to share results with stakeholders.* **5. Cyber security managementstrategies and implementation plans** The Proposer shall submit method statement, management strategies and implementation plans and innovations to manage cyber security risks.”
ITP 11.3(d)	The Proposer shall submit the following additional documents in the Financial Part of its Proposal: ***N/A***
ITP 13.1	**Alternative Proposals are not permitted**
ITP 13.2	Alternatives to the Time Schedule **are not** permitted. If alternatives to the Time Schedule are permitted, the evaluation method will be as specified in Section III, Evaluation and Qualification Criteria.
ITP 13.4	Alternative technical solutions shall be permitted for the following parts of the Information System: ***not applicable***
ITP 15.2	Prequalification **has not** been undertaken.
ITP 16.2 (a)	In addition to the topics described in ITP Clause 11.2.2 (a), the Preliminary Project Plan must address the following topics:

Official Use Only

	i. Project Organization and Management Sub-Plan, including management authorities, Key Contract Implementation Team and their Qualification/profile. responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format); *ii. Implementation Sub-Plan;* *iii. Change Management and risk management plan* *iv. Training Sub-Plan;* *v. Testing and Quality Assurance Sub-Plan;* *vi. Warranty Defect Repair and Technical Support Service Sub-Plan* *Certificate of registration by the Data Commissioner as per the requirement of Kenya's Data Protection Act (DPA)for both as a Data Processor and a Data Controller or equivalent from host country (for foreign bidding entities)* *vii. Valid ISO/IEC 27001:2022 certification, issued by an accredited certification body, covering the scope of services for Information Security Management Systems* *viii. An ISO 9001 certification in Quality Management Systems.* *ix. Quality certification documents, Data sheets and Technical Brochures along with the web links to proposed solutions and access over internet to the Datasheet.* *x. SOC II compliant, provide certificate, report to be provided upon the request by ICTA* *xi. Valid ICTA-1 Certificate for Data Center, Information Security , Cloud and System Applications. OR Equivalent from Host Country:* ***xii.** Hardware & Software Warranty for the Five years (The proposed Hardware should not be listed or declared to be going towards end of sale in five years – Provide OEM Data Sheets for Prove of this)*
ITP 16.3	• In the interest of effective integration, cost-effective technical support, and reduced re-training and staffing costs, Proposers shall offer the following items: • AS Build Training on SOC Operations. • Technical training Proposal. • The Bidder should provide licenses for a period of 5 years (fully prepaid/subscription covering all core modules • Cyber Security awareness training for MDA both in Virtual Set-up • Five(5) Year Support , Maintenance and Local professional support including 24x7x365 operations with Real-Time monitoring, Threat hunting, Threat detection, and incident handling response capabilities, (**Costed Separately).**
ITP 17.2	The Proposer **must** propose Recurrent Cost Items

ITP 17.2	The Proposer **must** propose for contracts for Recurrent Cost Items not included in the main Contract.
ITP 17.5	The Incoterms edition is: **Incoterm 2020**
ITP 17.5 (a)	Named place of destination is: **23rd Floor, Telposta Towers, Along Kenyatta Avenue, Nairobi, Kenya**
ITP 17.6	Named place of final destination (or Project site) is: **23rd Floor, Telposta Towers, Along Kenyatta Avenue, Nairobi, Kenya**
ITP 17.8	***There are no modifications to ITP 17.8***
ITP 17.9	The prices quoted by the Proposer **shall not** be subject to adjustment during the performance of the Contract.
ITP 18.1	The Proposer **is** required to quote in the currency of the Purchaser's Country the portion of the Proposal price that corresponds to expenditures incurred in that currency.
ITP 19.1	The Proposal shall be valid until: **7th June 2027**
ITP 19.3 (a)	The Proposal price shall be adjusted by the following factor(s): **Not Applicable**
ITP 20.1	A Proposal Security **shall be** required. The Proposal Security shall be in the form of (**Unconditional Bank Guarantee from a reputable bank)** in the form and content provided in **Section IV**-Bidding Forms valid for a period of at least 28 calendar days beyond the Proposal Validity Period. The amount and currency of the Proposal Security shall be **KES 10 Million (Kenya Shillings Ten Million Only) or Equivalent in a Freely Convertible Currency**
ITP 20.3 (d)	Other types of acceptable securities: **None**
ITP 20.9	Not Applicable
ITP 21.3	The written confirmation of authorization to sign on behalf of the Proposer shall consist of: **Power of Attorney** The Power of Attorney shall be drawn up by **Commissioner of Oaths** (or attested by a **Notary Public** for international bidders) and bear the legal stamp/seal.

Official Use Only

	If the Bidder is a Joint Venture (JV), the Power of Attorney shall be executed by all authorized partners/members of the JV, appointing a Lead Partner with authority to sign on behalf of the JV and bind all members legally
D. Submission and Opening of Proposals	
ITP 22.1	In addition to the original of the Proposal, the number of copies is: **Two (2) copies of the Technical** and **the original of the financial proposal** in a separate envelope. In addition, a Flash Drive shall be enclosed, containing the full copy of Technical Proposal in PDF format, with search and copy functions enabled in the technical part's envelope. **Important: electronic copy of financial Proposal shall be included only in the Financial Part' envelope.** In case of any discrepancy between electronic copy, hard copies and original hard copy, the original hard copy shall prevail.
ITP 23.1	For Proposal submission purposes only, the Purchaser's address is: Attention: **Chief Executive Officer** Street Address: **Kenyatta Avenue** Floor/Room number: **12th Floor Boardroom** City: **Nairobi** Country: **Kenya** The deadline for Proposal submission is: Date: **7th January 2027** Time: **10:00am**
ITP 23.1	Proposers **shall not** have the option of submitting their Proposals electronically.
E. Public Opening of Technical Parts of Proposals	
ITP 26.1	The Proposal opening shall take place at: Street Address: **Kenyatta Avenue** Floor/Room number: **12th Floor Boardroom, ICT Authority** City: **Nairobi** Country: **Kenya** Date: **7th January 2027** Time: **10:00 am**
ITP 26.1	The electronic Proposal opening procedures shall be: **Not Applicable**
G. Evaluation of Technical Part of Proposals	

ITP 32.2	The weighting to be given for Rated Criteria (including technical and non-price factors) is: **80% or 0.8.** The Rated Criteria, sub-criteria, marks and scoring methodology are set out in **Section III, Evaluation and Qualification Criteria, Clause 2 – Consolidated Technical Scoring Matrix (100 points)**, which is the only technical scoring matrix applicable to this RFP. The minimum technical qualifying score is 70 points out of 100. **Technical Proposal Scoring Methodology** The evaluation of this bid shall be done in four stages, 1. **Mandatory (M) requirements of the Section VII functionality checklists – PASS/FAIL.** 2. **Rated criteria – scored in accordance with the Consolidated Technical Scoring Matrix in Section III.** 3. **Financial Proposals.** 4. **Proof of Concept of the Most Advantageous Proposal – PASS/FAIL, prior to Contract award (ITP 39.9 and Section III, Clause 6).**
H. Notification of Evaluation of Technical Parts and Public Opening of Financial Parts	
ITP 33.8	During the first opening session all representatives of the Purchaser shall initial the physical seals and flaps of the unopened Financial Envelopes to prevent unauthorized access, along with all key pages and signature pages of the opened Technical Proposal Submission Letter, any notices of modification or withdrawal, the original Proposal Security instrument, Powers of Attorney, Joint Venture agreements, and summary technical schedules or compliance forms. **Each Technical and Financial Proposal shall be numbered.**
I. Evaluation of Financial Part of Proposals	
36.1(f)	The adjustments shall be determined using the following criteria, from amongst those set out in Section III, Evaluation and Qualification Criteria: (a) Deviation in Time for Completion: **No** (b) Present value of Recurrent Costs **No** (c) Functional Guarantees of the Facilities **No** (d) Work, services, facilities, etc., to be provided by the Purchaser **No**
ITP 36.2	The currency(ies) of the Proposal shall be converted into a single currency as follows: **Kenya Shillings**

Official Use Only

	The currency that shall be used for Proposal evaluation and comparison purposes to convert all Proposal prices expressed in various currencies into a single currency is: **Kenya Shillings** The source of exchange rate shall be: **Central Bank of Kenya** The date for the exchange rate shall be: **Proposal Submission Deadline**
J. Evaluation of Combined Technical and Financial Parts and Most Advantageous Proposal	
ITP 39.1	The weight to be given for cost is: **20% OR 0.2** Discount Rate (I) for net present value calculations of recurrent costs (if any) is: Not Applicable.
ITP 39.2	BAFO **does not apply**
ITP 39.5	Negotiation does not apply
ITP 39.9	As additional qualification measures, the Information System (or components/parts of it) offered by the Proposer with the Most Advantageous Proposal shall be subjected to the following tests and performance benchmarks prior to Contract award: ***Proof of Concept (PoC) in accordance with Section III, Evaluation and Qualification Criteria, Clause 6, which sets out the PoC sequence, procedure, mandatory test scenarios, pass/fail criteria and the consequence of failure. A Proposal that fails the PoC shall be rejected and the Proposer with the next Most Advantageous Proposal shall be invited to the same PoC.***
K. AWARD OF CONTRACT	
ITP 44	The maximum percentage by which quantities may be increased is: **15 percent** The maximum percentage by which quantities may be decreased is: **15 percent** The items for which the Purchaser may increase of decrease the quantities are the following. **N/A**
ITP 49	The Appointing Authority for the Adjudicator is: The Registrar, **Nairobi Centre for International Arbitration** (NCIA) The hourly rate shall be determined in accordance with the prevailing fee schedule of the Nairobi Centre for International Arbitration (NCIA).
ITP 50.1	The procedures for making a Procurement-related Complaint are detailed in the "Procurement Regulations for IPF Borrowers (Annex III)." A Procurement-related Complaint may challenge any of the following: 1. The terms of the request for proposals document;

Official Use Only

	2. the Purchaser's decision to exclude a Proposer from the procurement process prior to the award of contract; and 3. The Purchaser's decision to award the contract. If a Proposer wishes to make a Procurement-related Complaint, the Proposer 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: **Jessy K. Maruti** Title/position: **Chief Executive Officer** Purchaser: **The Information and Communications Technology Authority** Email address*:* **info@icta.go.ke / procurement@ict.go.ke** Fax number: **Not Applicable** A copy of the complaint can be sent for the Bank's information and monitoring to: **pprocurementcomplaints@worldbank.org**

SECTION III - EVALUATION AND QUALIFICATION CRITERIA (WITHOUT PREQUALIFICATION)

This Section contains all the criteria that the Purchaser shall use to evaluate Proposals and qualify Proposers. No other factors, methods or criteria shall be used. The Proposer shall provide all the information requested in the forms included in Section IV, Proposal Forms.

1. Qualification

1.1 Qualification Requirements

The Proposer's qualification shall be assessed in accordance with the Qualification table included in this section.

1.2 Financial Resources

Using the relevant Form, FIN 1.3.3 in Section IV, Proposal Forms, the Proposer must demonstrate access to, or availability of, financial resources such as liquid assets, unencumbered real assets, lines of credit, and other financial means, other than any contractual advance payments to meet:

(i) the following cash-flow requirement:

and

(ii) the overall cash flow requirements for this contract and its current supply and services' commitment.

1.3 Key Personnel

The Proposer must demonstrate that it will have suitably qualified key personnel. The Proposer shall complete the relevant Forms in Section IV, Proposal Forms.

1.4 Subcontractors/vendors/manufacturers

Subcontractors/vendors/manufacturers for major items of supply or services identified in the prequalification document must meet or continue to meet the minimum criteria specified therein for each item.

Subcontractors for the following additional major items of supply or services must meet the following minimum criteria, herein listed for that item:

Official Use Only

Item No.	Description of Item	Minimum Criteria to be met
1		
2		
3		
…		

Failure to comply with this requirement will result in the rejection of the subcontractor.

1.5 Manufacturer's authorization

For all powered (active) hardware and/or software components of the Information System which the Proposer does not itself produce, by submission of documentary evidence in its Proposal, the Proposer must establish to the Purchaser's satisfaction that it is not prohibited to supply those components in the Purchaser's country under the Contract(s) that may result from this procurement. This comprise of hardware components including servers, cooling system, workstations, video wall systems and controller, UPS and software components including SIEM, SOAR, TIP and Anti-DDOS

(i) In the case of powered (active) hardware and other powered equipment, this must tbe documented by including Manufacturer's Authorizations in the Proposal (based on the sample found in the Sample Proposal Forms in Section IV.);

(ii) In the case of proprietary commercial software (i.e., excluding open source or "freeware" software) that the Proposer does not manufacture itself and for which the Proposer has or will establish an Original Equipment Manufacturer (OEM) relationship with the manufacturer, the Proposer must provide Manufacture's Authorizations;

(iii) In the case of proprietary commercial software (i.e., excluding open source or "freeware" software) that the Proposer does not manufacture itself and for which the Proposer does not or will not establish an OEM relationship with the manufacturer, the Proposer must document to the Purchaser's satisfaction that the Proposer is not excluded from sourcing these items from the manufacturer's distribution channels and proposing offering these items for supply in the Borrower's Country.

(iv) In the case of open source software, the Proposer must identify the software item as open source and provide copies of the relevant open source license(s).

The Proposer is responsible for ensuring that the manufacturer or producer complies with the requirements of ITP 4 and ITP 5 and meets the minimum criteria listed above for that item.

One OEM may authorize more than one proposer.

Official Use Only

1.6 Local Representative

In the case of a Proposer not doing business within the Purchaser's country, the Proposer shall submit documentary evidence in its Proposal to establish to the Purchaser's satisfaction that it is or will be (if awarded the Contract) represented by an agent in that country who is equipped and able to carry out / manage the Proposer's maintenance, technical support, training, Incidence Response Services and warranty repair obligations specified in the Purchaser's Requirements (including any response time, problem-resolution norms or other aspects that may be specified in the Contract).

2. Technical Evaluation

The Purchaser shall assess each Bid against the following Qualification Criteria. Requirements not included in the text below shall not be used in the evaluation of the Bidder's qualifications.

(a) **Financial Capability**: The Bidder shall submit audited financial statements or, if not required by the law of the Bidder's country, other financial statements acceptable to the Purchaser, for the last **Three (3)** years (2023, 2024 and 2025, or the financial years 2022/2023, 2023/2024 and 2024/2025 where the Proposer's financial year does not coincide with the calendar year) prior to bid submission deadline, demonstrating the current soundness of the Bidder's financial position. For a joint venture, this requirement MUST be met by each member.

(i) Specific Experience: The Bidder shall demonstrate that it has successfully completed at least **T**wo **(**2) contracts within the last **Five (5) years** prior to bid submission deadline, each with a value of at least **Kes. 100 million or equivalent** that have been successfully and substantially completed and that are similar in nature and complexity to the Contract for the delivery Supply, Delivery, Installation of Technology, Configuration & Commissioning of a Security Operation Center- SOC. For a joint venture, this requirement **MUST** be met by all members.

(iii) Minimum Average Annual turnover of **Kenya Shillings 300,000,000** Or equivalent calculated as total certified payments received for contracts in progress or completed, averaged over the same three (3) years as the audited financial statements in (a) above

(b) **Documentary Evidence:** The Bidder shall furnish documentary evidence to demonstrate that the Goods it offers meet the following usage requirement: **as per the technical checklist in section Page 117** under Technical Specifications**.**

(c) As a Cybersecurity Risk practice, the Bidder MUST provide evidence of compliance w ith applicable data-protection legislation in its country of establishment and shall undertake to complete registration with the ODPC in Kenya before Contract signing, where registration is required by applicable Kenyan law.

(d) They will also prove availability of Certified Solution deployment engineers to execute the implementation of the proposed solution.

(e) **Manufacturing Experience and Technical Capacity**:

1. **Manufacturer's authorization**: A Bidder who does not manufacture an item/s where a manufacturer authorization is required in accordance with BDS ITB 17.2 (a), the Bidder

Official Use Only

shall provide a Manufacturer's Authorization Form, duly filled using th Form in Section IV and signed by the manufacturer, authorising the Bidder to supply, install, configure, commission, and provide warranty and after-sales support for the item(s) offered under the Bid

EVALUTION CRITERIA

The weighting to be given for Rated Criteria (including technical and non-price factors) is: ***0.8 OR 80%.***

Main Rated Criteria are:

i. Specified Hardware & GovSOC Software Performance requirements - **50 points**
ii. Company Profile, Organizational Proposal and Experience – **15 points**
iii. Key Contract Implementation Team (Deployment Staff) – 20 points
iv. GovSOC Retainer & Incident Response Team – 15 points

The rating will be as follows:

Consolidated Technical Scoring Matrix (100 points)

No.	Criterion / Sub-criterion	Marks
1	**Specified Hardware & GovSOC Software Performance Requirements**	**50**
1.1	**SOC Hardware & Devices (Table A)**	**25**
	• Modular Power Supply System (UPS): capacity 2.0; battery autonomy 2.0; efficiency & monitoring 1.0	5.0
	• SOC Analyst Workstations & Operations Floor: workstation computer 3.0; display setup 2.0; operations floor 2.0	7.0
	• Video Wall System (Display): display panels 6.0; reliability & warranty 1.0	7.0
	• Video Wall System (Controller & Management): controller & inputs 1.0; resilience & control 2.0	3.0
	• Remote Monitoring Supervisor Tablets: display & performance 1.0; security & device management 2.0	3.0
1.2	**Enterprise Security Software and Technology Tools (Table B)**	**25**
	• Phase I – Security Information & Event Management (SIEM)	6.2
	• Phase I – Security Orchestration, Automation and Response (SOAR)	6.0
	• Phase I – Anti-DDoS Solution	2.7
	• Phase I – Threat Intelligence Platform (TIP)	4.0
	• Phase II – File Integrity Monitoring (FIM)	2.4
	• Phase II – Advanced Attack Surface Management (ASM)	3.7
	• Sub-total Phase I = 18.9; Phase II = 6.1	
2	**Company Profile, Organizational Proposal and Experience (Table C)**	**15**
2.1	**Past experience in similar assignments**	**4.0**
2.2	**Training plan and package (scored by package tier, Table D)**	**2.5**
2.3	**Implementation plan, methodology and workplan**	**4.0**
2.4	**Proposed Service Level Agreement (SLA)**	**3.0**
2.5	**Company profile**	**1.5**
3	**Key Contract Implementation Team (Table C)**	**20**
3.1	**Project Manager (1)**	**4.0**

Official Use Only

3.2	Cyber-Security Engineers (2)	6.0
3.3	Integration Engineers (2)	4.5
3.4	Lead Enterprise Security Architect (1)	4.0
3.5	Network Engineer / Administrator (1)	1.5
4	GovSOC Retainer & Incident Response Team (Table C)	15
4.1	SOC Team Lead / Manager (1)	6.0
4.2	SOC Analysts (3), 3.0 marks per Analyst	9.0
	TOTAL TECHNICAL SCORE	100

Scoring methodology. Every sub-criterion above is scored by applying the multiplier for the level achieved, as described in the 50%, 75% and 100% columns of Tables A to D: significantly in excess of requirements (100% descriptor) – 100%; moderately in excess of requirements (75% descriptor) – 75%; meeting the minimum requirements (50% descriptor) – 50%; below the minimum requirements – 0%. Sub-criterion score = marks × multiplier. A candidate who does not meet the minimum educational qualification for a position receives zero (0) marks for that position.

Qualifying score. Proposals scoring at least 70 points out of 100 shall be considered technically responsive; only their Financial Parts shall be opened.

Single matrix. This Consolidated Technical Scoring Matrix, read with Tables A to D, is the only technical scoring matrix of this RFP. Mandatory (M) requirements in the Section VII checklists are assessed Pass/Fail before scoring; Desirable (D) requirements are reflected in the rated criteria above. The Proof of Concept (Clause 6) is Pass/Fail and does not change the technical score.

i. SOC Hardware & Devices – 25 Marks (Table A: scoring descriptors)

Equipment	Measurable Specifications	Minimum (Specification)	Marks	50%	75%	100%
Modular Power Supply System (UPS)	Capacity &	Online double-conversion; sized ≥125% of connected load	2.0	Online double-conversion, ≥125% of load	Modular, hot-swap, N+1	Modular N+1 with A+B feeds and ≥50% scalable growth
	Battery autonomy	≥30 min at full load	2.0	30 min	60 min	≥90 min, or ≥30 min with auto-start generator and ATS
	Efficiency & monitoring	Efficiency ≥94% at 50–100% load; SNMP monitoring	1.0	≥94%, SNMP monitoring	≥96%, battery health monitoring	≥97%, Li-ion batteries, full remote alerting, 24×7 support
SOC Analyst Workstations & Operations Floor	Workstation computer	Core i7 / Ryzen 7 class, 32 GB RAM, 1 TB SSD, TPM 2.0	3.0	i7-class, 32 GB, 1 TB SSD	i9-class, 64 GB, 1 TB NVMe	≥64 GB, ≥2 TB NVMe, discrete GPU, 5-yr on-site warranty
	Display setup per analyst	Dual 24" FHD (1920×1080) monitors	2.0	Dual 24" FHD	Dual 27" QHD	Triple 27" or dual 32" 4K,

						height-adjustable
	Operations floor, ergonomics & access security	≥4 m² per analyst; ergonomic desks; structured cabling; access control; CCTV	2.0	Minimum specification met	Adds sit-stand desks, KVM, acoustic treatment	Adds biometric/dual-factor access, CCTV coverage, tray/raised-floor cable management
Video Wall System (Display)	Display panels	Narrow-bezel 55" FHD LCD, ≥500 nits, bezel ≤3.5 mm, sized to floor design (e.g. 2×2 or larger)	6.0	FHD, ≥500 nits, bezel ≤3.5 mm	4K, ≥700 nits, bezel ≤1.8 mm	4K or fine-pitch LED (≤P1.2), ≥800 nits, seamless
	Reliability & warranty	24×7 rated; ≥50,000 hrs life; 3-yr on-site warranty	1.0	50,000 hrs, 3-yr warranty	60,000 hrs, 5-yr warranty	≥100,000 hrs, redundant PSU, 5-yr warranty
Video Wall System (Controller & Management)	Controller & inputs	Wall processor with ≥8 inputs (HDMI/DP/IP), multi-window, FHD/4K support	1.0	8 inputs, FHD	16 inputs, 4K	≥32 inputs, 4K60, IP decoding
	Resilience & control	Web/GUI layout management; preset layouts; RBAC	2.0	GUI control and preset layouts	Adds RBAC and redundant PSU	Adds hot-standby controller and SIEM/SOAR dashboard integration
Remote Monitoring Supervisor Tablets	Display & performance	10–11" FHD, 6 GB RAM, 128 GB storage, ≥8 hr battery	1.0	10", FHD, 6/128 GB, 8 hr	11", 8/256 GB, 10 hr	≥12", ≥8/256 GB, ≥12 hr, LTE/5G
	Security & device management	MDM enrolment; full-disk encryption; VPN; biometric/PIN lock	2.0	Encryption, MDM, VPN	Adds biometric, remote wipe, MFA	Adds per-app VPN, rugged rating (IP65+), 3-yr warranty
Total – SOC Hardware & Devices (Table A)						**25**

ii. Enterprise Security Software and Technology Tools (GovSOC) – 25 Marks

Security Software and Technology tools, Integration, Support, Capacity Building and Five-Year Maintenance Support. **25 Marks**

The scope includes enterprise-grade detection and response technologies enabling centralized monitoring, threat intelligence, attack mitigation, and integrity assurance across the ICT environment.

Phase 1: Core Operational GoVSOC Capability; and (ii)
Phase 2: Advanced Visibility and SOC Maturity Enhancement. Bidders shall structure their proposals, and implementation plans in accordance with this phased delivery model.

The phased implementation model is intended to establish an initial minimum viable operational GovSOC capability while enabling progressive deployment of advanced security visibility and maturity enhancement functions in subsequent stages	
Phase I: Core Operational GovSOC capability (SIEM, SOAR, TIP and Anti-DDoS	**18.9 Marks**
(i) **Security Information & Event Management (SIEM)** (sub-criterion marks and descriptors: Table B) a) Functional Capability to Log ingestion scale, correlation, UEBA, MITRE ATT&CK mapping, analytics depth b) Integration- Integration with SOAR, TIP, EDR/NDR, APIs, data normalization c) OEM Maturity- Market leadership, R&D, roadmap, threat research capability d) Support & Sustainability- Local support, SLAs, updates, training 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	**6.2 Marks**
(ii) **Security Orchestration, Automation, and Response (SOAR)** (sub-criterion marks and descriptors: Table B) a) Functional Capability Multi-Layer Playbooks: Ability to automate complex, multi-tool workflows (Cloud, On-prem, Identity). Effectiveness: Documented reduction in MTTR by >60% . Throughput: Processing >500000 events/second without latency. b) Integration: Universal Connectors: Out-of-the-box integration with the specific SIEM and Data Center stack mentioned; Open API for custom Python/PowerShell scripting. c) OEM Maturity Carrier-Grade: Evidence of deployment in National SOCs or Global Telcos with endpoints; d) Support & Sustainability: Local Presence support of: 24/7/365 L3 support engineers based in-country or within the same time zone;Remote support with contractually committed response times is an acceptable equivalent to on-site support, provided that the Proposer demonstrates compliance with all specified availability, response, escalation and service-level requirements.; quarterly playbook optimization audits included. 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	**6 Marks**
(iii) **Anti-DDoS Solution (sub-criterion marks and descriptors: Table B)** a) Functional Capability with Multi-layer detection, mitigation effectiveness, throughput, latency impact b) Integration with SIEM, SOC dashboards, API orchestration c) OEM Maturity with demonstrated experience delivering DDoS mitigation services to similar entities or critical national infrastructure operators, evidenced by reference contracts, case studies, or independent audit reports d) Support & Sustainability with 24/7 response, with support with contractually committed response times is an acceptable equivalent, 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	**2.7 Marks**
(iv) **Threat Intelligence Platform (TIP) (sub-criterion marks and descriptors: Table B)** a) Functional Capability with feed ingestion of STIX/TAXII, enrichment, scoring	

b) Integration with SIEM/SOAR integration, IOC automation, interoperability c) OEM Maturity with Quality of intel sources, global coverage d) Support & Sustainability on Feed updates, support model, training 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	**4 Marks**
Phase II: Advanced Visibility and maturity enhancement (FIM, ASM) 6.1 Marks	
(i) **File Integrity Monitoring (FIM) (sub-criterion marks and descriptors: Table B)** a) Functional Capability with Real-time monitoring, baselining, policy enforcement b) Integration with SIEM integration, alert forwarding c) OEM Maturity proven Stability, compliance alignment (e.g., ISO, PCI-DSS, HIPA d) Support & Sustainability with Updates, documentation, vendor support 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	**2.4 Marks**
(ii) **Advanced Attack Surface Management (ASM) (sub-criterion marks and descriptors: Table B)** a) Functional Capability Identifies "Shadow IT," forgotten subdomains, and leaked credentials. Mitigation: Provides actionable remediation steps for discovered vulnerabilities. Latency: Real-time scanning of the external perimeter (1.5 Marks) b) Integration Orchestration Ready: Integration with the SOAR tool (native or through documented APIs) to trigger an automatic "Scan" playbook when a new asset is discovered and is confirmed to belong to the government(1.0 Marks) c) OEM Maturity Global Reach: Utilizes a global distributed scanning network to see the organization from the outside in across different geographic regions (0.6 Marks) d) Support & Sustainability with 24/7 response, updates, local presence (0.6 Marks) 1) Significantly in excess of requirements - Multiplier of 100% 2) Moderately in excess of requirements - Multiplier of 75% percent 3) Meeting requirements - Multiplier of 50% percent Below requirements - Multiplier of 0 % Percent	**3.7 Marks**
1. Criterion 2 – Company Profile, Method Statement: Organizational Proposal and Experience of the Bidders' Capacity on services Delivery.	**15 Marks**
(ii) **Description and Organization of the Bidder (Assess the quality of the bidder's understanding and approach to implement the contract and associated services)** Past Experience in Previous Assignments and the nature and similarity of complexity of such assignments to this project Physical Set-up, Technology Supply, Delivery, Installation, Configuration Commissioning, Training, Support and Maintenance of an Security Operation Centre of similar nature The firm must have completed at Minimum; two (**2**) similar assignments of similar magnitude, similarity of complexity of the assignments to this project with Minimum Budget of **Kshs 100 Million** each that have been executed during the **last 5 years**. should be verified by submission of copies of completed contracts and acceptance certificate	**4 Marks**

Official Use Only

issued with the Employer/Client. Provide contact details, project details and company/organization. And Project Budget Provide evidence e.g., contracts/award letter/LPO, completion certificate/letter etc.). Also provide Contact Person, Telephone Number/Email). 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	
(iii) **The vendor/Bidder will provide a training plan/program strictly committed to a maximum of 6 months from day of Award. The training which should be on OEM approved training curriculum and certification for ICTA technical staff for at least 15 (Staff) in English language** Security Operation Centre within a Government Agency**, Optimization, configuration of the provided for solution & Managements in an OEM approved facility.** 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	**2.5 Marks**
(iv) **The Bidder MUST provide a project <u>implementation plan, Methodology, workplan</u> that outlines the bidders strategy in implementing and integrating and solution without adversely affecting GOK service with specific key Milestones. He will also provide Compliance** to Technical requirements **cross referencing to the relevant supporting information for entire Technical Specifications Section. The cross reference should document the relevant publicly accessible documents and sites where the details are located.:** 1. Significantly in excess of requirements - Multiplier of 100% 2. Moderately in excess of requirements - Multiplier of 75% percent 3. Meeting requirements - Multiplier of 50% percent 4. Below requirements - Multiplier of 0 % Percent	**4 Marks**
Proposed Service Level Agreement Completeness of Proposed Service Level Agreement (SLA) indicating Service Descriptions, Support requirements, Escalation matrix and contacts, and support engagement. To ensure clarity and enforceability, the SLA section will require bidders to include: ✓ Scope of covered services, including post-implementation support, maintenance, and incident management; ✓ Defined service desk and escalation structure with named contacts; ✓ Response time commitments for incident acknowledgement; and ✓ Resolution time targets based on severity classifications (e.g., critical, high, medium, low); and ✓ Procedures for monitoring, reporting, and service performance review. 1. Significantly in excess of requirements 2. Moderately in excess of requirements 3. Meeting requirements 4. Below requirements	**3 Marks**

(v) **Company Profile: The Bidder or Must provide an organization profile indicating Core business, Organogram, Mission and Leadership. No of years in existence and Proof of implementation of enterprise level IT Cyber security projects and OEM Partnership level** 1. Significantly in excess of requirements 2. Moderately in excess of requirements 3. Meeting requirements 4. Below requirements	**1.5 Marks**
2. Criterion 3 – Key Contract Implementation Team: Qualifications and competence of the key personnel for the assignment as well as partnership Level.	**20 Marks**
The partner Must have Engineers certified to the highest level of security certifications for the proposed solutions. The proposed personnel shall hold the stated certification or an equivalent certification demonstrating comparable competencies , supported by provide evidence of certification and role relevance Each position is scored using the descriptors in Table C (marks shown against each position below). The proposed personnel shall hold the stated certification or an equivalent certification demonstrating comparable competencies. a) **Project Manager (1) – 4.0 Marks** a. Master's degree in information technology / computer science, or IT discipline b. Minimum of 10 years' experience in IT with minimum 5 years proven delivery as a manager in charge of the project) in Project Management – (Provide CV.) c. Five (5) Years of Experience in managing IT Project Management, at least 3 NO Projects in similar entities. d. PMP or Prince 2 or other equivalent project management certifications. e. ITIL Service Management or other equivalent project management certifications. b) **Cyber-Security engineers (2) – 6.0 Marks** a. Degree in Engineering with Information Technology / Computer as specialization, Computer Science, or IT discipline b. Minimum of 7 years' experience in system security and Extensive knowledge of computer systems and networks through professional experience. c. Relevant Certifications in security d. 2 years of experience in similar occupations, such as network administrator and extensive knowledge of networks and active equipment installation through professional experience. e. . Must be certified Ethical Hacker Certified The Engineers must be certified to the highest level of security certifications for the proposed solutions The proposed personnel shall hold the stated certification or an equivalent certification demonstrating comparable competencies , supported by provide evidence of certification and role relevance	

Integration engineer (2) – 4.5 Marks a. Degree in Engineering with Information Technology / Cybersecurity, / Computer as specialization, Computer Science, or IT discipline b. Minimum of 5 years' experience in security tools that includes integration of (SIEM, SOAR, API-based integrations, log source onboarding) c. Certification in proposed OEM **Lead Enterprise Security Architect (1) – 4.0 Marks** a. Degree in Engineering, Computer Science, Cybersecurity Information Technology / Computer as specialization, Computer Science, or IT discipline. b. Minimum of 10 years' experience in enterprise security architecture, including designing security reference architectures, threat modelling, and security control framework. c. The Engineers MUST have Cloud Security and Cloud network Certified at Professional level. d. The Engineers MUST have Information Security Architecture Certification or equivalent like CISPP+ISSAP or SABSA which are purpose-built for security architecture roles e. The Engineers MUST have Information Security Architecture Certification or equivalent like CISPP+ISSAP, TOGAF or SABSA which are purpose-built for security architecture roles **Network engineers/administrator (1) – 1.5 Marks** a. Degree in Engineering, Cybersecurity, Information Technology / Computer Science specialization, Computer Science, or IT discipline b. 5 years of experience in similar occupations, such as network administrator and extensive knowledge of networks and active equipment installation through professional experience. c. . At least one Professional Level Security certification: CCNP Security, PCNSE (Palo Alto), Fortinet NSE 7, or Check Point CCSE, or an equivalent certification, aligned to the Solution being proposed by the Bidder.	**PM 4.0; Cyber-Security Engineers 6.0; Integration Engineers 4.5; Lead Enterprise Security Architect 4.0; Network Engineer 1.5 (Total 20)**
3. Criterion 4 – GOVSOC Retainer & Incidence Response Service Practice Leads Personel. The bidder shall propose named personnel for each of the positions and submit detailed CVs, copies of relevant academic and professional certificates, and evidence of relevant assignments. The proposed personnel shall demonstrate hands-on experience in Security Operations Centre (SOC), Cyber Incident Response, Threat Detection, Investigation, Containment and Recovery. The bidder shall not substitute proposed key personnel without prior written approval of the Procuring Entity	**15 Marks**
SOC Team Lead/Manager (1) – 6.0 Marks	

a) Bachelor's degree in ICT, Computer Science, Cybersecurity, Information Security or related field; b) 8+ years ICT/Cybersecurity experience, 5+ years managing SOC/CSIRT/Incident Response operations c) At least one of the following Certifications; CISSP, CISM, CRISC, GIAC, ISO 27001/22301 or equivalent **SOC Analyst (3 in No.) – 9.0 Marks (3.0 per Analyst)** a) Bachelor's degree/diploma in ICT, Cybersecurity, Computer Science or related field; b) 5+ years cybersecurity/SOC experience, including hands-on monitoring, triage, investigation and incident response c) At least one of the following Certifications; Security+, CySA+, GCIH, GCIA, CEH or equivalent a)	**6.0 Marks** **9.0 Marks**
TOTAL	**100**
"Bidders whose Technical Proposals achieve or exceed the minimum technical qualifying score of 70% (70 points out of 100) shall be determined technically responsive, and their Financial Proposals will be opened publicly. Bids passing this technical threshold will be evaluated using a weighting of 80% for Technical and 20% for Financial."	

Table B – Scoring descriptors: Enterprise Security Software and Technology Tools (25 Marks)

Security Tool	Measurable Specifications	Minimum (Specification)	Marks	50%	75%	100%
	Functional Capability – log ingestion scale, correlation, UEBA, MITRE ATT&CK mapping, analytics depth	Sustained ≥50,000 EPS without event loss; real-time correlation; UEBA module; detections mapped to MITRE ATT&CK; ≥90 days searchable hot data	2.0	50,000 EPS sustained; correlation, basic UEBA, ATT&CK-tagged rules	≥100,000 EPS sustained; ML-based UEBA; ATT&CK coverage view	≥200,000 EPS with scale-out; advanced UEBA with risk scoring; ATT&CK heatmap with gap analysis; evidenced in the Technical Proposal (verified at PoC)
	Integration – SOAR, TIP, EDR/NDR, APIs, data normalisation	Integration with SOAR, TIP, EDR and NDR via API/connectors; REST API;	2.0	API integration with SOAR, TIP, EDR and NDR	Native connectors for all four; common-schema normalisation	Bidirectional native connectors; ≥300 out-of-box parsers; custom parser tooling; all

		normalisation to a common schema				evidenced in the Technical Proposal (verified at PoC)
Security Information & Event Management (SIEM)	OEM Maturity – market leadership, R&D, roadmap, threat research	≥5 years in market; published product roadmap; ≥2 comparable similar or large-enterprise references	1.2	≥5 years; published roadmap; 2 references	In-house threat research team; ≥5 comparable deployments	Leader-level independent recognition (or equivalent evidence); in-house threat research; ≥5 comparable similar deployments
	Support & Sustainability – local support, SLAs, updates, training	24×7 support; P1 response ≤1 hr; regular updates; OEM training	1.0	24×7; P1 ≤1 hr; OEM training	Local/regional L2; P1 ≤30 min; quarterly updates	In-country L3; P1 ≤15 min; monthly detection updates; OEM-certified training
Security Orchestration, Automation and Response (SOAR)	Functional Capability – multi-layer playbooks (cloud, on-prem, identity); documented MTTR reduction; throughput	Multi-tool playbooks across cloud, on-prem and identity; documented MTTR reduction >60%; >500,000 events/second without latency (as per RFB)	2.5	Meets RFB figures: MTTR reduction >60%; >500,000 events/sec	MTTR reduction ≥70% with customer evidence; ≥750,000 events/sec	MTTR reduction ≥80%, independently verified; ≥1,000,000 events/sec; evidenced in the Technical Proposal (verified at PoC)
	Integration – universal connectors; open API	Out-of-box connectors for the proposed SIEM and data-centre stack; open API; Python/PowerShell scripting	1.5	Out-of-box for SIEM and data-centre stack; API and scripting	Adds TIP, EDR/NDR, firewall and ticketing connectors (≥200 integrations)	≥400 integrations; custom connector SDK; bidirectional; evidenced in the Technical Proposal (verified at PoC)
	OEM Maturity – carrier-grade evidence	Deployment in national SOCs or global telcos; independent "Leader" status >5 years (or equivalent evidence)	1.0	1 national-SOC/telco deployment; Leader status >5 years	2 deployments; Leader status ≥7 years	≥3 deployments across ≥2 regions; Leader status ≥7 years; public case studies
	Support & Sustainability – local presence; playbook audits	24/7/365 L3 engineers in-country or same time zone; quarterly playbook optimisation audits	1.0	As per minimum specification	Adds named technical account manager and P1 ≤30 min	Adds monthly playbook audits, P1 ≤15 min, dedicated in-country engineer
	Functional Capability – multi-layer detection, mitigation effectiveness,	L3–L7 detection and mitigation incl. TLS-encrypted attacks; mitigation capacity ≥20 Gbps (size to link	1.2	20 Gbps; ≤60 s; ≤5 ms	≥40 Gbps; ≤30 s; ≤2 ms; hybrid cloud scrubbing	≥100 Gbps or hybrid with cloud scrubbing capacity; ≤10 s automatic mitigation; ≤1

	throughput, latency impact	capacity); time-to-mitigate ≤60 s; added latency ≤5 ms				ms; independently tested
	Integration – SIEM, SOC dashboards, API orchestration	Log/alert export to SIEM (syslog/CEF); REST API	0.5	Log export to SIEM; REST API	Native SIEM connector and SOC dashboard integration	Bidirectional API orchestration (SOAR can trigger mitigation); real-time dashboards; evidenced in the Technical Proposal (verified at PoC)
Anti-DDoS Solution –	OEM Maturity – similar/critical-infrastructure experience (reference contracts, case studies, independent audit reports)	≥1 similar or critical national infrastructure reference, evidenced by contract, case study or audit report	0.5	1 verified reference	≥3 verified references	≥5 verified references across ≥2 countries plus independent audit/test report
	Support & Sustainability – 24/7 response; contractually committed response times acceptable	24×7 response with contractual response times (P1 ≤1 hr)	0.5	24×7; P1 ≤1 hr contractual	P1 ≤30 min; local/regional presence	P1 ≤15 min; in-country engineers; attack-time incident bridge; frequent signature updates
Threat Intelligence Platform (TIP)	Functional Capability – feed ingestion (STIX/TAXII), enrichment, scoring	STIX 2.x/TAXII 2.1 ingestion; ≥10 feeds; IOC deduplication, enrichment and confidence scoring	2.0	STIX/TAXII; ≥10 feeds; dedup and scoring	≥25 feeds incl. commercial; enrichment and IOC ageing	≥50 feeds; context-based scoring; sector and regional relevance; documented low false-positive rate
	Integration – SIEM/SOAR integration, IOC automation, interoperability	IOC push to SIEM and SOAR by API; STIX/TAXII sharing	1.0	API/TAXII push to SIEM and SOAR	Native SIEM/SOAR connectors; automated IOC push	Bidirectional automated sharing incl. firewall/EDR; MISP interoperability; evidenced in the Technical Proposal (verified at PoC)
	OEM Maturity – quality of intel sources, global coverage	Documented intelligence sources incl. own research; coverage in multiple regions	0.5	Documented sources; ≥2 regions	Proprietary research plus coverage relevant to your region	Proprietary global network; strong regional coverage; published source-quality metrics

	Support & Sustainability – feed updates, support model, training	Feed updates at least daily; 24×7 support; OEM training	**0.5**	Daily updates; 24×7 support	Hourly updates; regional support; training	Near-real-time updates; in-country support; certified training
File Integrity Monitoring	Functional Capability – real-time monitoring, baselining, policy enforcement	Change detection on files, registry and configs on Windows/Linux; baseline; policy-based alerts	**1.0**	Detection ≤5 min; baselining; policy alerts	Detection ≤60 s; compliance policy templates; change attribution	Real-time; agent and agentless; network/cloud config coverage; automated remediation or rollback
	Integration – SIEM integration, alert forwarding, workflow integration	Alert forwarding to SIEM (syslog/API)	**0.6**	Syslog/API alert forwarding to SIEM	Native SIEM connector	Native SIEM connector plus SOAR/ticketing workflow triggers
	OEM Maturity – stability, compliance alignment (e.g. ISO, PCI-DSS, HIPAA)	Product in market ≥3 years; alignment to at least one recognised standard	**0.4**	≥3 years; one standard mapped	Two or more standards mapped	Three or more standards with built-in audit reports
	Support & Sustainability – updates, documentation, vendor support	Regular updates; product documentation; vendor support	**0.4**	Updates and documentation	Adds business-hours vendor support	Adds 24×7 support and release roadmap
Advanced Attack Surface Management	Functional Capability – shadow IT, forgotten subdomains, leaked credentials; actionable remediation; real-time perimeter scanning	Continuous discovery of subdomains, shadow IT and forgotten assets; leaked-credential detection; near-real-time external scanning; proprietary internet indexing with confidence scoring; actionable remediation steps	**1.5**	Documented ≥80% discovery of known assets (verified at acceptance testing); remediation guidance	≥90% discovery; leaked-credential detection; risk prioritisation	≥95% discovery; attribution confidence scoring; continuous scanning; low false positives; ticketed remediation
	Integration – orchestration ready (native SOAR integration; auto scan on new government-owned asset)	SOAR integration that triggers a scan playbook when a new asset is discovered and confirmed as Government-owned	**1.0**	API-triggered playbook via SOAR	Native SOAR connector with automatic trigger on new asset	Native two-way SOAR integration; ownership-confirmation workflow; SIEM and ticketing integration
	OEM Maturity – global reach (distributed scanning network)	Scanning from multiple geographic regions to view the organisation from outside in	**0.6**	Scanning from ≥3 regions	≥5 regions across ≥3 continents	≥10 regions; proprietary internet index

	Support & Sustainability – 24/7 response, updates, local presence	24×7 response; regular updates; local or regional presence	0.6	24×7; P1 ≤1 hr	P1 ≤30 min; regional presence	P1 ≤15 min; in-country engineers; continuous updates
Total – Enterprise Security Software and Technology Tools (Phase I 18.9 + Phase II 6.1)			**25**			

Table C – Scoring descriptors: Criteria 2, 3 and 4 (Company Profile, Organizational Proposal and Experience; Key Contract Implementation Team; GovSOC Retainer & Incident Response Team)

Evaluation Item / Position	Measurable Specifications	Minimum (Specification)	Marks	50%	75%	100%
Past experience in similar assignments	Number, value and complexity of completed similar assignments (physical set-up, technology supply, delivery, installation, configuration, commissioning, training, support and maintenance of a SOC of similar nature) in the last 5 years; verified by contracts, award letters/LPOs, completion/acceptance certificates and client contacts	≥2 completed similar assignments, each ≥ Kshs 100 million, within the last 5 years, fully evidenced	4	2 similar assignments, each ≥ Kshs 100M, within the last 5 years,, fully evidenced	3 similar assignments, each ≥ Kshs 100M, within the last 5 years,	≥4 similar assignments, each ≥ Kshs 100M, with client commendation letters
Training plan(*On Tier 1 – 3, Refer to* *Training Plan and Package – Composite Scoring by Package Tier in Table D below*)	Training programme on OEM-approved curriculum and certification for ICTA technical staff, in English, at an OEM-approved facility, covering SOC operations, optimisation, configuration and management of the solutions	Plan committed to ≤6 months from award; ≥15 ICTA staff trained and certified	2.5	The package includes every Tier 1 (core) component across all eight items, but is missing one or more Tier 2 (enhanced) components in any item.	The package includes every Tier 1 and Tier 2 component across all eight items, but is missing one or more Tier 3 (premium) components in any item.	The proposed package includes every Tier 1, Tier 2 and Tier 3 component, across all eight items. Nothing required for the full package is missing.
Implementation plan, methodology and workplan	Strategy to implement and integrate the solutions without adversely affecting GOK services, with key milestones; compliance to technical requirements cross-referenced to publicly accessible supporting documents	Implementation plan, methodology, workplan with milestones, risk management, and technical compliance cross-reference	4	Plan, methodology, milestones and compliance cross-reference provided	Adds risk register, cut-over/rollback plan and UAT plan	Adds phased delivery aligned to Phase I/II, service-continuity safeguards, and every requirement cross-referenced with no gaps

Official Use Only

Proposed Service Level Agreement (SLA)	Completeness and enforceability: scope of covered services (post-implementation support, maintenance, incident management); service desk and escalation with named contacts; response times; resolution targets by severity; monitoring, reporting and performance review	All five SLA elements present, with severity classifications (critical, high, medium, low)	3	All five elements present	Adds P1 response ≤30 min, resolution targets and monthly reporting	Adds P1 response ≤15 min with resolution ≤4 hrs, OEM escalation, service credits and quarterly reviews
Company profile	Core business, organogram, mission and leadership; years in existence; proof of enterprise-level IT cybersecurity projects; OEM partnership level	Complete profile; ≥5 years in existence; OEM-authorised partner for the proposed solutions	1.5	Complete profile; ≥5 years; OEM-authorised partner	≥8 years; ≥3 enterprise cybersecurity projects; advanced partner tier	≥10 years; ≥5 enterprise cybersecurity projects; highest OEM partner tier
Project Manager (1)	Education, years of experience, related project delivery, and project management and service management certifications (CV and certified copies required notarized by a Commissioner for Oaths)	Master's in IT/CS; ≥10 years in IT with ≥5 years as project manager; ≥3 related projects; PMP/PRINCE2 (or equivalent) and ITIL (or equivalent)	4	Meets all minimums If a proposed candidate fails to meet the minimum required educational qualification **the candidate will be awarded zero (0) marks for the entire Evaluation Position**	≥12 years; ≥5 related projects; has delivered a SOC or cybersecurity project	≥15 years; ≥5 related projects incl. ≥2 SOC/large cybersecurity deployments; PMP plus PRINCE2 plus ITIL
Cyber-Security Engineers (2)	Education, years in system security, networking background, ethical hacking certification, and highest-level security certifications for the proposed solutions	Degree in Engineering/IT/CS; ≥7 years in system security; ≥2 years in similar roles (e.g. network administration); Certified Ethical Hacker; ≥1 professional-level security certification for the proposed solutions	6	Meets all minimums If a proposed candidate fails to meet the minimum required educational qualification **the candidate will be awarded zero (0) marks for the entire Evaluation Position**	Both ≥10 years with ≥2 professional-level certifications	Both ≥12 years with expert-level certification on the proposed solutions plus CEH; related SOC experience
Integration Engineers (2)	Education, years integrating security tools (SIEM, SOAR, API-based integrations, log-source onboarding), and OEM certification	Degree in Engineering/IT/Cybersecurity/CS; ≥5 years integrating security tools; certification in the proposed OEM	4.5	Meets all minimums If a proposed candidate fails to meet the minimum required educational qualification **the candidate will be awarded zero**	Both ≥7 years; professional-level OEM certification for SIEM and SOAR	Both ≥10 years; expert-level OEM certification (SIEM and SOAR); ≥20 log-source integrations; scripting/API skills demonstrated

				(0) marks for the entire Evaluation Position		
Lead Enterprise Security Architect (1)	Education, years in security architecture (reference architectures, threat modelling, control frameworks), cloud security certifications, security architecture certification	Degree in Engineering/CS/Cybersecurity/IT; ≥10 years in enterprise security architecture; professional-level cloud security and cloud network certification; CISSP-ISSAP, SABSA, TOGAF or equivalent	4	Meets all minimums If a proposed candidate fails to meet the minimum required educational qualification **the candidate will be awarded zero (0) marks for the entire Evaluation Position**	≥12 years; ≥2 similar large-enterprise architectures delivered	≥15 years; ≥2 architecture certifications; professional cloud certification on ≥2 platforms; ≥3 related SOC architectures
Network Engineer / Administrator (1)	Education, years in network administration and active-equipment installation, and professional-level security certification aligned to the proposed solution	Degree in Engineering/Cybersecurity/IT/CS; ≥5 years in network administration and active-equipment installation; ≥1 professional-level security certification (e.g. CCNP Security, PCNSE, NSE 7, CCSE)	1.5	Meets all minimums If a proposed candidate fails to meet the minimum required educational qualification **the candidate will be awarded zero (0) marks for the entire Evaluation Position**	≥7 years; two professional-level certifications aligned to the solution	≥10 years; expert-level certification (e.g. CCIE Security); SOC or data-centre network deployments
GOVSOC Retained Incidence Response Management & Response Team						
SOC Team Lead / Manager (1)	Education, years in ICT/cybersecurity and in managing SOC/CSIRT/IR operations, and management/security certifications	Bachelor's in ICT/CS/Cybersecurity/InfoSec; ≥8 years ICT/cyber with ≥5 years managing SOC/CSIRT/IR; ≥1 of CISSP, CISM, CRISC, GIAC, ISO 27001/22301 or equivalent	6	Meets all minimums If a proposed candidate fails to meet the minimum required educational qualification **the candidate will be awarded zero (0) marks for the entire Evaluation Position**	≥10 years with ≥7 years managing SOC/CSIRT; ≥2 certifications; has led a similar SOC	≥12 years with ≥8 years managing SOC/CSIRT; ≥2 senior certifications incl. ISO 27001 lead role; led major incident response; Master's degree
SOC Analysts (3 in No.)	Education, years in SOC monitoring, triage, investigation and incident response, and security analyst certifications	Bachelor's/diploma in ICT/Cybersecurity/CS; ≥5 years cybersecurity/SOC experience; ≥1 of Security+, CySA+, GCIH, GCIA, CEH or equivalent	9 (3 per Analyst)	Meets all minimums	All three ≥6 years; at least one senior certification (e.g. GCIH/GCIA) each	All three ≥7 years; GIAC-level certification each; OEM SIEM certification

Table D – Training Plan and Package: Composite Scoring by Package Tier (Sub-criterion 2.2)

EVALUATION ITEM	TIER 1 – CORE COMPONENTS (REQUIRED FOR 50%)	TIER 2 – ENHANCED COMPONENTS (ADD THESE TO REACH 75%)	TIER 3 – PREMIUM COMPONENTS (ADD THESE TO REACH 100%)
Curriculum coverage and depth	Written syllabus covering administration and day-to-day operations for every proposed solution	Adds use-case, correlation-rule and/or playbook authoring and tuning modules	Adds troubleshooting and upgrade/patch-management modules, plus scenario-based exercises built on realistic attack chains
Training methodology and delivery format	Instructor-led training with hands-on lab exercises on a representative (non-production) environment	Adds self-paced e-learning content attendees can revisit after the classroom ends	Adds a dedicated sandbox/lab environment retained by ICTA after training, plus red-team/blue-team or scenario-based exercises
OEM-approved curriculum and training provider	OEM-approved curriculum delivered by an OEM-certified trainer or OEM-authorised training partner	Adds a trainer who is OEM-certified with ≥2 years delivering this specific curriculum	Adds ≥3 comparable similarlarge-enterprise deployments trained, with a reference-checkable track record
Training materials and documentation	Manuals and lab guides provided, retained by ICTA after training with no further licensing restriction	Adds a searchable knowledge base and quick-reference runbooks for on-the-job use	Adds recorded training sessions, version-controlled documentation, and update rights as the solution evolves
Certification and competency validation	Assessment-based certificate of completion (competency-based, not attendance-only)	Adds a pathway to a recognised OEM associate/professional certification, exam voucher included	Adds OEM professional/expert-level certification achieved, with a documented pass rate from prior deliveries
Post-training support and mentoring	A named point of contact for post-training queries for at least 30 days	Adds a structured mentoring programme (60–90 days) with scheduled check-ins	Adds a train-the-trainer track on top of 90-day mentoring, so ICTA can sustain training internally
Customisation to ICTA's environment	Generic OEM course supplemented with a walkthrough of the as-built ICTA configuration	Adds course content explicitly adapted to reference ICTA's architecture, log sources and integrations throughout	Adds a fully customised curriculum built around ICTA's own sanitised use cases, data and SOPs
Logistics, language and accessibility	English-language training, suitable venue, scheduled to avoid leaving the SOC uncovered	Adds staggered cohort scheduling so the SOC stays fully staffed throughout training	Adds an on-site delivery option, recorded sessions and make-up sessions for anyone who could not attend live

3. Technical alternatives – None

4. Financial Evaluation

The following factors and methods will apply:

(a) Time Schedule:

The number of weeks, from the effective date specified in Article 3 of the Contract Agreement, to achieve Operational Acceptance must be no more than: ***35 weeks***

A Proposal offering to achieve Operational Acceptance earlier than the maximum number of weeks ***shall not*** be given credit for proposal evaluation purposes.

(b) Recurrent Costs

Since the operation and maintenance of the system being procured form a major part of the implementation, the resulting recurrent costs will be evaluated according to the principles given hereafter, including the cost of recurrent cost items for the initial period of operation stated below, based on prices furnished by each Proposer in Price Schedule Nos. 3.3 and 3.5.

Recurrent cost items for post- warranty service period if subject to evaluation shall be included in the main contract or a separate contract signed together with the main contract.

Such costs shall be added to the Proposal price for evaluation.

The recurrent cost factors for calculation of the implementation schedule are:

(i) number of years for implementation

(ii) hardware maintenance

(iii) software licenses and updates

(iv) technical services

(v) telecommunication services, and

(vi) other services (if any).

The Recurrent Costs (R) are reduced to net present value and determined using the following formula:

$$R \sum_{X=1}^{N} \frac{R_x}{(1+I)^x}$$

where

N = number of years of evaluated recurrent costs

x = an index number 1, 2, 3, ... N.

R_x = total Recurrent Costs for year "x," as recorded in the Recurrent Cost Sub-Table.

I = discount rate to be used for the Net Present Value calculation, as specified **in the PDS for ITP 39.1.**

(c) Specific additional criteria

The relevant evaluation method, if any, shall be as follows:

Not Applicable

5. Combined Evaluation

The Purchaser will evaluate and compare the Proposals that have been determined to be substantially responsive.

An Evaluated Proposal Score (B) will be calculated for each responsive Proposal using the following formula, which permits a comprehensive assessment of the evaluated cost and the technical merits of each Proposal:

$$B \equiv \frac{Clow}{C} * X * 100 + \frac{T}{Thigh} * (1 - X) * 100$$

where

C = Evaluated Proposal Price

C_{low} = the lowest of all Evaluated Proposal Prices among responsive Proposals

T = the total Technical Score awarded to the Proposal

T_{high} = the Technical Score achieved by the Proposal that was scored best among all responsive Proposals

X = weight for the Cost as specified in the PDS

6. Proof of concept

A Proof of Concept (PoC) shall be carried out, prior to Contract award, on the Most Advantageous Proposal to verify critical functional, technical, integration, and security requirements of the proposed GovSOC solutions, including SIEM, SOAR, TIP, and Anti-DDoS, using predefined test scenarios and acceptance criteria. It shall be conducted at a date and venue specified by the Procuring Entity, under the supervision of the designated evaluation team, with the Proposer responsible for providing the required demonstration resources. The

Official Use Only

solution must satisfy all mandatory PoC criteria to pass. . The PoC shall be conducted in accordance with the following procedure:

(a) Sequence: the PoC shall take place after the combined evaluation of the Technical and Financial Parts (ITP 39) and before the Notification of Intention to Award. Only the Proposer with the Most Advantageous Proposal shall be invited, in writing, to the PoC.

(b) Timing and venue: the PoC shall start within ten (10) Business Days of the written invitation and shall be completed within five (5) Business Days, at the GovSOC site (23rd Floor, Telposta Towers, Nairobi) or another test environment designated by the Purchaser in the invitation.

(c) Resources: the Proposer shall provide, at its own cost, the proposed software, any required hardware or virtual appliances, temporary licences and qualified personnel. The Purchaser shall provide the test environment, network connectivity, test data sets and simulated events. The test scripts and data sets shall be issued to the Proposer with the invitation.

(d) Assessment: each mandatory test scenario in the table below shall be assessed as Pass or Fail by the Purchaser's evaluation committee against the stated pass criteria. The Proposer's representatives may attend, and the results shall be recorded in a PoC report signed by the committee. The PoC shall not be used to re-score the Technical Proposal, and no change to the Proposal or its price shall be sought or permitted.

(e) Pass/fail criterion: the Proposal passes the PoC only if all six (6) mandatory test scenarios are passed. The PoC shall be conducted on the components, versions and configuration offered in the Proposal.

(f) Consequence of failure: a Proposal that fails any mandatory test scenario shall be rejected. The Purchaser shall then invite the Proposer with the next Most Advantageous Proposal to a PoC under the same procedure, and so on, in accordance with the Procurement Regulations.

The mandatory PoC test scenarios and pass criteria are set out in the table below. The thresholds applied shall be those stated in the corresponding requirements of Section VII; no other criteria shall be applied.

No.	Solution	Mandatory test scenario	Pass criteria
1	SIEM	Ingest logs from designated security devic es and generate an alert for a predefined s ecurity event.	All designated log sources are successfully integrated, and the predefined event is dete cted and alerted according to the specified t est cases.
2	SOAR	Execute a predefined incident-response playbook triggered by a simulate d security alert.	The playbook executes all mandatory steps, records actions, and produces an auditable incident record without unauthorized action s.

3	TIP	Import a test set of threat indicators and c orrelate them with simulated security even ts.	All designated test indicators are imported, matched, and enriched correctly in accorda nce with the specified test cases.
4	Anti-DDoS	Detect and mitigate an approved simulate d DDoS attack in a controlled test environ ment.	The solution detects the defined attack, app lies the required mitigation, and maintains l egitimate traffic within the specified perfor mance and availability thresholds.
5	Integrati on	Demonstrate information exchange betwe en the proposed tools using the specified i nterfaces or APIs.	All mandatory integration test cases succee d, with accurate data exchange, appropriate access controls, and auditable results.
6	Reportin g and au dit	Generate an incident report and retrieve re levant event and response logs.	Required reports are generated accurately, and relevant events, user actions, and respo nse activities are traceable.

1. Qualification

Factor	1.1 ELIGIBILITY					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.1 Nationality	Nationality in accordance with ITP 4.4.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Form ELI –1.1 and 1.2, with attachments
1.2 Conflict of Interest	No- conflicts of interests as described in ITP 4.2.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Proposal
1.3 Bank Ineligibility	Not having been declared ineligible by the Bank as described in ITP 4.5.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Proposal
1.4 State owned Entity of the Borrower country	Compliance with conditions of ITP 4.6	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Form ELI –1.1 and 1.2, with attachments

Official Use Only

Factor	1.1 ELIGIBILITY					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.1.5 United Nations resolution or Borrower's country law	Not having been excluded as a result of prohibition in the Borrower's country laws or official regulations against commercial relations with the Proposer's country, or by an act of compliance with UN Security Council resolution, both in accordance with ITP 4.8	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Proposal

Factor	1.2 HISTORICAL CONTRACT NON-PERFORMANCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.2.1 History of non-performing contracts	Non-performance of a contract[1] did not occur as a result of Proposer's default since 1st January *2021*.	Must meet requirement by itself or as member to past or existing JV	N / A	Must meet requirement[2]	N / A	Form CON - 2
1.2.2 Suspension	Not under suspension based on execution of a Bid-Securing Declaration or Proposal-Securing Declaration pursuant to ITP 4.7 and ITP 20.10	Must meet requirement	N / A	Must meet requirement	N / A	Letter of Proposal

[1] Nonperformance, as decided by the Purchaser, shall include all contracts where (a) nonperformance was not challenged by the contractor, including through referral to the dispute resolution mechanism under the respective contract, and (b) contracts that were so challenged but fully settled against the contractor. Nonperformance shall not include contracts where Purchaser decision was overruled by the dispute resolution mechanism. Nonperformance must be based on all information on fully settled disputes or litigation, i.e. dispute or litigation that has been resolved in accordance with the dispute resolution mechanism under the respective contract and where all appeal instances available to the applicant have been exhausted.

[2] This requirement also applies to contracts executed by the Applicant as JV member.

Official Use Only

1.2.3 Pending Litigation	Proposer's financial position and prospective long term profitability still sound according to criteria established in 2.3.1 below and assuming that all pending litigation will be resolved against the Proposer.	Must meet requirement by itself or as member to past or existing JV	N / A	Must meet requirement	N / A	Form CON – 2
1.2.4 Litigation History	No consistent history of court/arbitral award decisions against the Proposer[3] since 1st January *2021*	Must meet requirement	Must meet requirement	Must meet requirement	N/A	Form CON – 2
1.2.5 Bank's SEA and/or SH Disqualification[4]	At the time of Contract Award, not subject to disqualification by the Bank for non-compliance with SEA/ SH obligations	Must meet requirement (including each subcontractor proposed by the Proposer)	N/A	Must meet requirement (including each subcontractor proposed by the Proposer)	N/A	Letter of Proposal, Form CON-3

[3] The Proposer shall provide accurate information on the related Letter of Proposal about any litigation or arbitration resulting from contracts completed or ongoing under its execution over the last five years. A consistent history of awards against the Proposer or any member of a joint venture may result in failure of the Proposal.

Official Use Only

Factor	1.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.3.1 Historical Financial Performance	Submission of audited financial statements for the last **Three (3)** years (2023, 2024 and 2025, or the financial years 2022/2023, 2023/2024 and 2024/2025 where the Proposer's financial year does not coincide with the calendar year) to demonstrate the current soundness of the Proposers financial position and its prospective long term profitability.	Must meet requirement	N / A	Must meet requirement	N / A	Form FIN – 1.3.1 with attachments
1.3.2 Average Annual Turnover	Minimum average annual turnover of __ **KES 300 Million** (calculated as total certified payments received for contracts in progress or completed, within the last three **(3)** years (2023, 2024 and 2025), being the same years as the audited financial statements under Sub-Factor 1.3.1)	Must meet requirement	Must meet requirement	N/A	N/A	Form FIN –1.3.2

Factor	1.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.3.3 Financial Resources	The Proposer must demonstrate access to, or availability of, financial resources such as liquid assets, unencumbered real assets, lines of credit, and other financial means, other than any contractual advance payments to meet the following cash-flow requirement: **KES 80 million**.	Must meet requirement	Must meet requirement	N/A	N/A	Form FIN –1.3.3

Factor	1.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
1.4.1 General Experience	Experience under supply and installation of information systems/ICT security solutions in the role of prime supplier, management contractor, JV member, or subcontractor for at least the last **five** [**5**] years prior to the applications submission deadline.	Must meet requirement	N / A	Must meet requirement	N / A	Form EXP-1.4.1
1.4.2 Specific Experience	Participation as a prime supplier, management contractor, JV[5] member, sub-contractor, in at least The Bidder shall demonstrate that it has successfully completed at least Two (2) contracts within the last Five (5) years prior to bid submission deadline, each with a value of at least Kes. 100 million or equivalent that have been successfully and substantially completed and that are similar in nature and complexity to the Contract for the delivery Supply,	Must meet requirement	Must meet requirements	N / A		Form EXP 1.4.2

[5] For contracts under which the Proposer participated as a joint venture member or sub-contractor, only the Proposer's share, by value, and role and responsibilities shall be considered to meet this requirement.

Official Use Only

Factor	1.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Proposer				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
	Delivery, Installation of Technology, Configuration & Commissioning of a Security Operation Center- SOC The successfully completed similar contracts shall be documented by a copy of an Operational acceptance certificate (or equivalent documentation satisfactory to the Purchaser) issued by the purchaser(s).					

SECTION IV - PROPOSAL FORMS

Table of Forms

Letter of Proposal- Technical Part **88**

FORM ELI 1.1.1- PROPOSER INFORMATION FORM **91**

FORM ELI 1.1.2- PROPOSER'S JV MEMBERS INFORMATION FORM **93**

FORM CON – 2- HISTORICAL CONTRACT NON-PERFORMANCE, PENDING LITIGATION AND LITIGATION HISTORY **95**

FORM CON – 3 ..... **97**

SEXUAL EXPLOITATION AND ABUSE (SEA) AND/OR SEXUAL HARASSMENT PERFORMANCE DECLARATION **97**

FORM EXP 1.4.1- GENERAL EXPERIENCE **98**

FORM EXP 1.4.2- SPECIFIC EXPERIENCE **99**

FORM EXP 1.4.2 (CONT.)- SPECIFIC EXPERIENCE (CONT.) **100**

FORM CCC- SUMMARY SHEET: CURRENT CONTRACT COMMITMENTS / WORK IN PROGRESS **101**

FORM FIN 1.3.1- FINANCIAL SITUATION: HISTORICAL FINANCIAL PERFORMANCE **102**

FORM FIN 1.3.2- AVERAGE ANNUAL TURNOVER **103**

FORM FIN 1.3.3- FINANCIAL RESOURCES **104**

PERSONNEL CAPABILITIES- KEY PERSONNEL **105**

CODE OF CONDUCT FOR SUPPLIER'S PERSONNEL FORM **108**

TECHNICAL CAPABILITIES **112**

MANUFACTURER'S AUTHORIZATION **113**

SUBCONTRACTOR'S AGREEMENT **114**

INTELLECTUAL PROPERTY FORMS **116**

CONFORMANCE OF INFORMATION SYSTEM MATERIALS **119**

FORM OF PROPOSAL SECURITY (BANK GUARANTEE) **122**

PRICE SCHEDULE FORMS **127**

Official Use Only

Letter of Proposal- Technical Part

INSTRUCTIONS TO PROPOSERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE DOCUMENT

The Proposer must prepare this Letter of Proposal on stationery with its letterhead clearly showing the Proposer's complete name and business address.

Note: All italicized text is to help Proposers in preparing this form.

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

RFP No.: *[insert **number of RFP process**]*

Alternative No.: *[insert **identification No if this is a Proposal for an alternative,** otherwise state **"not applicable"**]*

We, the undersigned, declare that:

To: *[insert **complete name of Purchaser**]*

(a) **No reservations:** We have examined and have no reservations to the request for proposals document, including Addenda issued in accordance with Instructions to Proposers (ITP 8);

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

(c) **Proposal-Securing Declaration:** We have not been suspended nor declared ineligible by the Purchaser based on execution of a Bid-Securing Declaration or Proposal-Securing Declaration in the Purchaser's Country in accordance with ITP 4.7;

(d) **Sexual Exploitation and Abuse (SEA) and/or Sexual Harassment (SH):** [*select the appropriate option from (i) to (v) below and delete the others. In case of JV members and/or subcontractors, indicate the status of disqualification by the Bank of each JV member and/or subcontractor]*.

We, including any of our subcontractors:

(i) [have not been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations.]

(ii) [are subject to disqualification by the Bank for non-compliance with SEA/ SH obligations.]

(iii) [had been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations, and were removed from the disqualification list. An arbitral award on the disqualification case has been made in our favor.]

Official Use Only

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

(f) **Proposal Validity:** Our Proposal shall be valid until *[insert day, month and year in accordance with ITP 19.1],* and it shall remain binding upon us and may be accepted at any time before the expiration of that period;

(g) **Performance Security:** If our Proposal is accepted, we commit to obtain a Performance Security in accordance with the request for proposals document;

(h) **One Proposal Per Proposer:** We are not submitting any other Proposal(s) as an individual Proposer, and we are not participating in any other Proposal(s) as a Joint Venture member, and meet the requirements of ITP 4.3, other than alternative Proposals submitted in accordance with ITP 13;

(i) **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 World Bank Group or a debarment imposed by the World Bank Group in accordance with the Agreement for Mutual Enforcement of Debarment Decisions between the World Bank and other development banks. Further, we are not ineligible under the Purchaser's Country laws or official regulations or pursuant to a decision of the United Nations Security Council;

(j) **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 ITP 4.6***];

(k) **Commissions, gratuities and fees**: We have paid, or will pay the following commissions, gratuities, or fees with respect to the procurement 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****."]*

(l) **Binding Contract**: We understand that this Proposal, together with your written acceptance thereof included in your Letter of Acceptance, shall constitute a binding contract between us, until a formal contract is prepared and executed;

Official Use Only

(m) **Not Bound to Accept:** We understand that you are not bound to accept the lowest evaluated cost Proposal, the Most Advantageous Proposal or any other Proposal that you may receive; and

(n) **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 Proposer: **[insert **complete name of the Proposer**]*

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

Title of the person signing the Proposal: *[insert **complete title of the person signing the Proposal**]*

Signature of the person named above: *[insert **signature of person whose name and capacity are shown above**]*

Date signed *[insert **number**]* day of *[insert **month**]*, *[insert **year**]*

*: In the case of the Proposal submitted by joint venture specify the name of the Joint Venture as Proposer

**: Person signing the Proposal shall have the power of attorney given by the Proposer to be attached with the Proposal

FORM ELI 1.1.1- PROPOSER INFORMATION FORM

*[**Note**: The Proposer 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 Proposal submission***]

RFP No.: *[insert **number of Request for Proposals process**]*

Alternative No.: *[insert **identification No if this is a Proposal for an alternative]** otherwise state **"not applicable"***

Page _____ of_ _____ pages

1. Proposer's Name *[insert **Proposer's legal name**]*
2. In case of JV, legal name of each member : *[insert **legal name of each member in JV**]*
3. Proposer's actual or intended country of registration: *[insert **actual or intended country of registration**]*
4. Proposer's year of registration: *[insert **Proposer's year of registration**]*
5. Proposer's Address in country of registration: *[insert **Proposer's legal address in country of registration**]*
6. Proposer'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 ITP 4.4. ☐ In case of JV, letter of intent to form JV or JV agreement, in accordance with ITP 4.1. ☐ In case of state-owned enterprise or institution, in accordance with ITP 4.6 documents establishing: • Legal and financial autonomy • Operation under commercial law

- Establishing that the Proposer is not under the supervision of the Purchaser

8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership. *[The successful Proposer shall provide additional information on beneficial ownership, using the Beneficial Ownership Disclosure Form.]*

FORM ELI 1.1.2- PROPOSER'S JV MEMBERS INFORMATION FORM

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

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

RFP No.: *[insert **number of Request for Proposals process**]*

Alternative No.: *[insert **identification No if this is a Proposal for an alternative,** otherwise state **"not applicable"**]*

Page _____ of_ _____ pages

1. Proposer's Name: *[insert **Proposer's legal name**]*
2. Proposer's JV Member's name: *[insert **JV's Member legal name**]*
3. Proposer's JV Member's country of registration: *[insert **JV's Member country of registration**]*
4. Proposer's JV Member's year of registration: *[insert **JV's Member year of registration**]*
5. Proposer's JV Member's legal address in country of registration: *[insert **JV's Member legal address in country of registration**]*
6. Proposer'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**]*

Official Use Only

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 ITP 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 Purchaser in accordance with ITP 4.6.

8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership. *[The successful Proposer shall provide additional information on beneficial ownership for each JV member using the Beneficial Ownership Disclosure Form.]*

FORM CON – 2- HISTORICAL CONTRACT NON-PERFORMANCE, PENDING LITIGATION AND LITIGATION HISTORY

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

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: _____*[insert **date**]*

JV member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Non-Performed Contracts in accordance with Section III, Evaluation and Qualification Criteria			
☐ Contract non-performance did not occur since 1st January *[insert year]* specified in Section III, Evaluation and Qualification Criteria, Sub-Factor 1.2.1. ☐ Contract(s) not performed since 1st January *[insert year]* specified in Section III, Evaluation and Qualification Criteria, requirement 1.2.1			
Year	**Non-performed portion of contract**	**Contract Identification**	**Total Contract Amount (current value, currency, exchange rate and US$ equivalent)**
*[insert **year**]*	*[insert **amount and percentage**]*	Contract Identification: *[indicate **complete contract name/ number, and any other identification**]* Name of Employer: *[insert **full name**]* Address of Employer: *[insert **street/city/country**]* Reason(s) for nonperformance: *[indicate **main reason(s)**]*	*[insert **amount**]*
Pending Litigation, in accordance with Section III, Evaluation and Qualification Criteria			
☐ No pending litigation in accordance with Sub-Factor 1.2.3. ☐ Pending litigation in accordance with Sub-Factor 1.2.3 as indicated below.			

Official Use Only

Year of dispute	Amount in dispute (currency)	Contract Identification	Total Contract Amount (currency), USD Equivalent (exchange rate)
*[specify **year**]*	*[specify **amount and currency**]*	Contract Identification: *[insert **Contract ID**]* Name of Employer: *[insert **Name of Employer**]* Address of Employer: *[insert **Address of Employer**]* Matter in dispute: *[describe **Matter of dispute**]* Party who initiated the dispute: *[specify **Initiator of dispute**]* Status of dispute: *[specify **Status of dispute**]*	*[specify **total contract amount and currency, USD equivalent and exchange rate**]*
*[specify **year**]*	*[specify **amount and currency**]*	Contract Identification: *[insert **Contract ID**]* Name of Employer: *[insert **Name of Employer**]* Address of Employer: *[insert **Address of Employer**]* Matter in dispute: *[describe **Matter of dispute**]* Party who initiated the dispute: *[specify **Initiator of dispute**]* Status of dispute: *[specify **Status of dispute**]*	*[specify **total contract amount and currency, USD equivalent and exchange rate**]*
Litigation History in accordance with Section III, Evaluation and Qualification Criteria			
☐ No Litigation History in accordance with Sub-Factor 1.2.4. ☐ Litigation History in accordance with Sub-Factor 1.2.4 as indicated below.			
Year of award	**Outcome as percentage of Net Worth**	**Contract Identification**	**Total Contract Amount (currency), USD Equivalent (exchange rate)**
*[specify **year**]*	*[specify **percentage of net worth**]*	Contract Identification: *[insert **Contract ID**]* Name of Employer: *[insert **Name of Employer**]* Address of Employer: *[insert **Address of Employer**]*	*[specify **total contract amount and currency, USD equivalent and exchange rate**]*

FORM CON – 3

SEXUAL EXPLOITATION AND ABUSE (SEA) AND/OR SEXUAL HARASSMENT PERFORMANCE DECLARATION

[The following table shall be filled in by the Proposer, each member of a Joint Venture and each subcontractor proposed by the Proposer]

Proposer's Name: *[insert full name]*
Date: *[insert day, month, year]*
Joint Venture Member's or Subcontractor's Name: *[insert full name]*
RFP No. and title: *[insert RFP number and title]*
Page *[insert page number]* of *[insert total number]* pages

SEA and/or SH Declaration **in accordance with Section III, Qualification Criteria, and Requirements**
We: ☐ (a) have not been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations ☐ (b) are subject to disqualification by the Bank for non-compliance with SEA/ SH obligations ☐ (c) had been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations, and were removed from the disqualification list. An arbitral award on the disqualification case has been made in our favor.
[*If (c) above is applicable, attach evidence of an arbitral award reversing the findings on the issues underlying the disqualification.]*

FORM EXP 1.4.1- GENERAL EXPERIENCE

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Starting Month / Year	Ending Month / Year	Years *	Contract Identification	Role of Proposer
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*
*[insert **month / year**]*	*[insert **month / year**]*	*[insert **number of years**]*	Contract name: *[insert **Name of Contract**]* Brief Description of the Information System performed by the Proposer: *[describe **Information System**]* Name of Purchaser: *[insert **Name of Purchaser**]* Address: *[insert **Address of Purchaser**]*	*[describe **role of Proposer under the contract**]*

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

FORM EXP 1.4.2- SPECIFIC EXPERIENCE

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Similar Contract Number: ___ of ___ required.	**Information**		
Contract Identification	*[insert **Contract ID**]*		
Award date Completion date	*[insert **Date of Award*** *[insert **Date of Completion***		
Role in Contract	☐ Prime Supplier	☐ Management Contractor	☐ Subcontractor
Total contract amount			
If member in a JV or subcontractor, specify participation of total contract amount			
Purchaser's Name:	_____		
Address: Telephone/fax number: E-mail:	_____ _____ _____		

FORM EXP 1.4.2 (CONT.)- SPECIFIC EXPERIENCE (CONT.)

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Similar Contract No. *[insert **specific number**]* **of** *[**insert total number of contracts**]* **required**	**Information**
Description of the similarity in accordance with Sub-Factor 1.4.2 of Section III:	
Amount	*[insert **contract amount and currency and USD equivalent and exchange rate**]*
Geographical Scope	*[describe **geographic scope of the users of the information system**]*
Functional Scope	*[describe **the functionalities provided by the information system**]*
Methods/Technology	*[describe **methodologies and technologies used to implement the information system**]*
Key Activities	*[describe **the key activities of the Proposer under the contract**]*

Official Use Only

FORM CCC- SUMMARY SHEET: CURRENT CONTRACT COMMITMENTS / WORK IN PROGRESS

[Proposers and each partner to a Joint Venture should provide information on their current commitments on all contracts that have been awarded, or for which a letter 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.]

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Name of contract	Purchaser, contact address/tel./fax	Value of outstanding Information System (current US$ equivalent)	Estimated completion date	Average monthly invoicing over last six months (US$ equivalent/month)
1. *[insert **Name o Contract]***	*[insert **Name of Purchaser, contact address, telephone / fax number]***	*[insert **Total Outstanding Contract Value of the information system in USD equivalent and exchange rate]***	*[insert **Estimated completion date]***	*[insert **Average monthly invoices in USD equivalent and exchange rate]***
2. *[insert **Name o Contract]***	*[insert **Name of Purchaser, contact address, telephone / fax number]***	*[insert **Total Outstanding Contract Value of the information system in USD equivalent and exchange rate]***	*[insert **Estimated completion date]***	*[insert **Average monthly invoices in USD equivalent and exchange rate]***
3. *[insert **Name o Contract]***	*[insert **Name of Purchaser, contact address, telephone / fax number]***	*[insert **Total Outstanding Contract Value of the information system in USD equivalent and exchange rate]***	*[insert **Estimated completion date]***	*[insert **Average monthly invoices in USD equivalent and exchange rate]***
...				

FORM FIN 1.3.1- FINANCIAL SITUATION: HISTORICAL FINANCIAL PERFORMANCE

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

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Financial information in US$ equivalent	**Historic information for previous** *[insert **number**]* **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 Proposer 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)

FORM FIN 1.3.2- AVERAGE ANNUAL TURNOVER

[To be completed by the Proposer and, if JV, by each member]

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Annual turnover data (applicable activities only)		
Year	Amount and Currency	US$ equivalent
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*[insert **year**]*	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*
*Average Annual Turnover	*[insert **amount and currency**]*	*[insert **amount in USD equivalent and exchange rate**]*

*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 1.3.2.

FORM FIN 1.3.3- FINANCIAL RESOURCES

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

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

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. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*
2. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*
3. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*
4. *[describe **type and source of available financing**]*	*[insert **amount of available financing in USD equivalent and exchange rate**]*

Official Use Only

PERSONNEL CAPABILITIES- KEY PERSONNEL

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

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Proposers 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.

Key Personnel

1.	Title of position: *[insert **Title of position / role in team**]*	
	Name of candidate: *[insert **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: *[insert **Title of position / role in team**]*	
	Name of candidate: *[insert **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: **Cyber security Expert/s** ***[Include as required]***	

Official Use Only

Name of candidate: *[insert **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***]

Candidate Summary

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

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

Position; *[insert **Title of Position**]*		Prime ☐ Alternate
Candidate information	Name of candidate *[insert **Name Candidate**]*	Date of birth *[insert **Date of Birth**]*
	Professional qualifications *[describe **Professional qualifications**]*	
Present employment	Name of Employer *[insert **Name of Present Employer**]*	
	Address of Employer *[insert **Address of Present Employer**]*	
	Telephone *[insert **Telephone** of **Contact**]*	Contact (manager / personnel officer) *[insert **Name**]*
	Fax *[insert **fax of Contact**]*	email *[insert **email** of **Contact**]*
	Job title of candidate *[insert **Job Title Candidate**]*	Years with present Employer *[insert **Number of years**]*

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 experienc
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*
*[insert **year**]*	*[insert **year**]*	*[describe **experience relevant to the proposed Contract under the RFP**]*

Official Use Only

CODE OF CONDUCT FOR SUPPLIER'S PERSONNEL FORM

***Note to the Purchaser**:*

***The following minimum requirements shall not be modified**. The Purchaser may add additional requirements to address identified issues, informed by relevant environmental and social assessment.*

Delete this Box prior to issuance of the Request for Proposals document.

Note to the Proposer:

The minimum content of the Code of Conduct form as set out by the Purchaser shall not be substantially modified. However, the Proposer may add requirements as appropriate, including to take into account Contract-specific issues/risks.

The Proposer shall initial and submit the Code of Conduct form as part of its proposal.

CODE OF CONDUCT FOR SUPPLIER'S PERSONNEL

We are the Supplier, [*enter name of Supplier*]. We have signed a contract with [*enter name of Purchaser*] for [*enter description of the Information System*]. The Information System will be supplied to and installed at [*enter the Project Site/s]*. Our contract requires us to implement measures to address environmental and social risks.

This Code of Conduct identifies the behavior that we require from Supplier's Personnel employed in the execution of the Contract at the Project Site/s.

Our workplace is an environment where unsafe, offensive, abusive or violent behavior will not be tolerated and where all persons should feel comfortable raising issues or concerns without fear of retaliation.

REQUIRED CONDUCT

Supplier's Personnel employed in the execution of the Contract at the Project Site/s shall:

1. carry out his/her duties competently and diligently;
2. comply with this Code of Conduct and all applicable laws, regulations and other requirements, including requirements to protect the health, safety and well-being of other Supplier's Personnel and any other person;
3. maintain a safe working environment including by:

a. ensuring that workplaces, machinery, equipment and processes under each person's control are safe and without risk to health;

b. wearing required personal protective equipment;

c. using appropriate measures relating to chemical, physical and biological substances and agents; and

d. following applicable emergency operating procedures.

4. report work situations that he/she believes are not safe or healthy and remove himself/herself from a work situation which he/she reasonably believes presents an imminent and serious danger to his/her life or health;
5. treat other people with respect, and not discriminate against specific groups such as women, people with disabilities, migrant workers or children;
6. not engage in any form of sexual harassment including unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature with other Supplier's or Purchaser's Personnel;
7. not engage in Sexual Exploitation, which means any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another;
8. not engage in in Sexual Abuse, which means the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions;
9. not engage in any form of sexual activity with individuals under the age of 18, except in case of pre-existing marriage;
10. complete relevant training courses that will be provided related to the environmental and social aspects of the Contract, including on health and safety matters, and Sexual Exploitation and Abuse, and Sexual Harassment (SH);
11. report violations of this Code of Conduct; and
12. not retaliate against any person who reports violations of this Code of Conduct, whether to us or the Purchaser, or who makes use of the grievance mechanism for Supplier's Personnel or the project's Grievance Redress Mechanism.

RAISING CONCERNS

If any person observes behavior that he/she believes may represent a violation of this Code of Conduct, or that otherwise concerns him/her, he/she should raise the issue promptly. This can be done in either of the following ways:

1. Contact [*enter name of the Supplier's Social Expert with relevant experience in handling sexual exploitation, sexual abuse and sexual harassment cases, or if such person is not required under the Contract, another individual designated by the Supplier to handle these matters*] in writing at this address [ ] or by telephone at [ ] or in person at [ ]; or
2. Call [ ] to reach the Supplier's hotline *(if any)* and leave a message.

The person's identity will be kept confidential, unless reporting of allegations is mandated by the country law. Anonymous complaints or allegations may also be submitted and will be given all due and appropriate consideration. We take seriously all reports of possible misconduct and will investigate and take appropriate action. We will provide warm referrals to service providers that may help support the person who experienced the alleged incident, as appropriate.

There will be no retaliation against any person who raises a concern in good faith about any behavior prohibited by this Code of Conduct. Such retaliation would be a violation of this Code of Conduct.

CONSEQUENCES OF VIOLATING THE CODE OF CONDUCT

Any violation of this Code of Conduct by the Supplier's Personnel may result in serious consequences, up to and including termination and possible referral to legal authorities.

FOR SUPPLIER's PERSONNEL:

I have received a copy of this Code of Conduct written in a language that I comprehend. I understand that if I have any questions about this Code of Conduct, I can contact [*enter name of Supplier's contact person(s) with relevant experience*] requesting an explanation.

Name of Supplier's Personnel: *[insert **name**]*

Signature: _____

Date: (day month year): *[insert **date**]*

Countersignature of authorized representative of the Supplier:

Signature: _____

Date: (day month year): *[insert **date**]*

ATTACHMENT 1: Behaviors constituting SEA and behaviors constituting SH

ATTACHMENT 1 TO THE CODE OF CONDUCT FORM

BEHAVIORS CONSTITUTING SEXUAL EXPLOITATION AND ABUSE (SEA) AND BEHAVIORS CONSTITUTING SEXUAL HARASSMENT (SH)

The following non-exhaustive list is intended to illustrate types of prohibited behaviors.

(1) **Examples of sexual exploitation and abuse** include, but are not limited to:

- A Supplier's Personnel tells a member of the community that he/she can get them jobs related to the project site in exchange for sex.
- A Supplier's Personnel rapes, or otherwise sexually assaults a member of the community.
- A Supplier's Personnel denies a person access to the Project Site/s unless he/she performs a sexual favor.
- A Supplier's Personnel tells a person applying for employment under the Contract that he/she will only hire him/her if he/she has sex with him/her.

(2) **Examples of sexual harassment in a work context**

- A Supplier's Personnel comment on the appearance of another Supplier's Personnel (either positive or negative) and sexual desirability.
- When a Supplier's Personnel complains about comments made by another Supplier's Personnel on his/her appearance, the other Supplier's Personnel comment that he/she is "asking for it" because of how he/she dresses.
- Unwelcome touching of a Supplier's Personnel or Purchaser's Personnel by another Supplier's Personnel.
- A Supplier's Personnel tells another Supplier's Personnel that he/she will get him/her a salary raise, or promotion if he/she sends him/her naked photographs of himself/herself.

TECHNICAL CAPABILITIES

*[**Note**: To be completed by the Proposer and, if JV, by each member]*

Proposer's Legal Name: *[insert **Proposer's Legal Name**]*

Date: *[insert **Date**]*

JV Member Legal Name: *[insert **JV Member Legal Name**]*

RFP No.: *[insert **RFP number**]*

Page _____ of _____ pages

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

MANUFACTURER'S AUTHORIZATION

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

Invitation for Proposals Title and No.: *[Purchaser insert: **RFP Title and Number**]*

To: *[Purchaser insert: **Purchaser'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 hereby authorize *[insert: **name of Proposer or Joint Venture**]* located at *[insert: **address of Proposer or Joint Venture**]* (hereinafter, the "Proposer") to submit a proposal 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 request for proposals process results in a Contract between you and the Proposer, 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)]

SUBCONTRACTOR'S AGREEMENT

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

Invitation for Proposals Title and No.: *[Purchaser insert: **RFP Title and Number**]*

To: *[Purchaser insert: **Purchaser's Officer to receive the Subcontractor's Agreement]***

WHEREAS *[insert: **Name of Subcontractor**],* having head offices at *[insert: **address of Subcontractor**],* have been informed by *[insert: **name of Proposer or Joint Venture**]* located at *[insert: **address of Proposer or Joint Venture**]* (hereinafter, the "Proposer") that it will submit a proposal 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 Proposal 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)]

List of Proposed Subcontractors

	Item	Proposed Subcontractor	Place of Registration & Qualifications

INTELLECTUAL PROPERTY FORMS

Notes to Proposers on working with the Intellectual Property Forms

In accordance with ITP 11.1(j), Proposers must submit, as part of their proposals, lists of all the Software included in the proposal assigned to one of the following categories: (a) System, General-Purpose, or Application Software; (b) Standard or Custom Software; (c) Proprietary or Open Source. Proposers must also submit a list of all Custom Materials. These categorizations are needed to support the Intellectual Property in the GCC and SCC. The Proposer must also include the text of the software licenses for the software titles proposed.

Software List

	(select one per title)			(select one per title)		(select one per title)	
Title	System	General-Purpose	Application	Standard	Custom	Proprietary	Open Source
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							

Attachments: Proposed Software Licenses

List of Custom Materials

Custom Materials
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*

CONFORMANCE OF INFORMATION SYSTEM MATERIALS

Format of the Technical Proposal

In accordance with ITP 16.2, the documentary evidence of conformity of the Information System to the request for proposals documents includes (but is not restricted to):

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

(b). A written confirmation by the Proposer 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 proposal, the Proposer must use the Technical Responsiveness Checklist (Format). Failure to do so increases significantly the risk that the Proposer's Technical Proposal 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 Proposer's Technical Proposal.

Note: The Technical Requirements are voiced as requirements of the *Supplier* and/or the *System*. The Proposer'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 Proposer should indicate *that* – and to the greatest extent practical – *how* the Proposer 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

Official Use Only

requirement is for the Supplier to provide certifications (e.g., ISO 9001), copies of these certifications must be included in the Technical Proposal.

Note: As required in PDS 11.2 (j), include method statement, management strategies and implementation plans and innovations, to manage cyber security risks.

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

Note: As a matter of practice, the contract cannot be awarded to a Proposer whose Technical Proposal 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 proposal evaluation and contract award, Proposers are encouraged not to overload the supporting materials with documents that do not directly address the Purchaser's requirements.

(e). Any separate and enforceable contract(s) for Recurrent Cost items which the PDS ITP 17.2 required Proposers to propose.

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

Technical Responsiveness Checklist (Format)

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

FORM OF PROPOSAL SECURITY (BANK GUARANTEE)

[The bank shall fill in this Bank Guarantee Form in accordance with the instructions indicated.]

[Guarantor letterhead or SWIFT identifier code]

Beneficiary: *[Purchaser to insert its **name and address**]*

RFP No.: *[Purchaser to insert reference **number for the RFP**]*

Alternative No.*: [Insert identification No if this is a Proposal for an alternative]*

Date: *[Insert **date of issue**]*

PROPOSAL GUARANTEE No.: *[Insert **guarantee reference number**]*

We have been informed that *[insert **name of the Proposer**, which in the case of a joint venture shall be the name of the joint venture (whether legally constituted or prospective) or the names of all members thereof]* (hereinafter called "the Applicant") has submitted or will submit the Beneficiary its proposal (hereinafter called "the Proposal") for the execution of *[insert **Name of Contract**]* under Request for Proposals No. [*insert **number**]* ("the RFP").

Furthermore, we understand that, according to the Beneficiary's, Proposals must be supported by a Proposal guarantee.

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 *[insert **amount in figures** ([insert **amount in words**])]* 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 the demand, stating that either the Applicant:

(a) has withdrawn its Proposal prior to the Proposal validity expiry date set forth in the Applicant's Letter of Proposal, or any extended date provided by the Applicant; or

(b) having been notified of the acceptance of its Proposal by the Beneficiary prior to the expiry date of the Proposal validity or any extension thereof provided by the Applicant has failed to: (i) execute the Contract Agreement, if required, or (ii) furnish the performance security, in accordance with the Instructions to Proposers ("ITP") of the Beneficiary's request for proposals document.

This guarantee will expire: (a) if the Applicant is the successful Proposer, upon our receipt of copies of the contract agreement signed by the Applicant and the Performance Security issued to the Beneficiary in relation to such Contract Agreement; or (b) if the Applicant is not the successful Proposer, upon the earlier of (i) our receipt of a copy of the Beneficiary's notification to the Applicant of the results of the request for proposals process; or (ii) twenty-eight days after the expiry date of the Proposal validity.

Official Use Only

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

This guarantee is subject to the Uniform Rules for Demand Guarantees (URDG) 2010 Revision, ICC Publication No. 758.

_____

[signature(s)

Official Use Only

Letter of Proposal - Financial Part

INSTRUCTIONS TO PROPOSERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE DOCUMENT

The Proposer must prepare this Letter of Proposal on stationery with its letterhead clearly showing the Proposer's complete name and business address.

Note: All italicized text is to help Proposers in preparing this form.

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

Request for Proposal No.: [*insert identification*]

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

To: **[*insert complete name of Purchaser*]**

We, the undersigned, hereby submit the second part of our Proposal, the Proposal Price and Priced Activity Schedule. This accompanies the Letter of Proposal- Technical Part.

In submitting our Proposal, we make the following additional declarations:

(a) **Proposal Validity**: Our Proposal shall be valid until *[insert day, month and year in accordance with ITP 19.1]*, and it shall remain binding upon us and may be accepted at any time on or before this date;

(b) **Total Price**: The total price of our Proposal, excluding any discounts offered in item (c) below is:

Total price is: [*insert the total price of the Proposal in words and figures, indicating the various amounts and the respective currencies, as applicable*];

(c) **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*];

(d) **Commissions,** gratuities **and fees:** We have paid, or will pay the following commissions, gratuities, or fees with respect to the procurement 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.")

Name of the Proposer:*[*insert complete name of the Proposer*]

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

Title of the person signing the Proposal: [*insert complete title of the person signing the Proposal*]

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*]

*: In the case of the Proposal submitted by a Joint Venture specify the name of the Joint Venture as Proposer.

**: Person signing the Proposal shall have the power of attorney given by the Proposer. The power of attorney shall be attached with the Proposal Schedules

Official Use Only

PRICE SCHEDULE FORMS

Notes to Proposers on working with the Price Schedules

General

1. The Price Schedules are divided into separate Schedules as follows:

   3.1 Grand Summary Cost Table

   3.2 Supply and Installation Cost Summary Table

   3.3 Recurrent Cost Summary Table

   3.4 Supply and Installation Cost Sub-Table(s)

   3.5 Recurrent Cost Sub-Tables(s)

   3.6 Country of Origin Code Table

   [insert: ***any other Schedules as appropriate*** *]*

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 Proposers shall have read the Technical Requirements and other sections of these request for proposals 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.

3. If Proposers are unclear or uncertain as to the scope of any item, they shall seek clarification in accordance with the Instructions to Proposers in the request for proposals documents prior to submitting their proposal.

Pricing

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

5. Proposal prices shall be quoted in the manner indicated and in the currencies specified in ITP 18.1 and ITP 18.2. Prices must correspond to items of the scope and quality defined in the Technical Requirements or elsewhere in these request for proposals documents.

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

7. Payments will be made to the Supplier in the currency or currencies indicated under each respective item. As specified in ITP 18.2, no more than three foreign currencies may be used.

Official Use Only

3.1 Grand Summary Cost Table

		[insert: ***Local Currency]*** ***Price***	*[insert:* ***Foreign Currency A]*** ***Price***	*[insert:* ***Foreign Currency B]*** ***Price***	*[insert:* ***Foreign Currency C]*** ***Price***
1.	Supply and Installation Costs (from Supply and Installation Cost Summary Table)				
2.	Recurrent Costs (from Recurrent Cost Summary Table)				
4.	Grand Totals (to Proposal Submission Form)				

Name of Proposer:		
Authorized Signature of Proposer:		

Official Use Only

3.2 Supply and Installation Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITP 17 and 18.

			Supply & Installation Prices				
			Locally supplied items	**Items supplied from outside the Purchaser's Country**			
Line Item No.	**Subsystem / Item**	**Supply and Installation Cost Sub-Table No.**	*[insert: **Local Currency**]* Price	*[insert: **Local Currency**]* Price	*[insert: **Foreign Currency A]*** Price	*[insert: **Foreign Currency B]*** Price	*[insert: **Foreign Currency C]*** Price
0	Project Plan	- -	- -	- -	- -	- -	- -
1	Subsystem 1	1					
SUBTOTALS							
TOTAL (To Grand Summary Table)							

Note: - - indicates not applicable. "Indicates repetition of table entry above. Refer to the relevant Supply and Installation Cost Sub-Table for the specific components that constitute each Subsystem or line item in this summary table

Name of Proposer:		
Authorized Signature of Proposer:		

Official Use Only

3.3 Recurrent Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITP 17 and ITP 18.

Line Item No.	**Subsystem / Item**	**Recurrent Cost Sub-Table No.**	*[insert:* ***Local Currency]*** ***Price***	*[insert:* ***Foreign Currency A]*** ***Price***	*[insert:* ***Foreign Currency B]*** ***Price***	*[insert:* ***Foreign Currency C]*** ***Price***
y	Recurrent Cost Items					
y.1	____	y.1				
	Subtotals (to Grand Summary Table)					

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

Name of Proposer:		
Authorized Signature of Proposer:		

3.4 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 ITP 17 and ITP 18.

				Unit Prices / Rates					**Total Prices**				
				Supplied Locally	**Supplied from outside the Purchaser's Country**				**Supplied Locally**	**Supplied from outside the Purchaser's Country**			
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: **foreign currency C]***	*[insert: **local currency]***	*[insert: **local currency]***	*[insert: **foreign currency A]***	*[insert: **foreign currency B]***	*[insert: **foreign currency C]***
X.1	____	- -	- -	- -	- -	- -	- -	- -					
Subtotals (to *[insert: **line item**]* of Supply and Installation Cost Summary Table)													

Note: - - indicates not applicable.

Name of Proposer:		
Authorized Signature of Proposer:		

3.5 Recurrent Cost Sub-Table *[insert: **identifying number**] -- **Warranty Period***

Line item number**:** *[specify: **relevant line item number from the Recurrent Cost Summary Table** – (e.g., y.1)]*

Currency: *[specify: **the currency of the Recurrent Costs in which the costs expressed in this Sub-Table are expressed**]*

*[As necessary for operation of the System, specify: **the detailed components and quantities in the Sub-Table below for the line item specified above, modifying the sample components and sample table entries as needed.** Repeat the Sub-Table as needed to cover each and every line item in the Recurrent Cost Summary Table that requires elaboration.]*

Costs MUST reflect prices and rates quoted in accordance with ITP 17 and ITP 18.

		Maximum all-inclusive costs (for costs in *[insert: **currency**]*)						
Component No.	Component	Y1	Y2	Y3	Y4	...	Yn	Sub-total for *[insert: **currency**]*
1.	Hardware Maintenance	Incl. in Warranty	Incl. in Warranty	Incl. in Warranty				
2.	Software Licenses & Updates	Incl. in Warranty						
2.1	System and General-Purpose Software	Incl. in Warranty						
2.2	Application, Standard and Custom Software	Incl. in Warranty						
3.	Technical Services							
3.1	Sr. Systems Analyst							

		Maximum all-inclusive costs (for costs in *[insert: **currency**]*)						
Component No.	Component	Y1	Y2	Y3	Y4	...	Yn	Sub-total for *[insert: **currency**]*
3.2	Sr. Programmer							
3.3	Sr. Network Specialist, ….. etc.							
4.	Telecommunications costs [to be detailed]							
5.	[Identify other recurrent costs as may apply]							
	Annual Subtotals:							- -
Cumulative Subtotal (to *[insert: **currency**]* entry for *[insert: **line item**]* in the Recurrent Cost Summary Table)								

Name of Proposer:		
Authorized Signature of Proposer:		

3.6 Country of Origin Code Table

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

SECTION V - ELIGIBLE COUNTRIES

Eligibility for the Provision of Information System

In reference to ITP 4.8 and ITP 5.1, for the information of the Proposers, at the present time firms and information systems from the following countries are excluded from this procurement process:

Under ITP 4.8(a) and ITP 5.1: **None**

Under ITP 4.8(b) and ITP 5.1: **None**

Official Use Only

SECTION VI - FRAUD AND CORRUPTION

(Section VI shall not be modified)

1. Purpose

1.1 The Bank's Anti-Corruption Guidelines and this annex apply with respect to procurement under Bank Investment Project Financing operations.

2. Requirements

2.1 The Bank requires that Borrowers (including beneficiaries of Bank financing); bidders (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, observe the highest standard of ethics during the procurement process, selection and contract execution of Bank-financed contracts, and refrain from Fraud and Corruption.

2.2 To this end, the Bank:

a. Defines, for the purposes of this provision, the terms set forth below as follows:

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:

(a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation 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

(b) acts intended to materially impede the exercise of the Bank's inspection and audit rights provided for under paragraph 2.2 e. below.

b. Rejects a proposal for award if the Bank determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-

Official Use Only

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;

c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring misprocurement, if the Bank determines at any time that representatives of the Borrower or of a recipient of any part of the proceeds of the loan engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the Borrower having taken timely and appropriate action satisfactory to the Bank to address such practices when they occur, including by failing to inform the Bank in a timely manner at the time they knew of the practices;

d. Pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with the Bank's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a Bank-financed contract, financially or in any other manner;[1] (ii) to be a nominated[2] sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a Bank-financed contract; and (iii) to receive the proceeds of any loan made by the Bank or otherwise to participate further in the preparation or implementation of any Bank-financed project;

e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by a Bank loan, requiring (i) bidders (applicants/proposers), consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents, personnel, permit the Bank to inspect[3] 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 Bank.

---

[1] For the avoidance of doubt, a sanctioned party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in a consultancy, and bidding, 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] A nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider (different names are used depending on the particular bidding document) is one which has been: (i) included by the bidder in its pre-qualification application or bid because it brings specific and critical experience and know-how that allow the bidder to meet the qualification requirements for the particular bid; or (ii) appointed by the Borrower.

[3] Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Bank or persons appointed by the Bank 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 thereof 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 thereof as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

Official Use Only

PART 2 – PURCHASER'S REQUIREMENTS

Official Use Only
Official Use Only

SECTION VII - REQUIREMENTS OF THE INFORMATION SYSTEM

(INCLUDING TECHNICAL REQUIREMENTS, IMPLEMENTATION SCHEDULE, SYSTEM INVENTORY TABLES, BACKGROUND AND INFORMATIONAL MATERIALS)

Notes on preparing the Requirements of the Information System

The Requirements of the Information System comprise four significant and closely related subsections:

- *Technical Requirements*
- *Implementation Schedule*
- *System Inventory Tables*
- *Background and Informational Materials*

Each subsection is presented and discussed separately

Official Use Only
Official Use Only

Technical Requirements

Notes on preparing the Technical Requirements

To the greatest extent possible, the Technical Requirements should be expressed in terms of the Purchaser's business activities, rather than a technological design. This leaves it up to the market to determine what specific Information Technologies can best satisfy these business needs. This is particularly relevant where the Information System will embody complex business logic in the form of application software.

Even in the case of a relatively straight-forward Information System, where the business needs can be clearly linked to technological and methodological requirements known in advance of any procurement, the requirements must still be vendor-neutral and admit the widest possible range of technical responses.

A specification of a required level of standard performance benchmark test is more appropriate, allowing different technical approaches to achieving the Purchaser's functional and performance objectives. In general, the Purchaser should try to use widely accepted direct measures of performance and functionality whenever possible and carefully review specifications for those that might dictate technical architectures.

Where national standards or codes of practice are specified, the Purchaser should include a statement that other national or international standards "that are substantially equivalent" will also be acceptable.

It is important that the Technical Requirements clearly identify which are mandatory features (for which a proposal's nonconformance might require rejection for non-responsiveness) and which are preferable features that can be included or excluded from a Proposal at the Proposer's option.

Any applicable environmental and social requirements shall be specified. The ES requirements should be prepared in manner that does not conflict with the relevant General Conditions (and the corresponding Special Conditions of Contract if any) and other parts of the specifications.

1.6.4 below indicates noise levels and emission standard. Additional environmental and social requirements/ sustainable procurement requirements, as applicable, may include, but not limited to, aspects related to the protection of the environment including management and safety of hazardous materials, resource efficiency, pollution prevention and management measures.

The following presents a sample outline format for the Technical Requirements. This can and should be adapted to meet the Purchaser's needs for the specific Information System to be procured.

Official Use Only
Official Use Only

Technical Requirements

Table of Contents: Technical Requirements

A. Acronyms Used in The Technical Requirements 143

0.1 Acronym Table 143

B. Functional, Architectural and Performance Requirements.....146

1.1 Legal and Regulatory Requirements to be met by the Information System146
1.2 Business Function Requirements to be met by the Information System 151
1.3 Architectural Requirements to be met by the Information System 143
1.4 Systems Administration and Management Functions Required to be met by the Information System 144
1.5 Performance Requirements of the Information System.....144
1.6 Cyber Security 154
1.6.1 [Include contract specific cyber security requirements, including cyber security accreditations, as appropriate.] 154

C. Service Specifications – Supply & Install Items.....155

2.1 System Analysis, Design and Customization/Development.....155
2.2 Software Customization / Development 155
2.3 System Integration (to other existing systems).....156
2.4 Training and Training Materials 207
2.5 Data Conversion and Migration.....210
2.6 Documentation Requirements.....211
2.7 Requirements of the Supplier's Technical Team.....212

D. Technology Specifications – Supply & Install Items.....218

3.0 General Technical Requirements.....230
3.1 Computing Hardware Specifications *[If this has to be specified; As applicable]* 231
3.2 Network and Communications Specifications*[If this has to be specified; As applicable]* 231
3.3 Ancillary Hardware Specifications*[If this has to be specified; As applicable]*247

Official Use Only

3.4 Standard Software Specifications *[If this has to be specified; As applicable]* 248
3.5 Consumables 249
3.6 Other Non-IT Goods 249

E. Testing and Quality Assurance Requirements 249

4.1 Inspections 249
4.2 Pre-commissioning Tests 249
4.3 Operational Acceptance Tests 249

F. Service Specifications – Recurrent Cost Items 252

5.1 Warranty Defect Repair 252
5.2 Technical Support 252
5.3 Requirements of the Supplier's Technical Team 252

A. ACRONYMS USED IN THE TECHNICAL REQUIREMENTS

0.1 Acronym Table

Note: *Compile a table of organizational and technical acronyms used in the Requirements. This can be done, for example, by extending the following table.*

	Term	Explanation
	bps	bits per second
	cps	characters per second
	DBMS	Database Management System
	DOS	Disk Operating System

Official Use Only
Official Use Only

	Term	Explanation
	dpi	dots per inch
	Ethernet	IEEE 802.3 Standard LAN protocol
	GB	gigabyte
	Hz	Hertz (cycles per second)
	IEEE	Institute of Electrical and Electronics Engineers
	ISO	International Standards Organization
	KB	kilobyte
	kVA	Kilovolt ampere
	LAN	Local area network
	lpi	lines per inch
	lpm	lines per minute
	MB	megabyte
	MTBF	Mean time between failures
	NIC	Network interface card
	NOS	Network operating system
	ODBC	Open Database Connectivity
	OLE	Object Linking and Embedding
	OS	Operating system
	PCL	Printer Command Language
	ppm	pages per minute

Official Use Only
Official Use Only

	Term	Explanation
	PS	PostScript -- Adobe page description language
	RAID	Redundant array of inexpensive disks
	RAM	Random access memory
	RISC	Reduced instruction-set computer
	SCSI	Small Computer System Interface
	SNMP	Simple Network Management Protocol
	SQL	Structured Query Language
	TCP/IP	Transmission Control Protocol / Internet Protocol
	V	Volt
	WLAN	Wireless LAN

Official Use Only
Official Use Only

B. FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS

INTRODUCTION

The ICT Authority is an Agency under the Ministry of Information Communication Technology & The Digital Economy, functioning as a key implementing agency of the ministry. The ICT Authority (ICTA) plays a pivotal role in the advancement and execution of ICT Infrastructure, e-governance and Cybersecurity projects and initiatives in the Government. It offers a comprehensive range of ICT services, including software development, managing countrywide Government network infrastructure, datacenter and cloud services, as well as web applications development and hosting. ICTA is entrusted with the responsibility of developing and maintaining various government websites and portals, facilitating online services and transactions for citizens and businesses in a secure manner.

The Ministry of Information, Communication and The Digital Economy, through the ICTA Authority hosts very Critical Government Infrastructure AND Digital Systems which require round-the-clock continuous protection, visibility and monitoring to ensure the Government's technology assets and services are notin any way adversely impacted by Cyber threats. Just to name a few, these include;

a. National Public Key Infrastructure (NPKI-GovCA)
b. Government Core Metro-networks (NOFBI, GCCN, CCP) - supporting all MCDAs.
c. Government E-mail Services.
d. Government Unified Communication Platform.
e. International Internet Gateways (IGW)
f. Government Datacenters (Konza, GDC, CBC, etc)
g. National Network Operation Centre (NOC)
h. ALL Government Websites
i. ALL External phasing Applications for delivery of various MCDA's and citizenry services e.g. (NEMIS, IPRS, E-Citizen, TIMS, ArdhiSasa, etc.)
j. Databases, Servers and data centers, and other technologies

The strategic benefits of establishing a Government Systems Security Operation Centre (GOVSOC) are anchored in the four main functions of an ICT GOVSOC which are;

Official Use Only
Official Use Only

a. To Provide a pro-active Cyber-risk Prevention and detection.
b. To provide a platform for Threats Analysis and Investigation.
c. To Provide a platform for Incidence Response and Management.
d. To Pro-Active Threat Intelligence Sharing

The ICT Authority has a vast network of offices and centers spread across the country up to county level, providing technical support and expertise to various government entities. It collaborates with various stakeholders, including government agencies, public sector organizations, and industry partners, to promote innovation, efficiency, and transparency in the delivery of government services. Overall, the ICT Authority plays a crucial role in the digital transformation of the Kenyan government, enabling efficient and accessible online services, data management, and IT solutions for the benefit of citizens and the administration. Security and sustained availability of such services being provided by ICTA is critical for the performance of public duties and acts in which the public are interested. Establishment of Government Security Operations Centres (GSOC) is envisaged for 24X7X365 monitoring and protection of the Government ICT infrastructure.

The ICT Authority (ICT-A) is thus seeking for Qualified bidders and Vendors for the establishment of a Government Security Operations Centre (GovSOC) to serve as a centralized capability for cybersecurity monitoring, threat detection, incident response, and coordination across Government Ministries, Departments, and Agencies (MDAs). The GovSOC is a critical component of the Government's broader digital transformation and cybersecurity resilience agenda, aimed at safeguarding national digital infrastructure, protecting government information assets, and enhancing the country's abilityto anticipate, prevent, detect, and respond to cyber threats. The establishment of the GovSOC is intended to deliver a secure, resilient, and scalable operational environment capable of supporting 24/7 national-level cybersecurity operations, incident coordination, and situational awareness.

The current Government cybersecurity monitoring environment comprises of a combination of decentralized security controls, limited visibility across MDAs, and fragmented monitoring and incident response capabilities. Existing arrangements rely on disparate tools, manual processes, and varying levels of maturity across institutions, resulting in inconsistent threat detection, delayed incident response, and limited situational awareness at a national level.

The Technical Requirements defined in this section set out the baseline specifications for the supply, delivery, installation, integration, testing, and commissioning of the GovSOC Information System. These requirements are intended to ensure that

Official Use Only
Official Use Only

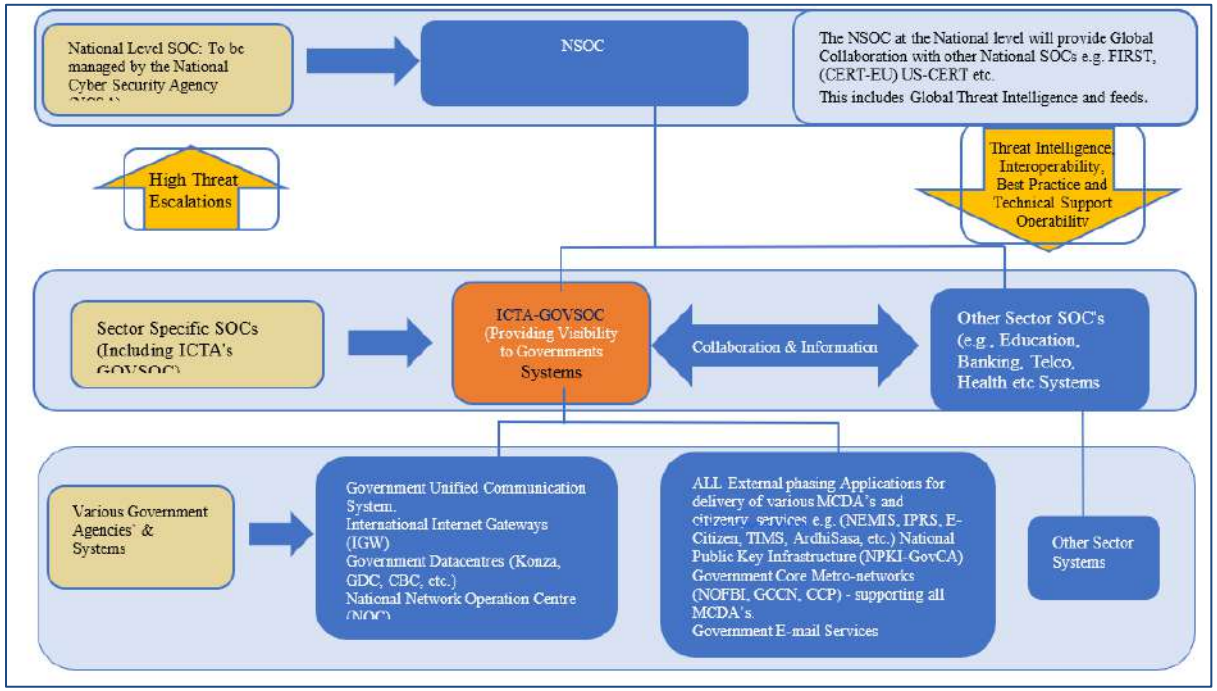
the GovSOC infrastructure, tools, and platforms are interoperable, resilient, secure by design and aligned with international best practices in cybersecurity operations, incident triage, threat intelligence, and service availability.

TheContract shall be executed through two sequential implementation phases, each with clearly defined deliverables, acceptance criteria, contractual milestones, and payment milestones. Progression to Phase II shall be subject to successful completion, testing, acceptance and formal sign-off of all Phase I deliverables. The phased implementation schedule and corresponding acceptance requirements are set out in the tables below.

Official Use Only
Official Use Only

SECURITY TOOLS & TECHNOLOGY STACK DEPLOYMENT PHASE I

The Implementation and Set-up of the Government Security Operation Centre (GOVSOC) shall be based on a hierarchy model as defined in the CMCA regulations and the National Cybersecurity Strategy. A multi-tier model of the Security Operations Centre design helps to effectively distribute responsibilities among different sectors of SOCs, according to the sector requirements, Systems Sensitivity and classification, mandate, skills availability and experience of SOC engineers and the complexity of issues they deal with. The envisaged model for the National SOC and Sector SOC (GovSOC) as depicted below



The GOVSOC will be established at:

- **ICT Authority Head Office :** Nairobi;
- **Disaster Recovery (DR) Site:** Private ICTA/Government Cloud

Official Use Only
Official Use Only

In the event of any service failures at Primary SOC in ICT Authority Head Office : Nairobi; operations shall automatically transition to the DR site at Private ICTA/Government Cloud for hardware/software failover , to ensure uninterrupted service delivery The DR for SOC operations shall incorporate, at a minimum, the following critical Security Technology

components implemented in a Phased Approach:

PHASE I: CORE OPERATIONAL GOVSOC CAPABILITY

1) Security Information & Event Manager (SIEM
2) Security Orchestration, Automation and Response (SOAR).
3) Anti- Distributed Denial of Service (Ant-DDOS)
4) Threat Intelligence Platform
5) SOC MISP & Ticket System

PHASE II: ADVANCED VISIBILITY AND MATURITY ENHANCEMENT

1) File Integrity Monitoring (FIM)
2) Advanced Attack Surface Management
3) Vulnerability Management

These components shall be deployed at both the Primary SOC and the DR site in High Availability (HA) configuration (at least N+1 redundancy at each site). The solutions must ensure:

- Automatically failover from the Primary SOC to the DR site in the event of failure, without any manual intervention.
- Continuous data synchronization between the Primary SOC and DR site at all times through automated tools.
- Provision by the VENDOR of all hardware, software, and ancillary components necessary for DR operations, including synchronization, failover, and operational continuity;
- Retention of a complete log archive (As per log retention policy of the Purchaser) at the DR site to ensure full forensic and compliance coverage.

This Request for Proposal (RFP) has therefore been issued for the selection of a Government Security Operations Service Provider (GOVSOC) to supply, implement, operate, and manage a comprehensive Government Cyber Security Operations Centre (GovSOC) Structured for implementation in two Phases for the ICT Authority. The objective of this engagement is to ensure that the Government Cyber Security Operations Centre (GovSOC) provides:

Official Use Only
Official Use Only

GOVSOC Strategic Objectives

1. Strengthen National Cyber Resilience
2. Provide Centralized Situational Awareness
3. Enhance Coordination Across Government Agencies

GOVSOC Operational Objectives

- Protect National Critical Information Infrastructure (CII)
- Continuous Knowledge development and Upskilling
- Establish 24/7 Monitoring and Rapid Incident Response
- Standardize Incident Response Across MDAs
- Implement Structured National Threat Intelligence
- Improve Visibility Through Standardized Telemetry

1.1 Legal and Regulatory Requirements to be met by the Information System

1.1 The Information System MUST comply with the following laws and regulations:

The proposed GOVSOC solution shall comply with applicable Kenyan laws, regulations, Government policies,standards and international good practices governing cybersecurity, information security, data protection and Government ICT operations.
The bidder shall provide a compliance matrix identifying each applicable legal, regulatory, policy and standards requirement and demonstrate how the proposed GOVSOC solution proposal will meet or support compliance with the requirement.

1.2 **The GOVSOC MIS Solution shall have the following features:**

The vendor shall provide a Managed Information System (MIS) to capture, present, and manage all information pertaining to the SOC components. MIS reports shall be supplied in a format and mode mutually agreed upon with the Purchaser, and at a periodicity defined in the SOC Operations Manual (e.g., yearly, quarterly, monthly, monthly, weekly, or daily). At a minimum, the MIS reports shall include:

The GOVSOC MIS Solution shall have the following features:

(a) Uptime and availability of systems.
(b) Incident reports covering disruptions, downtime, security violations, etc.
(c) Any other report relevant to the scope of work, as required by the Purchaser.

Official Use Only
Official Use Only

The GOVSOC MIS Solution shall have the following features:

a. The GOVSOC MIS solution shall be a web-based portal.
b. The GOVSOC MIS solution shall be integrated with the supplied security technology solutions
c. The GOVSOC MIS Solution should be able to ingest data from the supplied solutions and generate various customized dashboards as per the requirements of the ICT Authority.
d. The GOVSOC MIS solution shall seamlessly integrate with the ITSM solution for SLA measurement, penalty calculation, reporting etc. and shall provide customized dashboards related to SLAs and penalties.
e. The core features of the MIS solution should include but not limited to following:
    i. Availability of the supplied components.
    ii. Health and performance of the supplied components.
    iii. Track changes and revisions to the components supplied.
    iv. Track SLA compliance for the components supplied.
    v. Generate SLA reports and other custom reports for the data ingested in the MIS.
    vi. Perform predictive analytics based on past data and forecast future performance, downtimes, impacts.
    vii. Track availability and performance of the supplied manpower.
    viii. Track incident lifecycle.
    ix. Identify potential areas of underperformance and improvement.
    x. Calculate the applicable penalties as per the SLA compliance and the contractual terms.
    xi. Generate Business Intelligence and Analytics Reports as per the requirements of the Purchaser.
    xii. Build custom dashboards, reports and live analytics based on custom queries from the user.
    xiii. Advanced Search Functionality to search through all the data ingested into the MIS platform.
f. Define multiple templates for monitoring and tracking different contracts and their respective SLA compliance.
g. Retention of all ingested data and generated reports for the entire contract period.
h. Integrate MIS with new data sources.
i. Patching and bug fixing for the MIS Platform.
j. Generate Alerts based on specific user-defined conditions.
k. Send reports, alerts, notifications through email, SMS, other messaging platforms.
l. MIS should also integrate with SIEM, SOAR and other platforms.

Official Use Only
Official Use Only

1.3 Business Function Requirements to be met by the GOVSOC Technology Systems Stack –

1.2.1 The Information System MUST support the following business functions

The proposed GOVSOC Technology Systems stack proposal shall provide an integrated, operational and scalable cybersecurity capability to support continuous monitoring, detection, analysis, threat intelligence, orchestration, response and mitigation of cyber threats across the Government digital environment.

The scope of supply and responsibility for GovSOC infrastructure, cybersecurity technologies, connectivity, installation, integration and operational support shall be as defined in the Scope of Supply and Responsibility Matrix and the corresponding Technical Specifications and Price Schedules. All hardware, software, equipment and services expressly identified as Supplier deliverables shall be supplied and commissioned by the Supplier, while ICTA shall provide only the facilities Tabulated below. The Supplier shall be responsible for integrating the supplied components into a functional GovSOC solution.The bidder shall, however, be responsible for providing, configuring and operationalising the Core Enterprise Security Software and Technology Tools required to deliver the intended GOVSOC capabilities, including but not limited to Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Threat Intelligence Platform (TIP), Anti-DDoS and other associated cybersecurity technologies.

The proposed solutions shall operate as an integrated security ecosystem, with the capability to exchange security events, threat intelligence, alerts and response actions across platforms, while supporting interoperability with existing Government ICT and cybersecurity infrastructure.

The business functions specified below shall therefore focus on the capabilities and outcomes that the integrated GOVSOC solution must deliver, rather than the underlying hardware or compute infrastructure, and shall include the required configuration, customisation, integration, support, capacity building and ongoing optimisation throughout the five (5) year maintenance and support period.

The following items shall be provided ICTA Subject to confirming the availability and adequacy of its existing facilities

Official Use Only
Official Use Only

	Component or service	ICTA responsibility	Supplier responsibility
	GovSOC premises and physical facilities	Provide designated premises, physical access and existing building facilities.	Identify site requirements and install equipment in the designated space.
	Internet connectivity and government network access	Provide existing internet connectivity, bandwidth and government network access where available and confirmed adequate.	Specify bandwidth, latency, IP addressing and connectivity requirements; configure and integrate the solution.
	Power and electrical infrastructure	Provide building power supply and electrical access.	Supply and install the specified UPS and any other power-protection equipment included in the procurement.

1.6 Cyber Security

1.6.1 Cyber Security Management Strategy

Cybersecurity Management Strategy: The Proposal shall include a cybersecurity management strategy applicable to the Information System and the related goods, services, configuration, implementation, warranty, and support obligations. The cybersecurity provisions shall address, at a minimum:

- Secure configuration and hardening;
- Identity and privileged-access management;
- Encryption and authentication standards;
- Firmware and vulnerability management;
- Security updates during warranty and support;
- Logging and incident notification;
- Protection of management-plane traffic;
- Cloud-service and data-location requirements, where applicable;
- Handover of credentials and configurations;
- Removal of default passwords and undocumented remote access.

Official Use Only
Official Use Only

C. SERVICE SPECIFICATIONS – SUPPLY & INSTALL ITEMS

The Scope of activities to be performed by the successful vendor as part of work includes but **NOT** LIMITED to the following:

2.1 System Analysis, Design and Customization/Development

a) Supply, install, configure, implement, operationalize and maintain all components of the integrated SOC solution.
b) Develop and deploy a secure, resilient solution architecture leveraging the supplied SOC components.
c) Optimize SIEM log ingestion to minimize effective EPS while maintaining required log retention and archival requirements.
d) Develop and implement at least 120 SIEM/SOAR playbook rules, including correlation and response logic.
e) Continuously monitor, tune and update playbooks based on the operating environment and emerging requirements.
f) Establish baseline security hardening for all supplied and deployed infrastructure, applications, databases and services using CIS benchmarks.
g) Create, train, deploy and manage AI/ML models for approved SOC use cases.
h) Design and develop dashboards, visualizations, alerts, correlation rules and reports.
i) Establish a virtual simulation/test-bed environment replicating relevant security technologies and threat scenarios.
j) Support assessment and compliance of the GovSOC against SOC-CMM requirements and maintain compliance throughout the contract.

2.2 Software Customization / Development

2.2.1 The Supplier MUST perform Software Customization / Development using a formal software development methodology with the following characteristics and/or with the following technologies and/or tools.

a) Configure and customize SIEM/SOAR platforms to support ICT Authority-specific use cases.
b) Develop and configure correlation rules and detection logic.
c) Develop and implement the minimum 120 playbooks.
d) Develop and configure customized dashboards and visualizations.
e) Configure role-based and organization-specific dashboards.
f) Develop customized alerts, reports and automated workflows.
g) Develop and deploy approved AI/ML models and associated use cases.
h) Continuously tune and enhance detection rules, playbooks, dashboards and models based on operational requirements.

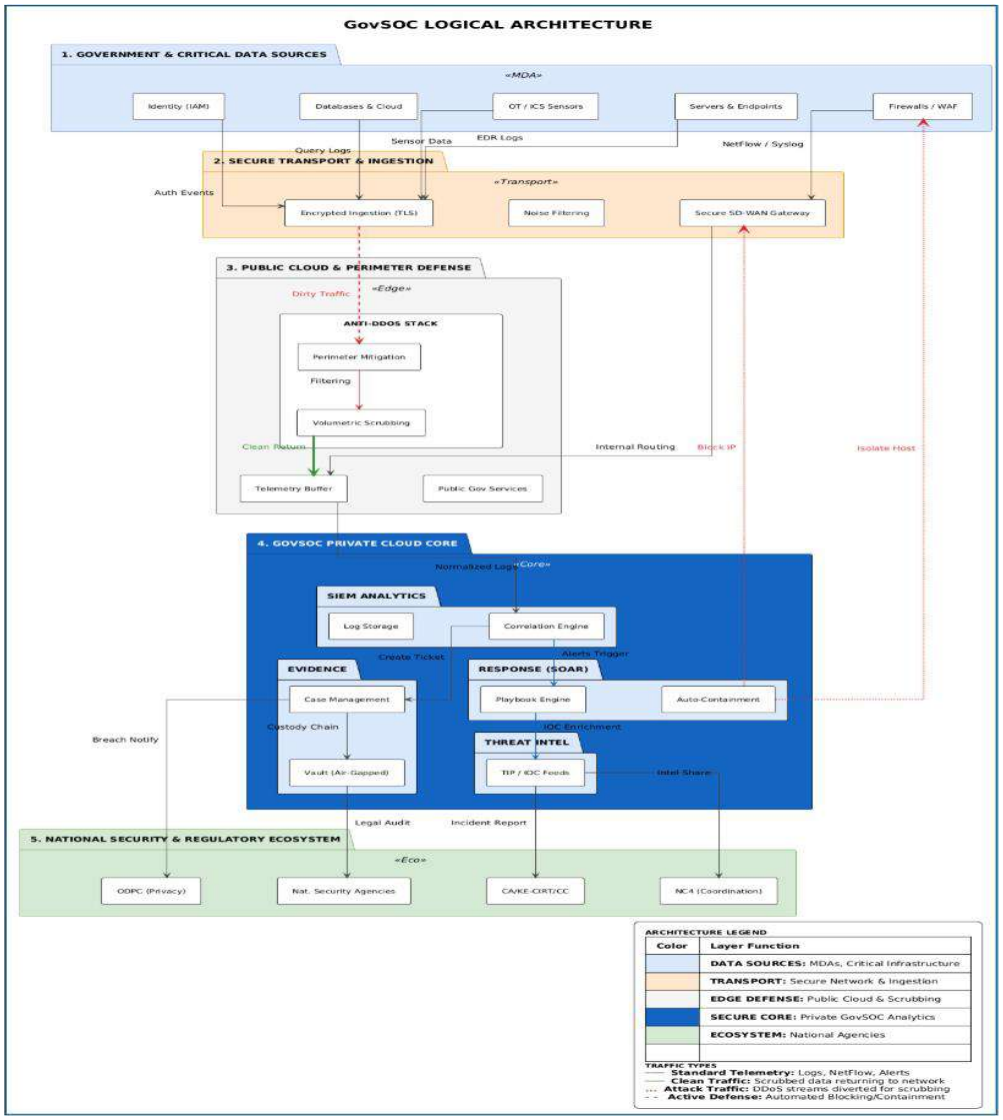
Official Use Only
Official Use Only

i) This prevents a bidder from simply claiming

2.3 System Integration (to other existing systems) –

The GovSOC Logical Architecture is designed as a strict pipeline that segregates data flow into distinct functional tiers. This design ensures that raw telemetry from government entities is securely ingested, rigorously scrubbed of attacks, and normalized before it ever reaches the analytical core. Architecture prioritizes the **integrity of the decision-making "brain"** (The Core) by placing it behind a robust Edge Defense layer, shielding it from direct exposure to volumetric internet attacks through functional boundaries of the defined Layered
architecture of the Security Technology stack at various layers

Official Use Only
Official Use Only



2.3.1 The Supplier MUST perform the following Integration Services

Official Use Only

a) Integrate the supplied SOC components with existing ICT Authority infrastructure, including but not limited to:
   i. Central logging platforms
   ii. Threat intelligence platforms
   iii. SSO/IAM
   iv. Endpoint security solutions
   v. Government email
   vi. SMS gateway
   vii. Databases
   viii. Applications
   ix. Network infrastructure
   x. Existing security technologies
   xi. Other ICT Authority platforms

b) Ensure logs and audit trails from all supplied components are retained locally for the specified period and streamed in real time to the Purchaser's central logging solution.
a) Enable logging on all supplied on-premise ICT systems and stream raw logs to the Purchaser's log management platform without alteration.
b) Integrate logs from the Purchaser's existing ICT systems with the supplied SIEM.
c) Configure SIEM live-log and archival capabilities.
d) Configure log archival/retention at the DR site.
e) Implement and conduct quarterly DR/switchover drills.
f) Support integration and coordination with Ministry/Department SOCs.
g) Facilitate coordination with other Government cybersecurity agencies through the sectorial cybersecurity structure.
h) Integrate and utilize the Purchaser's supplied vulnerability assessment tools.

Official Use Only
Official Use Only

GOVSOCAnalysts Compute and Hardware Devices

Technical requirements shall be classified as Mandatory (M) or Desirable (D), as shown in the M/D column of the checklist below. Only failure to meet an explicitly designated Mandatory requirement shall result in technical disqualification. Desirable requirements shall be assessed through the applicable rated criteria in Section III, Evaluation and Qualification Criteria.
Requirements shall be based on functional, security, interoperability, and performance outcomes. Equivalent technical approaches, including integrated and interoperable multi-vendor solutions, shall be accepted where they demonstrably meet the specified requirements.

No.	Technical & Functional Specification Description	M/D	Compliance (Y/N)	Reference / Page
4. MODULAR UNINTERRUPTIBLE POWER SUPPLY (UPS) SYSTEM				
4.1	Topology & Load Sizing: Online double-conversion topology sized >=125% of connected load (Best-in-Class: Modular N+1 with A+B feeds and >=50% scalable growth).	**M**		
4.2	Battery Runtime & Generator ATS: Minimum >=30 min runtime at full load (Best-in-Class: >=90 min, or >=30 min with auto-start generator, ATS <10 sec transfer, and >=24 hr fuel autonomy).	**M**		
4.3	Power Efficiency & Monitoring: Energy efficiency >=94% at 50–100% load with SNMP monitoring (Best-in-Class: >=97%, Li-ion batteries, full remote alerting, 24x7 support).	**M**		
4.4	Grid Waveform Compliance: Output compliant with the ITIC (CBEMA) curve for voltage sag/surge ride-through.	**M**		
4.5	Power Distribution Redundancy: N+1 minimum redundancy with dual A+B feed distribution to all downstream racks.	**D**		
4.6	Battery Technology Lifecycle: Li-ion battery technology preferred for lifespan (8–10 yrs vs 3–5 yrs VRLA) and reduced footprint/thermal load.	**D**		
4.7	Generator Failover Integration: Automatic Transfer Switch (ATS) with tested transfer time <10 sec; fuel autonomy >=24 hrs at full load for generator.	**D**		

Official Use Only
Official Use Only

No.	Technical & Functional Specification Description	M/D	Compliance (Y/N)	Reference / Page
4.8	Infrastructure Integration & Certification: Integration with DCIM/BMS; remote firmware update capability; NEBS or IEC 62040 compliance.	**D**		
4.9	Maintenance Bypass: Manual/static maintenance bypass switch enabling zero-downtime maintenance.	**M**		
5. SOC ANALYST WORKSTATIONS & COMPUTE				
5.1	Compute Hardware Spec: Core i7 / Ryzen 7 class, 32 GB RAM, 1 TB SSD, TPM 2.0 (Best-in-Class: >=64 GB RAM, >=2 TB NVMe, discrete GPU, 5-yr on-site warranty).	**M**		
5.2	Analyst Multi-Display Setup: Dual 24" FHD (1920x1080) monitors (Best-in-Class: Triple 27" or dual 32" 4K, height-adjustable).	**M**		
5.3	Floor Workspace & Ergonomics: Minimum >=4 m² per analyst, ergonomic desks, structured cabling, access control, CCTV (Best-in-Class: Biometric access, tray/raised-floor cabling).	**M**		
5.4	Endpoint Data Exfiltration Prevention: Hardware root of trust (TPM 2.0) plus port-lockdown (USB disabled by policy) for data-exfiltration control.	**M**		
5.5	Graphics Rendering Performance: Independent GPU output per monitor (not integrated-graphics splitting) to avoid rendering lag on SIEM dashboards.	**D**		
5.6	Secure Console Switching: KVM-over-IP switching for analysts working across classified/unclassified networks (air-gapped consoles).	**D**		
5.7	Ergonomic & Acoustic Standards: Compliance with ISO 9241 ergonomics standard and NC-40 or better acoustic rating for sustained shift work.	**D**		
5.8	Workstation Power Resiliency: Individual desktop UPS or dual power rail to workstations, not just rack-level UPS.	**D**		
5.9	Physical Asset Protection: Cable locks / chassis intrusion-detection switches reporting to asset management.	**D**		
6. VIDEO WALL SYSTEM (DISPLAY PANELS)				
6.1	The product should be a 24/7 with 55" inch in size	**M**		

Official Use Only

No.	Technical & Functional Specification Description	M/D	Compliance (Y/N)	Reference / Page
6.2	The display should support minimum 500cd/m2 brightness with 1100:1 contrast as minimum	M		
6.3	The display should support HDR signal	D		
6.4	The display should have mimimum haze level of 25%	D		
6.5	The display should spectra view engine technology	D		
	The display should have OPS expansion slot	D		
	The display should have builtin media player	D		
	The display should support effortless video wall set up with autosync	D		
	The display should support 4k UHD & daisy chain capability	D		
6.6	The display panel has to be IPS technology	D		
6.7	The product has to be with vertical scan inversion function	D		
7. VIDEO WALL SYSTEM (CONTROLLER & MANAGEMENT)				
7.1	**Technology Fully IP Based video wall Controller & Fully redundant with 0ms failover.** **Working on the LAN without any HDMI or video cabling**	D		
7.2	**Inputs** - Unlimited Expandability, Sender, Streamer, IP Stream.	D		
7.3	**Outputs -** Licensed Based – Unlimited Expandability, HD and UHD	D		
7.4	**Output Resolution:** Each Display at full Native resolution up to 4k/UHD with present version / player technology	M		

Official Use Only
Official Use Only

No.	Technical & Functional Specification Description	M/D	Compliance (Y/N)	Reference / Page
7.5	✓ **Content Type Combinations:** Supports movie formats that allow 4K video playback and high performance (60 FPS) 1080p playback. ✓ The IP Streams software, adds the capability to manage remote IP cameras and RTSP streams (H.264 and MJPEG) and stream them to the wall. ✓ The System can display Quicktime movies (.mov, .mp4) without conversion that were imported before version 4.0, assuming Quicktime is still installed. ✓ 30 or 60 frames per second preferred (30 FPS for 4K) ✓ Group size (1 frame interval) of ¼ second or less Bit rate of less than 100 Mbps (fixed or variable) ✓ Horizontal and vertical resolutions must be multiples of four ✓ AAC audio compression ✓ Container: .mp4, .mov, or .mkv preferred, though others may work. ✓ Videos in other formats, use one of the many open source video format conversion tools to transcode them to meet the above guidelines.	✓		
7.6	**Architecture :** Distributed Network (LAN Based) IGMP Layer 2, Version2	D		
7.7	**KVM :** KVM access to Sources from Control (Keyboard, Video, Mouse). Possibility to enable and restrict. Offering secure KVM windows to access the Software no third-party software needed for remote access.	D		
7.8	**Interface:** Enhancing Layout as well as UI and UI: A mini-map in the Controller viewer window, content targeting, easy content swap, SmartSnap anchor point snapping, real-time searchable contents list in control panel Control panel content tree expand/collapse HTML based API to manipulate dis/-appearance of single sources or a complete environment (layout of a wall) via 3rd party application	D		

Official Use Only
Official Use Only

No.	Technical & Functional Specification Description	M/D	Compliance (Y/N)	Reference / Page
7.9	**Redudancy:** Automatic failover.	M		
7.10	**Access Security:** User Authentication – Limit and Restrict access to Content. Offering login and access / restriction to defined functions (e.g. clear wall) as well as sources. Refining access to sources by enabling / restricting access to defined layouts (environment).	M		
7.11	**Logs:** Action logs of Users	M		
8. REMOTE MONITORING SUPERVISOR TABLETS				
8.1	Display & Compute Performance: 10–11" FHD, 6 GB RAM, 128 GB storage, >=8 hr battery (Best-in-Class: >=12", >=8/256 GB, >=12 hr, LTE/5G).	M		
8.2	Endpoint Security & Management: MDM enrolment; full-disk encryption; VPN; biometric/PIN lock (Best-in-Class: Per-app VPN, rugged rating IP65+, 3-yr warranty).	M		
8.3	Physical Durability Rating: IP65/IP67 ingress rating and MIL-STD-810G shock/drop tolerance for field use.	D		
8.4	Cellular & Wireless Redundancy: Dual-SIM or eSIM with automatic carrier failover; Wi-Fi 6/6E support.	D		
8.5	Hardware-Backed Authentication: Hardware-backed biometric (not software-only) plus FIDO2/hardware token support for SOC dashboard MFA.	D		
8.6	Power Management: Hot-swappable battery option for extended field shifts.	D		
8.7	Classified Data Certification: Common Criteria or FIPS 140-2 certification for devices handling classified SOC data.	D		
8.8	Automated Fleet Enrolment: Zero-touch enrolment (Android Enterprise/Apple DEP) for rapid fleet provisioning and remote wipe.	D		

Security Software And Technology Tools Functionality.

Official Use Only
Official Use Only

Tool 1: SIEM – Security Information & Event Manager,

- The below Checklist shall form part of the preliminary mandatory technical functionality compliance Checklist that Bidders must respond to in the given format for the functionality of the Items under this Procurement;

- Technical requirements shall be classified as Mandatory (M) or Desirable (D), as shown in the M/D column of the checklist below. Only failure to meet an explicitly designated Mandatory requirement shall result in technical disqualification. Desirable requirements shall be assessed through the applicable rated criteria in Section III, Evaluation and Qualification Criteria.
- Requirements shall be based on functional, security, interoperability, and performance outcomes. Equivalent technical approaches, including integrated and interoperable multi-vendor solutions, shall be accepted where they demonstrably meet the specified requirements.

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1. LOG INGESTION				
1	The solution should have scalable architecture and should be able to collect data at scale across all users, devices, applications, and infrastructure, both on-premises and in multiple cloud environments	M		
2	The solution should have the capability to export raw logs in various formats such as syslog, XML, CSV etc.	M		
3	A solution should have seamless integration and correlation of logs from multi cloud	D		
4	Solution should be scalable to cater the growing data source requirement	M		
5	The solution should keep the ingested data along with all the related system, infrastructure, diagnostics and support to address regulatory requirements and other compliance requirements such as SOC Type2, ISO27001	M		
6	The solution should be able to connect data/log sources for ingestion of logs, majorly through out-of-the-box connectors	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
7	The solution must support both agent and agentless log collection methods e.g. Syslog, Common Event Format (CEF), also support REST APIs	M		
8	The solution should have capability to ingest data in custom log formats	M		
9	Solution should have functional features such as data source health monitoring, view on specific service or data source issues via use cases.	M		
10	The solution must automate internal health checks and notify the user in case of problems via use cases.	M		
10.1	*The solution must have self-monitoring features to track health of all nodes, also monitor capacity requirements in terms of data consumption, performance, query limits and so on via use cases.*	*M*		
11	Provide out-of-the-box, service-to-service support for cloud related services	D		
12	Solution to provide options to export stored data for long term retention or archival	M		
13	The solution should allow the data to be retained in a low-cost archived state as per the retention policy	D		
14	The solution should be able to parse and correlate multi-line logs	M		
15	Solution should have capability to filter undesired, non-security logs at collection, processing and visualization layer	M		
16	The solution should Identify / remember frequently used queries/rules and provide means for optimization of queries/rules	D		
17	The solution should have the ability to perform free text search on events, incidents, rules and other parameters	M		
18	The solution should be sized to meet the data retention requirement. The minimum retention period for security event and log data shall be twelve (12) months. Data required for investigation, audit or legal hold shall be preserved for the period directed by the Purchaser or required by applicable law.	M		
19	The solution should be able to collect alerts/logs from a number of security products including but not limited to, Firewalls, PIM, DLP, IPS, WAF, Anti-APT, HIPS, AV, XDR (out of scope of this assignment), etc.	M		
20	The solution have in-built parser to parse the data.	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
21	Shall have a robust data ingestion pipeline architecture with health-monitoring capabilities	M		
22	Ability to build a highly robust resilient data/log ingestion pipeline	M		
23	Platform able to browse for content packs which are prebuilt integrations, playbooks, dashboards, fields, and data model rules used to support security automation and analysis.	D		
24	The solution should be capable of monitoring, alerting, and reporting features (e.g., security dashboard of violations, alerting to relevant stakeholders, detect and alert on any interruptions in log/event data).	M		
25	Data Collection	M		
26	*Ability to ingest logs from virtually any data source, including network, endpoint, cloud, identity, application, HR, and any other data source for threat hunting, correlation and detection.*	*M*		
27	*Built in threat hunting capabilities to detect threat before, during, and after a compromise*	*M*		
2. VISIBILITY AND DETECTION ANALYTICS				
1	Supervised and unsupervised machine learning capabilities	D		
2	Custom correlation rules that can retroactively detect attacks	M		
3	Granular alert exclusions for optional tuning of endpoint, network, cloud, or third-party alerts	M		
4	Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services	D		
5	Ability to consume threat intelligence feeds from third-party sources in JSON and CSV formats	M		
6	Detection of attack techniques across the attack lifecycle including discovery, lateral movement, command and control, and exfiltration	M		
7	Demonstrated ability to detect attacker tactics and techniques through MITRE ATT&CK Evaluations	D		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
8	Tagging of MITRE ATT&CK tactics and techniques in alerts, detection rules, and incidents	M		
9	The solution should have a centralized correlation engine and a management center/console which allows creation of an unlimited number of correlation rules/policies and parsers	M		
10	The solution should provide investigation capability to investigate incidents	M		
11	The solution should support logical operation and nested rules for creation of complex rules	M		
12	The solution should have the ability to correlate all the fields present in a log/flow data	M		
13	The solution should have rules/policies to detect any compromises by generating alerts collected together over a period of time	M		
14	Solution should provide out-of-the-box rules and built-in templates to help you create threat detection rules to notify suspicious events	M		
15	Solution should have capabilities to correlate alerts between different source & destination IPs to find similar or colluding threat events	M		
16	Should have capability to detect advanced multistage attacks mapped to Mitre Attack Framework	M		
17	Detect suspicious events and generate incidents/offenses on minimum basic use cases given below but limited to:	M		
17a	*Failed login attempts*	*M*		
17b	*Login attempts from suspicious locations*	*M*		
17c	*Authorization attempts outside of approved list*	*M*		
17d	*Vendor logins from unauthorized subnets*	*M*		
17e	*Vertical & Horizontal port scans*	*M*		
17f	*Traffic from blacklisted IPs*	*M*		
17g	*Login attempts at unusual timings*	*M*		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
18	Solution should provide use cases given below but not limited to the list:	M		
18a	*Failed login attempts*	*M*		
18b	*Credential harvesting*	*M*		
18c	*Credential Access*	*M*		
18d	*Unauthorised RDP connections*	*M*		
18e	*Unauthorised usage of PowerShell*	*M*		
18f	*Crypto mining*	*M*		
18g	*Data destruction*	*M*		
18h	*Resource abuse*	*M*		
18i	*Data Exfiltration (Mass file download, file share, mailbox exfiltration)*	*M*		
18j	*Denial of service*	*M*		
18k	*Lateral movement*	*M*		
18l	*Malware command and control*	*M*		
18m	*Ransomware executions*	*M*		
18n	*Resource hijacking*	*M*		
19	Detect emerging and unknown threats in your environment by applying extended ML analysis and by correlating a broader scope of anomalous signals, while keeping the alert fatigue low	D		
20	Solution should allow to add exceptions to analytic rules to reduce false positives	M		
21	Should provide entity insights based on following data sources:	M		
21a	*Syslog (Linux)*	*M*		
21b	*Security Events (Windows)*	*M*		
21c	*Audit & Sign-in logs (from AD and other cloud platforms)*	*M*		
21d	*Office Activity (Office 365)*	*D*		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
21e	*Behavior Analytics*	*M*		
21f	*Threat Intelligence Indicators*	*M*		
22	Sync user entities from Active Directory/LDAP to SIEM	M		
23	Built-in watchlist kind of templates for creating custom usecases such as to track:	D		
23a	*Privileged Users*	*D*		
23b	*Terminated Employees*	*D*		
23c	*Service Accounts/users*	*D*		
23d	*Identity Correlation*	*D*		
23e	*High Value/crown jewel assets*	*D*		
23f	*Network Mapping*	*D*		
24	The solution must align rules/use cases with MITRE attack framework	M		
3. INVESTIGATIONS				
1	Visualization of the chains of execution leading up to an alert	M		
2	Timeline analysis view to see all actions and alerts on a timeline	M		
3	A cloud investigation view with cloud-specific events and artifacts	D		
4	Querying for indicators of compromise (IOCs) and endpoint behaviors	M		
5	Querying for online and offline hosts	D		
6	Querying of log data from any source, including network, cloud, endpoint, identity & forensics data	M		
7	Advanced querying language with support for wildcards, regular expressions, JSON, data aggregating, field and value manipulation, merging of data from disparate sources, and visualization of data	M		
8	Ability for an analyst to easily pivot between views	M		
9	Granular filtering and sorting of query results	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
10	Automatic aggregation of relevant IP or hash information, including threat intelligence, events, and related incidents in a single view to simplify investigations	M		
11	Identification of whether an event was blocked by an endpoint agent, firewall, or another prevention technology	D		
12	Automated stitching of endpoint, network, cloud and identity data, including security alerts & events	D		
4. INCIDENT MANAGEMENT				
1	Automated grouping of related alerts from various sources into a single incident	M		
2	Intuitive incident view with an incident overview and MITRE tactics and key incident information.	M		
3	Customizable incident scoring	M		
4	Listing of notable artifacts from alerts and their threat intelligence information	M		
5	Listing of user and hosts involved in incidents to quickly determine the scope of an incident	M		
6	Ability to assign incidents to team members	M		
7	Automated notifications on incident assignment	M		
8	Ability to add comments to incidents	M		
9	End-to-end management of the incident lifecycle (new, investigation, closed, handled, etc.)	M		
10	Optional merging of incidents	D		
11	Ability to send incident data to third-party case management	D		
5. DATA COLLECTION, DATA INTEGRATION, AND FORENSICS				
1	Data Collection	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
2	*Ability to ingest logs from virtually any data source, including network, endpoint, cloud, identity, application, HR, and any other data source for threat hunting, correlation and detection.*	***M***		
3	*User information for analytics*	***M***		
4	*Domain and distinguished name*	***D***		
5	*Email address*	***D***		
6	*Organizational unit*	***D***		
7	*Phone number*	***D***		
8	*Logged-in user*	***D***		
9	*Typical user of a machine*	***D***		
10	*User creating the process that initiated communication*	***D***		
11	*User group and organizational unit from directory services*	***D***		
12	*User data from a variety of sources including network traffic logs, Windows event logs, Okta logs, PingOne and PingFederate logs, and Azure Active Directory logs*	***D***		
13	*System events for analytics*	***M***		
14	*User status change event, such as login and logout*	***M***		
15	*Host status change event*	***M***		
16	*Agent status change event*	***M***		
17	*Security alerts for analytics*	***M***		
18	*URL filtering logs*	***M***		
19	*Firewall threat logs*	***M***		
20	*Endpoint threat logs*	***M***		
6. DEPLOYMENT, MANAGEMENT, REPORTING AND SECURITY				
1	Scalable, cloud-based management and agent deployment	**D**		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
2	Role-based access control (RBAC) for granular permissions	M		
3	Multi-factor authentication (MFA) for management	M		
4	Customizable dashboard for high-level status of security and operational information	M		
5	Standards-based APIs to allow third-party management tools to integrate and perform administrative actions	M		
6	Best practices to ensure the entire solution and its infrastructure are secure, including hardening, encryption for data at rest and data in motion, network security, physical security, and regular assessment tests	M		
7	Provides default reports and dashboards.	M		
8	Reports can be built with predefined widgets or with custom widgets	D		
9	Dashboards offer dynamic filters and drill downs to allow users to easily pivot between data points	D		
10	Reports can be scheduled and saved with raw data attached as a CSV	D		
7. DATA RETENTION, COVERAGE, SLA, SECURITY AND PRIVACY REQUIREMENTS				
1	Visibility into lateral movement across the network and other parts of the infrastructure	M		
2	Continuous collection and centralized storage of all security data for behavioral analytics	M		
3	Data retention of 12 months included standard	M		
4	Optional retention of data for an unlimited length of time	D		
5	Data required for investigation, audit or legal hold shall be preserved for the period directed by the Purchaser or required by applicable law	M		
8. ADDITIONAL REQUIREMENTS				
1	The solution must provide AI-driven automated alert grouping that uses machine learning to intelligently cluster related alerts into unified incidents across all data sources (endpoint, network, cloud, identity) — not limited to rule-based correlation alone.	D		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
2	The proposed solution shall enable effective interoperability between SIEM, SOAR, endpoint security, and other relevant cybersecurity technologies through native capabilities or secure, documented interfaces/APIs. The solution shall support cross-platform event correlation, information exchange, synchronized incident management, automated and approval-based response workflows, and auditable actions. Integrated and multi-vendor architectures shall be equally acceptable where the required functionality, security, and performance outcomes are demonstrated.	M		

Tool 2: SOAR – Security Orchestration,Automation And Response,

- The below Checklist shall form part of the preliminary mandatory technical functionality compliance Checklist that Bidders must respond to in the given format for the functionality of the Items under this Procurement;

- Technical requirements shall be classified as Mandatory (M) or Desirable (D), as shown in the M/D column of the checklist below. Only failure to meet an explicitly designated Mandatory requirement shall result in technical disqualification. Desirable requirements shall be assessed through the applicable rated criteria in Section III, Evaluation and Qualification Criteria.
- Requirements shall be based on functional, security, interoperability, and performance outcomes. Equivalent technical approaches, including integrated and interoperable multi-vendor solutions, shall be accepted where they demonstrably meet the specified requirements.

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1. AUTOMATION (AT)				
1	The solution should be capable of automation features.	M		
2	The solution should have scripting language available for automation.	M		
3	The solution should provide automation for the following:	M		
3a	*Forensic tools*	*D*		
3b	*IT (e.g., AD, SAML...)*	*M*		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3c	*Communication tools (e.g., email, Slack, Hipchat)*	*D*		
3d	*SIEM tools*	*M*		
3e	*Endpoint Security*	*M*		
3f	*Network Security*	*M*		
3g	*Active Directory*	*M*		
4	The solution should be capable of editing existing automation capabilities.	M		
5	Pre-defined scripts to allow analysts of all experience levels to easily collect data and investigate and respond to threats	M		
6	Status window that displays script results, confirming whether scripts executed successfully	D		
7	Integration with firewalls to block access to malicious IP addresses or domains	M		
8	SOAR capability for incident analysis, orchestration and automated response, provided natively by the proposed platform or through secure, documented integration with the proposed SIEM and other GovSOC tools	M		
9	Automation playbook development capabilities within the proposed SOAR solution	D		
10	Resolve incidents or automate parts of the incident investigation and resolution workflow	M		
11	Solution should have the ability to automatically remediate exposures. This should include full resolution of the incident by reaching back via API and blocking the service at the port level.	D		
12	Allow customizability to the remediation path	M		
13	Integration with firewalls to block access to malicious IP addresses or domains	M		
2. PLAYBOOK (PL)				
1	The solution should be capable of using playbooks.	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
2	The solution should have built-in playbooks.	M		
3	The solution should be capable of adding custom playbooks.	M		
4	The solution should be capable of having parts of an existing playbook be included in a new playbook.	D		
5	The solution should define how playbooks are represented (e.g., workflow, task list, other).	D		
6	The solution should be capable of defining what task/building block types can be included (e.g. manual tasks, automated tasks, conditional tasks, etc.).	M		
7	The solution should be capable of defining a single playbook that contains both procedural and automated tasks.	M		
8	The solution should be capable of playbooks that can be run automatically.	M		
9	The solution should be capable of playbooks that can be run manually.	M		
10	The solution should be able to define how the execution of a playbook is documented.	M		
11	The solution should be capable of playbook execution that can be seen step by step for debugging.	D		
12	The solution should be capable of playbook execution that can be started from where it had stopped on error.	D		
13	The solution should be capable of playbooks that can map current and future CIRT processes and procedures to incident types.	M		
14	The solution should be capable of tasks that can be assigned to different team members inside a playbook execution and track all the actions in the investigation flow.	M		
15	The solution should be capable of playbooks that can pass parameters processed by upstream tasks to tasks further down the workflow within a playbook.	M		
16	The solution should be capable of playbooks that can parse the output from a sub-playbook and utilize it in subsequent playbook tasks.	D		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
17	The solution should be capable of describing the process of adding an ad-hoc task to a playbook.	D		
18	The solution should be capable of tasks that can be scheduled to run periodically.	M		
19	The solution should support undo/redo on the playbook canvas, keyboard shortcuts.	D		
20	The solution should be capable of playbooks that can call other playbooks as tasks.	M		
21	The solution should be capable of seeing historical run of playbooks or tasks (view via audit log).	M		
22	The solution should be capable of playbooks that can be scheduled as jobs.	D		
23	The solution should be capable of playbooks that can continue based on an email response to an end user.	D		
3. REST API				
1	The solution should have an authenticated API capable of executing the same functions as are available via the GUI.	M		
4. INCIDENT MANAGEMENT (IN)				
1	The solution should be capable of integrating with IT ticketing systems.	M		
2	The solution should be capable of providing ticketing functionality for the security team/IR team.	M		
3	The solution should be capable of assigning an incident to a user or team.	M		
4	The solution should be capable of a way to know which incidents are neglected, and of specifying an SLA for an incident.	M		
5	The solution should be capable of describing what happens when an incident is closed, and should have a platform to standardize/scale SLA management.	M		
6	The solution should be capable of showing how notifications are sent to other team members and of a way to know which incidents are neglected.	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
7	The solution should be capable of giving notifications to the user.	M		
8	The solution should be capable of setting reminders for tasks.	D		
9	The solution should be capable of showing how incidents are generated in the product.	M		
10	The solution should be capable of showing a way to map incident parameters from other products.	M		
11	The solution should be capable of levels of customizability that are available for incident management.	D		
12	The solution should offer auto-casing / auto-population based on the incident type or other relevant incident attributes.	D		
5. DOCUMENTATION				
1	The solution should be capable of showcasing how incidents are documented.	M		
2	The solution should be capable of identifying what parts of the incident can be documented.	M		
3	The solution should be capable of timestamping incident entries.	M		
4	The solution should be capable of user activity documentation (e.g., messages, running analysis on artifacts, notes, adding artifacts, etc.).	M		
5	The solution should be capable of showcasing how IOCs are documented.	M		
6	The solution should be capable of identifying IOCs that can be associated with a kill chain stage.	D		
6. COLLABORATION				
1	The solution should be capable of providing means of collaboration between users.	M		
2	The solution should be capable of other means of real-time collaboration or investigation.	D		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3	The solution should be capable of providing a way to collect data for an incident by collaborating with its users.	M		
7. INDICATOR REPOSITORY (IR)				
1	The solution should have an indicator repository.	M		
2	The solution should be capable of correlation of indicators to incident data.	M		
3	The solution should include an automated threat hunting playbook.	D		
4	The solution should be capable of importing STIX files.	M		
5	The solution should be capable of customizing the indicator structure.	D		
6	The solution should be capable of indicator whitelist management.	M		
7	The solution should be capable of exporting indicators to a STIX formatted file.	M		
8. ARCHITECTURE				
1	The solution should be capable of traversing a proxy.	D		
2	The solution should have search capabilities.	M		
3	The solution should have architecture features that support content management.	D		
4	The solution should be an internally hosted or externally hosted service, or hybrid.	M		
5	The solution should have an architecture feature that can help the user in terms of scalability and recovery.	M		
9. INTEGRATION WITH 3RD PARTY PRODUCTS				
1	The solution should support the ability to upload custom integrations via the console.	M		
2	The solution should support the ability to develop custom integrations via the console.	D		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3	The solution should support connecting to multiple instances of a given integration.	D		
10. DASHBOARDS / REPORTS				
1	The solution should have predefined reports.	M		
2	The solution should be capable of creating custom reports in the product.	M		
3	The solution should have a manager dashboard.	M		
4	The solution should have a widget library for dashboards and reports.	D		
5	The solution should have dashboards and reports that can be shared.	D		
6	The solution should be capable of showcasing how new playbooks, integrations and automations are updated.	D		
7	The solution should have list management ability (i.e., blacklisted IPs) and the ability to use these in playbooks.	M		
11. CONTENT				
1	The solution should have content (integrations, playbooks, reports, automations) that can be uploaded for offline environments.	D		
2	The solution should have content (new product integrations, playbooks, automation scripts, reports) that can be updated without updating the product.	D		
3	The solution should have content that can be granularly uploaded and downloaded.	D		
4	The solution should come with out-of-box reusable playbooks for well-known incident types (Phishing, Malware, IOC Hunt).	M		
12. USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)				
1	Behavioral analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, and user events over time	D		
2	Identity analytics to detect user-based threats such as lateral movement	D		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3	Predefined and customizable behavior-based detection rules	D		
4	The solution should be able to perform different correlations (but not limited to): rule based, historical based, heuristics based, behavioural based, etc., across different devices and applications	D		
5	UEBA feature should help build baseline behavioural profiles of organization's entities (such as users, hosts, IP addresses, and applications) across time and peer group horizon	D		
6	A 360-degree user view with user risk scores	D		
7	Behavioral analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, and user events over time	D		

TOOL 3 : Threat Intelligence Platform (TIP)

- The below Checklist shall form part of the preliminary mandatory technical functionality compliance Checklist that Bidders must respond to in the given format for the functionality of the Items under this Procurement;
- Technical requirements shall be classified as Mandatory (M) or Desirable (D), as shown in the M/D column of the checklist below. Only failure to meet an explicitly designated Mandatory requirement shall result in technical disqualification. Desirable requirements shall be assessed through the applicable rated criteria in Section III, Evaluation and Qualification Criteria.
- Requirements shall be based on functional, security, interoperability, and performance outcomes. Equivalent technical approaches, including integrated and interoperable multi-vendor solutions, shall be accepted where they demonstrably meet the specified requirements.

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1. THREAT INTELLIGENCE INGESTION & FEEDS				

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1	Out-of-the-box or secure API-based integration with one or more threat intelligence services for threat intelligence tags and additional context on key artifacts	M		
2	Ingestion of threat intelligence feeds from third-party sources in JSON and CSV formats	M		
3	Solution should be able to import threat intelligence by enabling data connectors to various threat intelligence platforms and feeds	M		
4	STIX 2.1 / TAXII 2.1 support (native or through secure, documented interfaces) for feed ingestion and interoperability with industry-standard threat-sharing protocols	M		
5	Support for ingesting intelligence from open-source (OSINT), commercial, government (e.g., CERT/CISA), and ISAC/ISAO sharing communities	M		
6	De-duplication and normalization of indicators ingested from multiple overlapping feeds into a single unified record	M		
7	Configurable feed source reliability/confidence scoring (e.g., Admiralty Code) to weight indicators by source trustworthiness	D		
8	Ability to prioritize or suppress specific feed sources based on historical accuracy and false-positive rate	D		
2. IOC / INDICATOR LIFECYCLE MANAGEMENT				
1	Ability to automatically scan historic data for IOCs as they are added to the system and raise alerts via SIEM	M		
2	IOC creation using APIs	M		
3	IOC creation from the management console	M		
4	Ability to import multiple IOCs using APIs	M		
5	Ability to import multiple IOCs from a CSV file using the management console	M		
6	Configurable severity level of an IOC	M		
7	View and manage the imported threat intelligence along with features to create new indicators	M		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
8	Add indicators in bulk to SIEM threat intelligence from a CSV or JSON file and support other formats such as STIX/TAXII, XML, txt, pdf, doc, email etc.	M		
9	The solution should be capable of customizing the indicator structure.	M		
10	Automated IOC expiration/aging policies to retire stale indicators and reduce alert fatigue	M		
11	Deduplication and merging of duplicate indicators submitted from multiple sources	M		
12	Whitelisting / false-positive suppression workflow with audit trail of analyst overrides	M		
13	Bulk tagging and categorization of indicators by threat type, campaign, or actor	D		
14	Version history / change tracking for each indicator (who added or modified it, when, and why)	D		
15	Support for indicator types beyond IP/domain/hash — including URLs, email addresses, file paths, registry keys, and YARA/Snort/Sigma rules	M		
3. ENRICHMENT & CONTEXTUALIZATION				
1	Threat Intelligence provided must be relevant, context-rich, timely and accurate	M		
2	Curation, normalization, enrichment, and risk scoring of data	M		
3	The solution should be able to enrich all imported threat intelligence indicators with Geolocation and WhoIs data via enrichment sources	M		
4	Automatic MITRE ATT&CK technique/tactic tagging for each indicator or threat actor	M		
5	Passive DNS and certificate history enrichment	D		
6	Malware family/classification enrichment (e.g., via sandbox detonation results)	D		
7	Confidence and severity scoring recalculated dynamically as new corroborating intelligence arrives	D		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
4. THREAT MODELING, ANALYSIS & VISUALIZATION				
1	The solution should be capable of providing a graphical representation of threat or incident data and its relationship with other data.	M		
2	Solution should have a knowledge base on methods used by attackers in various past breaches globally to create models to detect such attacks	D		
3	Threat actor and campaign profiling with links to associated TTPs, tools, and historical incidents	D		
4	Kill chain / Diamond Model mapping of intelligence to attack stages	D		
5	Link analysis / relationship graphing between indicators, actors, campaigns, and internal assets	M		
6	Vulnerability intelligence correlation — mapping CVEs to active exploitation intelligence for patch prioritization	D		
5. INTEGRATION & AUTOMATED RESPONSE (SIEM / SOAR / XDR)				
1	Shared threat intelligence to distribute crowdsourced threat intelligence from cloud-based malware analysis service to firewalls, endpoint agents, and detection and response services	D		
2	Threat Intelligence should provide data feeds and APIs for automated consumption by the SIEM tool	M		
3	Threat intelligence feeds should enable efficient security operations and reduce the time for investigation for security operations	M		
4	SOAR integration (native or through secure, documented APIs) to trigger automated containment playbooks (block, isolate, quarantine) upon high-confidence IOC match	M		
5	Bi-directional integration allowing SOC analyst feedback (true/false positive) to flow back and retrain feed prioritization	D		
6	Support for automated blocklist push to firewalls, proxies, EDR, and email security gateways	M		
7	Rate-limited, authenticated REST API for programmatic indicator query, submission, and bulk export	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
6. DASHBOARD, REPORTING & PORTAL				
1	Threat Intelligence should deliver a comprehensive range of timely adversary and technical threat intelligence through a customizable portal or dashboard	M		
2	The Threat Intelligence Portal/Dashboard should provide an end-to-end picture of threats via integration with SIEM/XDR	M		
3	Executive-level threat landscape reporting (industry-specific threat trends, sector targeting)	D		
4	Scheduled and on-demand reporting with export to PDF/CSV/STIX	M		
5	Role-based dashboard views tailored to SOC analyst, threat hunter, and CISO/executive audiences	D		
7. GOVERNANCE, SHARING, COMPLIANCE & SCALABILITY				
1	Support for Traffic Light Protocol (TLP) classification and enforcement on shared intelligence	M		
2	Role-based access control (RBAC) and multi-tenancy for MSSP / multi-business-unit deployments	D		
3	Full audit logging of all indicator additions, edits, deletions, and sharing actions	M		
4	Data retention policy configuration aligned with regulatory/compliance requirements	M		
5	High-availability, scalable architecture (cloud, on-premises, or hybrid) with a defined SLA for feed processing latency	M		
6	Compliance with data privacy requirements when handling PII embedded in threat intelligence (e.g., email addresses, usernames)	M		

TOOL 4: Anti-Distributed Denial Of Service (ANTI-DDOS)

Official Use Only

- The below Checklist shall form part of the preliminary mandatory technical functionality compliance Checklist that Bidders must respond to in the given format for the functionality of the Items under this Procurement;
- Technical requirements shall be classified as Mandatory (M) or Desirable (D). Only failure to meet an explicitly designated Mandatory requirement shall result in technical disqualification. Desirable requirements shall be assessed through the applicable technical scoring criteria.
-
- Requirements shall be based on functional, security, interoperability, and performance outcomes. Equivalent technical approaches, including integrated and interoperable multi-vendor solutions, shall be accepted where they demonstrably meet the specified requirements.
- The technical requirements specified herein are intended to define the minimum functional, operational, security, interoperability, and performance requirements of the proposed solution. References to specific technologies, architectures, deployment models, network designs, or operational approaches shall not be interpreted as restrictive to any particular vendor, manufacturer, or proprietary implementation, provided the proposed solution demonstrably meets or exceeds the stated functional and performance objectives of the Procuring Entity.

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1. DDOS PROVIDER INFRASTRUCTURE & ARCHITECTURE				
1.1	The provider of the solution should be hybrid. It must have on-premises devices that work in tandem with cloud DDOS mitigation services to protect the ICTA infrastructure during an attack.	**M**		
1.2	The proposed solution shall demonstrate resilient, scalable, and geographically distributed DDoS mitigation architecture capable of ensuring high availability, traffic redundancy, and low-latency mitigation services across multiple regions.	**M**		
1.3	The proposed solution shall demonstrate the capability to detect and mitigate volumetric and protocol-based DDoS attacks affecting protected	**M**		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
	services within a maximum mitigation initiation time while maintaining acceptable service latency for users accessing services from Kenya and the East African region. The solution shall detect a DDoS event within five (5) minutes of the event meeting the defined detection threshold and shall initiate mitigation within ten (10) minutes of detection or the agreed activation trigger. The Supplier shall record and report the timestamps used to measure compliance.			
1.4	The provider shall demonstrate secure, resilient, and high-capacity traffic routing architecture capable of supporting effective DDoS mitigation without introducing material service degradation or single points of failure.	**M**		
1.5	The provider should demonstrate optimized regional traffic routing and peering arrangements (e.g., direct IXP or Local POP) sufficient to minimize latency for locally originating traffic.	**D**		
1.6	The provider shall demonstrate compliance with internationally recognized security and data protection standards such as ISO/IEC 27001, SOC 2 Type II, GDPR, PCI-DSS, FedRAMP, or equivalent certifications.	**M**		
1.7	The proposed DDoS solution MUST be based on a modular, DEDICATED High Performance OEM Hardware Appliances Platform Each Hardware appliance MUST be: • Capable of supporting Mitigation (inspected) Throughput of up to 50 Gbps • Installed with a minimum 6x100 GigE 6 x40 GigE Fiber ports (with or without bypass) and minimum 12x 10GigE Ports (with bypass) and 24 x10 GigE Fiber Ports (without bypass). • Capable of Supporting SSL/TLS Traffic inspection on hardware. • Installed with a minimum of 1 10/100/1000 BaseT Copper and 1 RJ-45 serial console ports for management.	**D**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
	• Internal Hardware bypass capable NB: In this regard, bidders are advised to note that proposals based on outdated appliances, integrated hardware appliances such as Routers, Unified Threat Management Technologies (UTM), Application Delivery Controller, Intrusion Prevention System (IPS), Load Balancers, Proxy based architecture, Stateful Device, virtual servers, cloud environment etc. will be considered non responsive.			
1.8	Solution MUST support Legitimate/Clean Traffic of at least 10 Gbps from the date of commissioning, scalable up to 40 Gbps on same hardware appliances on a need basis.	M		
1.9	Successful bidder should implement, configure, Customize and undertake continuous optimization of the DDoS Protection Solution to deliver the following security services and features: i. SSL/TLS Traffic inspection for SSL traffic with both TLS 1.2 and 1.3 support. It should be hardware-based. ii. Support a minimum 100k SSL/TLS connections per second from the date of commissioning. iii. Ability to mitigate encrypted attacks without the need to decrypt the traffic.	M		
1.10	The solution should protect against complex DNS attacks: i. Water torture attacks ii. Dictionary attacks iii. Authenticated dictionary attacks	M		
1.11	Successful bidder should implement, configure, Customize and undertake continuous optimization of the DDoS Protection Solution to deliver the following security services and features at minimum: i. Protection against HTTP Flood attacks.	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
	ii. Protection against Web DDOS attacks iii. Protection against UDP Floods iv. Protection against burst attacks v. Protection against NTP attacks vi. Protection against Slowloris attacks			
1.12	The solution should support automatic behavioral-based detection algorithms to identify attacks more accurately and with fewer false positives than traditional rate-based systems. Mitigation should be done using real time signatures.	M		
1.14	Presence of a local POP in Kenya for mitigation to reduce MTTR. The OEM must also provide proof of ownership of the local POP: i. Name and location of the data centre, ii. IPs and ASNs for the provider, iii. BGP looking glass links that show routing from the region, iv. Connection to KIXP, v. traceroute samples for the IP prefixes, vi. Collocation agreement or letter of authorization, operational start date of the POP.	D		
1.15	The platforms utilize FPGA hardware acceleration modules.	D		
2. DDOS PROTECTION FEATURES & ATTACK MITIGATION				
2.1	The DDoS protection service may use always-on cloud scrubbing or on-demand cloud scrubbing with traffic diversion, including BGP and/or GRE redirection where appropriate. For on-demand mitigation, the Supplier shall initiate mitigation within the maximum time stated in the operational SLA following detection and activation of the mitigation procedure. The solution shall support the specified hybrid on-premises and cloud architecture The	M		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
	solution shall support the specified hybrid on-premises and cloud architecture			
2.2	The solution shall support mitigation of high-volume and sustained DDoS attacks without material degradation of protected services, and bidders shall clearly disclose any applicable service limitations or thresholds.	**M**		
2.3	The solution shall provide automated real-time detection and mitigation of network-layer attacks within industry-recognized response time thresholds using AI/ML behavioral profiling and threat baselining.	**M**		
2.4	The solution must mitigate various network-based DDoS attacks including, but not limited to: • SYN, ACK, RST, FIN, and SYN-ACK reflection flood attacks • Teardrop, Ping of Death, and L3/L4 payload/fragmentation attacks • DNS Flood attacks and DNS NXDOMAIN / Water Torture attacks • IPsec and VPN protocol-related flood attacks • Multi-Protocol floods (SNMP, ICMP, UDP, TCP, QUIC, GRE) • Various amplification attacks (NTP, SSDP, Memcached, LDAP, CHARGEN) • Reflection attacks and Carpet Bombing attacks (sub-rate distributed floods) • Smurf and Fraggle reflection attacks • Mirai and Mirai-variant L3/4 botnet attacks • Protocol violation, malformed header, and invalid checksum attacks • Voice-related DDoS attacks (e.g., SIP REGISTER/INVITE floods)	**M**		
2.5	The solution shall support secure traffic redirection and return-path mechanisms (BGP Anycast, GRE Tunnels, L2TP, DNS) suitable for deployment within hybrid or cloud-based mitigation architectures.	**M**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
2.6	The solution shall support automated traffic rerouting, route health monitoring, failover, and protection of multiple public network segments.	**M**		
2.7	The provider should support Connection exhaustion defenses using dynamic rate shaping, per-IP reputation scoring, TCP SYN cookies, and adaptive challenge mechanisms.	**D**		
2.8	The proposed solution shall provide geographically distributed mitigation capacity designed to avoid single points of failure.	**M**		
2.9	The provider must provide per-attack packet-level visibility with deep protocol breakdown and PCAP download capabilities.	**M**		
2.10	The provider solution must distinguish between legitimate surge traffic (e.g., viral campaigns, public announcements) and malicious L7 floods using dynamic behavioral baselining.	**M**		
2.11	The solution shall support configurable detection sensitivity and response thresholds per zone or service.	**M**		
2.12	The solution provider must be able to detect and mitigate slow POST attacks, HTTP Slowloris, Slow Read, HTTP/2 Rapid Reset, and credential stuffing amplification.	**M**		
2.13	The solution should support multiple detection methodologies including behavioral analysis, anomaly detection, signature-based detection, and advanced automated threat analysis techniques.	**M**		
2.14	The solution should support the following multi-DDoS protection features: i. Automatic creation of real time threat signatures in response to change of attack vectors during an attack ii. Use behavioral analysis to differentiate between normal and malicious traffic.	**M**		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
	iii. AI-based fine-tuning of the threat signatures.			
2.15	The solution should support an AI-enabled SOC analysis module running on the device for attack analysis and automatic mitigation recommendations	**D**		
2.16	The solution should support Integration with industry standards IP, ASN and TLS fingerprinting reputation feeds to block traffic from known malicious sources	**D**		
3. APPLICATION SECURITY PROTECTION FOR HOSTED DOMAINS & WEBSITES				
3.1	The solution shall support configurable mitigation and traffic handling policies including: ALLOW, BLOCK, CHALLENGE (JS/CAPTCHA), RATE LIMIT, REDIRECT, ALLOW, SUSPEND, REPORT AND BLOCK, and ADAPTIVE MITIGATION.	**M**		
3.2	The provider should stop abuse, DDoS, and brute-force attempts targeting applications and APIs by rate limiting individual IPs or by header attribute (e.g., key, cookie, token), ASN, or country with seamless integration with WAF.	**M**		
3.3	The provider should include threat intelligence feeds to allow creation of policies to block connections from IPs of known open SOCKS/HTTP proxies, anonymous VPNs, TOR exit nodes, botnets, command and control servers, malware sources, and anonymizers.	**M**		
3.4	The provider should also provide dedicated protection against DNS-based DDoS attacks like DNS amplification and DNS water torture (random subdomain) attacks. The solution must also support the creation of a domain scoped allow list	**M**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3.5	The provider should support distributed caching and traffic acceleration capabilities (CDN/Edge optimization) to improve resilience, optimize TLS handshakes, and absorb volumetric attacks targeting hosted services.	**D**		
3.6	The platform must provide API Security capabilities, including OpenAPI/Swagger schema validation, automated API discovery, and endpoint-level rate limiting.	**D**		
3.7	System must provide Protection against HTTP/S connection flood including C/R mechanism based on 302 redirect and JAVA script	**M**		
3.8	System must provide protection against Burst attacks	**M**		
3.9	System must provide Behavioral protection against HTTPS attacks without traffic decryption (including HTTPS connection flood, page flood and i.e. flood inside the TLS/SSL connection). It shouldn't be a rate limit methodology.	**M**		
3.10	System must provide protection against HTTPS attacks when running in OOP mode (including HTTPS connection flood, page flood and i.e. flood inside the TLS/SSL connection), with and without decryption	**M**		
3.11	System should provide automatic ability of the selective full SSL decryption only suspicious sessions under attack.	**D**		
3.12	System should provide the ability of the full SSL decryption towards a protected server	**D**		
3.13	System should support SSL protection without SSL keys (certificates)	**D**		
3.14	System should support GEO blocking and rate limit functionality	**M**		
3.15	System should support QUIC protection protocol	**D**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3.16	System should provide for Intrusion Prevention system module	**D**		
3.17	System should provide possibility to create own customer defined signatures (at least 100 signatures) under IPS	**D**		
3.18	The device itself should have a latency below 60 microseconds and must detect and protect in less than 18 seconds	**D**		
	The solution must provide a fully automated attack lifecycle management with no human intervention required	**D**		
4. MANAGEMENT, MULTI-TENANCY & REPORTING				
4.1	Provider must have full single-pane-of-glass management across all features which includes DDoS Protection, Application Security Protection, Certificate Management, DNS Management, Monitoring and Reporting, Security Analysis, User and Tenant Management.	**M**		
4.2	The platform must provide real-time and historical attack telemetry including: attack vectors, peak bits/packets/requests per second, top source IPs, ASNs, and countries, geographic distribution, attack duration, and mitigation actions taken; reports must be accessible via dashboard and API.	**M**		
4.3	The provider should have dashboard to configure Role-Based Access Control (RBAC) with configurable roles: Super Administrator, Security Administrator, Read-Only Analyst.	**M**		
4.4	The provider should have Multi-account management with separate tenant isolation. This is critical as ICTA is hosting and managing zones and assets of multiple government entities.	**M**		
4.5	The solution provider should have a detailed security analysis feature allowing ICTA view and prioritize alerts and incidents based on attack type,	**M**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
	location, designation asset etc. The platform should retain historical analytics for a minimum of 90 days.			
4.6	The solution provider must support log integration with multiple logs management and SIEM solutions via streaming logs to Splunk, Microsoft Sentinel, IBM QRadar, Elastic, etc., via open interfaces.	**M**		
4.7	The platform should also include full RESTful API (v4 or later) for all platform management functions with documented OpenAPI/Swagger specification.	**M**		
4.8	The proposed platform shall support compliance with internationally recognized security standards and frameworks such as PCI-DSS, ISO/IEC 27001, FedRAMP, or equivalent.	**D**		
4.9	Tool must offer contractually committed 99.99% Uptime SLA for platform availability and mitigation uptime.	**M**		
5. IMPLEMENTATION, LICENSING & SUPPORT				
5.1	The provider should include OEM Professional services for the installation and configuration of the proposed solution along with Bidder's onsite skill services. The OEM should take lead in the designing and validation of solution implementation as per OEM best practices.	**M**		
5.2	The Bidder should provide licenses for a period of 5 years (fully prepaid/subscription covering all core modules).	**M**		
5.3	The bidder should provide training for at least 5 ICTA staff on the proposed solution. The training should be classroom based with Labs delivered physically or virtually.	**M**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
5.4	Bidder must include OEM support for 24/7/365 Emergency Phone, Email, and Chat support delivered from an in-house team of experts with guaranteed emergency response SLAs.	M		

PHASE II: ADVANCED VISIBILITY AND MATURITY ENHANCEMENT

TOOL 5 – FILE INTEGRITY MONITORING (FIM)

MANDATORY PASS EVALUATION FOR FIM

- The below Checklist shall form part of the preliminary mandatory technical functionality compliance Checklist that Bidders must respond to in the given format for the functionality of the Items under this Procurement;
- Technical requirements shall be classified as Mandatory (M) or Desirable (D). Only failure to meet an explicitly designated Mandatory requirement shall result in technical disqualification. Desirable requirements shall be assessed through the applicable technical scoring criteria.
-
- Requirements shall be based on functional, security, interoperability, and performance outcomes. Equivalent technical approaches, including integrated and interoperable multi-vendor solutions, shall be accepted where they demonstrably meet the specified requirements.

-

- The below Checklist shall form part of the preliminary mandatory technical functionality compliance Checklist that Bidders must respond to in the given format for the functionality of the Items under this Procurement;

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1. INTEGRITY VERIFICATION & REAL-TIME DETECTION				
1.1	Can automatically check and monitor real-time changes to file and directory contents, checksums, and attributes.	**M**		
1.2	Can automatically check for changes to file/directory access permissions, ownership, and read/write flags.	**M**		
1.3	Can automatically check for changes to file/directory creation, modification, and access time/date stamps.	**M**		
1.4	Can automatically check for changes to file/directory names, moves, renames, and structural tree relocations.	**M**		
1.5	Can automatically check for additions, modifications, and deletions to Windows registry keys, values, and security descriptors.	**M**		
1.6	Supports multiple cryptographic hashing algorithms including SHA-256, SHA-512, SHA-3, and legacy MD5/SHA-1 for file validation.	**M**		
1.7	Can automatically detect granular changes to Access Control Lists (ACLs), SACLs, and DACLs on monitored assets.	**M**		
1.8	Ability to detect integrity changes across host server file systems (Windows NTFS/ReFS, Linux ext4/XFS, UNIX UFS/ZFS).	**M**		
1.9	Ability to monitor directory services file systems and database repositories (Active Directory NTDS.dit, LDAP directories, eDirectory).	**D**		
1.10	Ability to detect changes to hypervisor configurations and core file systems (VMware ESXi, Hyper-V, KVM, Nutanix AHV).	**D**		
1.11	Ability to detect changes to enterprise application file systems, web servers (IIS, Apache, Nginx), and container runtimes (Docker, K8s).	**M**		
1.12	Ability to detect changes as frequently as required – both via continuous real-time kernel-level drivers and scheduled scan-based approaches.	**M**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1.13	Enrichment & Risk Analytics: Specifies the relative risk significance of a change according to threat intelligence, asset criticality, and baseline context.	**D**		
1.14	Identifies systems whose configurations drift from designated hardening baselines or miss critical mandatory security settings.	**M**		
2. RULES-BASED CHANGE DETECTION & POLICY ENGINE				
2.1	Targeted monitoring: Can detect 'all changes' on a system node or selectively monitor designated critical application/system paths.	**M**		
2.2	Rule Tuning: Rules can be tuned with smart noise-reduction filters to automatically suppress non-impactful or routine log noise.	**M**		
2.3	Custom Rule Creation: Supports full customization of rule logic to monitor proprietary applications and custom file structures.	**M**		
2.4	Out-of-Box Rule Sets: Provides comprehensive, pre-packaged detection rule sets covering major OSs, databases, and network platforms.	**M**		
2.5	Wizard UI: Rules can be created or adjusted via a visual browser/wizard-based UI without needing manual regex coding.	**M**		
2.6	Risk Severity Categorization: Assigns dynamic severity levels (Critical, High, Medium, Low) to distinguish risk tiers for detected changes.	**M**		
2.7	Automated Reconciliation (SOAR): Supports automated methods of tagging changes as 'Accepted' or 'Requires Investigation' via SOAR playbooks.	**D**		
2.8	Authorized Change Reconciliation (ITSM): Differentiates authorized vs. unauthorized changes by correlating change windows, ticket IDs, and user identities via ServiceNow/Remedy integration.	**D**		
3. OPERATIONAL REQUIREMENTS & MANAGEMENT				

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3.1	Provides a role-based, multi-tenant, customizable web user interface with executive and operational dashboards.	**D**		
3.2	Provides a cross-platform centralized management console supporting both Windows, UNIX, Linux, and cloud environments.	**M**		
3.3	Lightweight agent deployment supporting Windows, Linux (RHEL, Ubuntu, SUSE), AIX, Solaris, and container hosts.	**M**		
3.4	Provides standard sets of default templates and policy baselines for all supported operating environments and workloads.	**M**		
3.5	Central management console continuously monitors agent health, operational status, versioning, and communication links.	**M**		
3.6	Single-pane-of-glass coverage across servers, desktops, POS endpoints, hypervisors, network infrastructure, databases, and container clusters.	**D**		
3.7	Centralized remote agent management: Remotely push policy updates, software upgrades, configuration changes, and debug logs.	**M**		
3.8	End-to-End Encryption: Encrypts all communications between agents, management servers, and database repositories using TLS 1.3/AES-256.	**M**		
3.9	Granular Access Control: Implements RBAC following the principle of least privilege for user accounts, groups, and tenant domains.	**M**		
3.10	Initial Baseline Generation: Captures a known-good cryptographic state baseline across file systems and configurations upon deployment.	**M**		
3.11	Gold Baseline Distribution: Creates single master baselines to distribute across server clusters to identify configuration drift.	**D**		
3.12	Delta Scanning: Transmits only delta (changed) data across the network after baseline initialization to minimize network footprint.	**D**		
3.13	Mass Baseline Updates: Supports streamlined multi-baseline updating following authorized maintenance windows or software patches.	**D**		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3.14	Granular Change Tracking: Stores every changed file, registry key, or configuration setting as a discrete, immutable audit record.	**M**		
3.15	Instant Data Retrieval: Provides real-time query and retrieval access to any historical discrete change record in the repository.	**M**		
3.16	Remote Policy Distribution: Pushes updated monitoring and compliance policies to target agent groups centrally without system restarts.	**M**		
3.17	Vendor Policy Library: Access to an continuously updated online library of vendor-maintained policy templates and benchmark rules.	**D**		
3.18	Dynamic Template Wildcards: Supports regular expressions, variables, and wildcards within policy templates to handle variable paths.	**D**		
3.19	Rule Grouping: Allows logical grouping of files, directories, and registry keys into reusable policy modules.	**M**		
3.20	Granular Severity Assignment: Allows administrators to assign distinct severity levels down to individual monitored files and folders.	**D**		
3.21	Directory Recursion: Full directory tree recursive scanning with configurable path depth and exclude options.	**M**		
3.22	Agent Grouping: Groups agents logically by location, OS, environment (Prod/Dev), business unit, or risk level.	**D**		
3.23	Read-Only Auditor Consoles: Supports dedicated view-only console views and access roles for internal and external compliance auditors.	**D**		
3.24	Network Efficiency: Operates seamlessly through firewalls via single standard ports and functions over low-bandwidth WAN connections.	**M**		
3.25	Visual Change Differencing: Provides side-by-side graphical diff tools to quickly highlight exact content line changes between file versions.	**D**		
3.26	Enterprise Scalability: Scalable architecture supporting hundreds of thousands of endpoints across distributed global environments.	**D**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3.27	Change Annotation: Enables security staff to add manual annotations, ticket references, or audit notes to any change record.	**D**		
4. POLICY MANAGEMENT & COMPLIANCE ASSESSMENT				
4.1	Continuous Compliance Integration: Seamlessly triggers immediate automated policy reassessments upon detecting file/config changes.	**M**		
4.2	Hardening Benchmarks: Out-of-the-box security policies based on Center for Internet Security (CIS) benchmarks and DISA STIGs.	**M**		
4.3	Standard Security Frameworks: Native compliance templates for NIST SP 800-53, ISO/IEC 27001, VMware Hardening, and Cyber Essentials.	**M**		
4.4	Regulatory Mapping: Pre-built templates for PCI-DSS v4.0, HIPAA, SOX, FISMA, NERC CIP, GLBA, and local data protection regulations.	**D**		
4.5	Custom Policy Modification: Easily customizes standard benchmark rules to match internal organizational security requirements.	**M**		
4.6	Automated Remediation Guidance: Provides clear, step-by-step remediation advice and scripts to rectify non-compliant configurations.	**M**		
4.7	Non-Existent File Handling: Intelligently handles and ignores policy-referenced files that are not present on target operating systems.	**D**		
4.8	Offline Policy Assessment: Evaluates compliance against existing stored baseline configuration data without re-scanning targets.	**D**		
4.9	Multi-Policy Mapping: Evaluates a single scan dataset against multiple distinct compliance frameworks simultaneously.	**D**		
4.10	Policy Scorecard Weighting: Assigns custom scoring weights to individual compliance tests based on organizational risk priority.	**D**		
4.11	Temporary Policy Exceptions: Supports formal policy exception waivers with start dates, expiration tracking, and approval logs.	**D**		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
4.12	Waiver Auditing: Generates dedicated reports on active policy exceptions, approved waivers, and upcoming expiration dates.	**D**		
5. SECURITY, AUDITING & REPORTING				
5.1	Group Level Access: Defines custom user groups with restricted administrative authority across specific target asset groups.	**M**		
5.2	Central Repository Security: Centralizes all change telemetry in a tamper-proof, write-once audit log repository.	**M**		
5.3	Attribution Auditing: Accurately reports who made a change, what exact lines were modified, when it occurred, and how.	**M**		
5.4	Compliance Proofing: Provides executive proof-of-compliance reports for internal risk committees and external regulatory bodies.	**M**		
5.5	Multi-Level Executive Dashboards: Real-time graphical reporting customized for CISO, SOC Lead, and Audit teams.	**D**		
5.6	Automated Report Exporting: Schedules and exports compliance reports in PDF, CSV, XML, and HTML formats via automated email.	**D**		
5.7	Real-Time Alerting: Sends immediate alerts via Syslog, SNMP traps, Webhooks, Email, and Teams/Slack upon critical changes.	**M**		
5.8	Agent Disconnection Alerts: Automatically triggers critical alerts if an endpoint agent loses connectivity or is tampered with.	**M**		
5.9	Advanced Search Engine: Performs complex, multi-criteria forensic searches across historical change logs and configuration baselines.	**D**		
6. ENTERPRISE INTEGRATION & INFRASTRUCTURE SUPPORT				
6.1	APIs & CLI: Provides complete RESTful APIs and CLI utilities for administrative orchestration and integration with CI/CD pipelines.	**M**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
6.2	ITSM Integration: Native bi-directional integration with ServiceNow, BMC Remedy, and Jira to automatically match changes to change tickets.	**D**		
6.3	SIEM/SOAR Streaming: Streams formatted change logs and alerts directly to Splunk, Microsoft Sentinel, IBM QRadar, and SOAR tools.	**M**		
6.4	Broad Infrastructure Support: Native agent/agentless coverage across Windows Server/Desktop, Linux, UNIX (AIX/Solaris), VMware ESXi, Network Devices (Cisco, Fortinet, Palo Alto), Active Directory, and Enterprise Databases (Oracle, MS SQL, PostgreSQL, DB2).	**M**		

Tool 6: MANDATORY PASS EVALUATION FOR A-ASM (ACTIVE ATTACK SURFACE MANAGEMENT)

- The below Checklist shall form part of the preliminary mandatory technical functionality compliance Checklist that Bidders must respond to in the given format for the functionality of the Items under this Procurement;

- Technical requirements shall be classified as Mandatory (M) or Desirable (D). Only failure to meet an explicitly designated Mandatory requirement shall result in technical disqualification. Desirable requirements shall be assessed through the applicable technical scoring criteria.
-
- Requirements shall be based on functional, security, interoperability, and performance outcomes. Equivalent technical approaches, including integrated and interoperable multi-vendor solutions, shall be accepted where they demonstrably meet the specified requirements.
-

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1. INTERNET INDEXING, DATA COLLECTION & DISCOVERY ENGINE				
1.1	Discovery Performance: The solution shall perform frequent, internet-wide discovery of the Purchaser's external assets using its own or licensed scanning and indexing sources, with confidence scoring for each attributed asset. Discovery performance (coverage, attribution accuracy and false-positive rate) shall be demonstrated against a list of known Government assets during acceptance testing.	**M**		
1.2	First-Party Data Generation: Generates direct, first-party scan data without relying on third-party data broker aggregations.	**D**		
1.3	Scanning Frequency: Conducts continuous internet indexing with daily or faster re-scan frequencies across identified organizational assets.	**M**		
1.4	Port Scanning Breadth: Covers 2,500+ network ports to ensure comprehensive detection of non-standard services and administrative interfaces.	**D**		
1.5	Full Protocol Handshakes: Performs full application layer protocol handshakes (not simple TCP banners) to accurately identify active services.	**D**		
1.6	Web Crawling & Visual Capture: Renders and crawls external web applications, capturing page screenshots, DOM structure, and security headers.	**D**		
1.7	Dual Stack Support: Full, native discovery support across both IPv4 and IPv6 address spaces.	**M**		
1.8	SOC Integration: Provides external asset visibility within the SOC platform, either natively or through secure, documented APIs, to map external exposure in near real time.	**M**		
1.9	Unified Automation Engine: Feeds discovered external assets and exposures directly into the SOC incident management engine natively or through secure, documented APIs.	**M**		

Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
1.10	Rogue Asset Discovery: Automatically detects unmanaged, shadow IT, and rogue assets connected to public-facing infrastructure.	**M**		
2. ASSET IDENTIFICATION & ENUMERATION				
2.1	IP Range Discovery: Discovers and maps organizational IPv4/IPv6 subnets, netblocks, and Hosted ASN ranges.	**M**		
2.2	Certificate Inventory: Automatically discovers SSL/TLS certificates, key lengths, expiration dates, and provides a dedicated Certificate Inventory UI.	**M**		
2.3	Apex & Paid Domain Discovery: Discovers all registered apex, second-level (SLD), and brand domains linked to the organization.	**M**		
2.4	Subdomain Enumeration: Discovers subdomains via passive DNS monitoring, Certificate Transparency logs, and active DNS crawling.	**M**		
2.5	Web Application Mapping: Discovers all active HTTP/HTTPS endpoints, virtual hosts, web apps, API endpoints, and web portals.	**M**		
2.6	Cloud Instance Enumeration: Discovers compute instances, storage buckets (S3, Azure Blobs), and serverless functions across multi-cloud environments.	**M**		
2.7	Service Fingerprinting: Identifies specific software components, versions, OS types, and underlying service frameworks.	**M**		
2.8	Registration & Whois Context: Extracts WHOIS registration context, registrar details, administrative contacts, and DNS SOA records.	**M**		
2.9	AI/ML Asset Attribution: Utilizes machine learning models and expert analyst tuning to map external assets accurately to the organization.	**D**		
3. DATA ENRICHMENT, CLOUD DISCOVERY & ASSET MANAGEMENT				

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3.1	Timestamped Telemetry: Records precise date/time stamps for every scan finding, asset change, and exposure discovery.	**M**		
3.2	GeoIP Context: Enriches discovered assets with precise physical location, country, city, ISP, and hosting provider metadata.	**M**		
3.3	CVE & Vulnerability Mapping: Automatically maps discovered software versions against NVD CVEs, KEV catalogs, and zero-day databases.	**M**		
3.4	Multi-Cloud Coverage: Discovers assets across AWS, Microsoft Azure, Google Cloud Platform, Oracle Cloud, and Alibaba Cloud.	**D**		
3.5	Dynamic CDN Disambiguation: Deduplicates dynamic CDN assets (Cloudflare, Akamai, CloudFront) to prevent duplicate IP noise.	**D**		
3.6	Co-Location Differentiation: Distinguishes between directly owned assets and shared/co-located multi-tenant infrastructure.	**D**		
3.7	Cloud Governance & Alerts: Allows configuration of approved vs unapproved cloud providers and generates immediate policy alerts for shadow cloud.	**D**		
3.8	Attribution Rationale: Provides detailed technical explanations showing why an asset was mapped to the organization.	**M**		
3.9	Confidence Scoring: Assigns a dynamic confidence score (High, Medium, Low) to every attributed asset based on evidence strength.	**M**		
3.10	Asset Sprawl Visibility: Delivers visibility into asset sprawl across domain registrars, DNS providers, certificate authorities, and cloud vendors.	**D**		
3.11	WHOIS & DNS Hygiene: Identifies stale WHOIS/DNS records that require updating to reflect current corporate ownership.	**D**		
3.12	Expirations Forecasting: Tracks and forecasts upcoming domain registration and SSL/TLS certificate expirations to prevent outage risks.	**D**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
3.13	Custom Tagging & RBAC: Supports custom tagging for grouping assets, filtering dashboards, and enforcing granular RBAC access controls.	**M**		
4. RISK ASSESSMENT, PRIORITIZATION & AUTOMATED REMEDIATION				
4.1	Threat Prioritization: Categorizes exposures and prioritizes incidents based on asset criticality, vulnerability severity, and exploitability.	**M**		
4.2	Industry Risk Standards: Utilizes standardized risk scoring models (CVSS v3.1/v4.0, EPSS, CISA KEV) with customization support.	**M**		
4.3	Remediation Guidance: Provides step-by-step technical remediation guidance and patch recommendations for identified exposures.	**M**		
4.4	Alert Correlation: Automatically groups related exposures and sub-domains impacting the same parent service into a single ticket.	**M**		
4.5	Automated Playbooks: Automates remediation via SOAR, including identifying owners, sending email alerts, and opening ServiceNow tickets.	**D**		
4.6	Custom Risk Weighting: Allows security teams to adjust incident weights and risk metrics based on internal business risk tolerance.	**D**		
4.7	Real-Time Risk Scoring: Instantly updates overall organizational security posture scores as new vulnerabilities are resolved or discovered.	**D**		
4.8	Custom Risk Rule Engine: Enables creation, modification, or removal of custom risk scoring logic and threat weighting rules.	**D**		
5. ATTRIBUTION PROOF & PLATFORM GOVERNANCE POLICIES				
5.1	Attribution Evidence Trail: Displays raw DNS records, WHOIS chains, IP ranges, or SSL certificates as proof of asset attribution.	**M**		
5.2	Explicit Confidence Metrics: Clearly displays numerical and qualitative confidence levels for all asset attribution links.	**M**		

Official Use Only
Official Use Only

No.	Description	M/D	Statement of Compliance (Y/N)	Reference / Page
5.3	Policy Engine: Flexible policy engine allowing security teams to quickly build custom fingerprints and detect zero-day CVEs.	D		
5.4	Session Timeout Controls: Configurable user login session timeout controls to ensure platform management security.	M		
5.5	Authorized IP/Domain Access: Restricts platform access to authorized organizational IP ranges and corporate domain lists.	M		
5.6	Distribution List Whitelisting: Configures specific approved domain lists for outgoing security notifications and alert distributions.	D		

2.4 Training and Training Materials

The vendor shall provide training to the ICT Authority and other stakeholders as defined below;

a) Provide cybersecurity training to ICT Authority personnel through OEMs of the supplied technologies.

USER Training should cover, at minimum:

i. SIEM administration
i. SOAR administration
ii. XDR/EDR/NDR
iii. Threat intelligence
iv. Incident response
v. Threat hunting
vi. Digital forensics
vii. Dashboard/report administration
viii. Playbook development
ix. AI/ML SOC use cases
x. System administration
xi. DR operations

b) Develop SOPs for defined cyberattack scenarios and incorporate them into SOC operations.

Official Use Only

c) Develop the SOC Operations Manual and maintain it throughout the contract.
d) Conduct practical exercises using the SOC simulation/test-bed environment.

Official Use Only
Official Use Only

The Vendor shall provide multiple training sessions on need basis.

1. **Operational training :**

As a part of deliverables, the vendor for a five year period will provide the following training

2. **Training on SOC Operations:**
   - The vendor will impart yearly operational training to at least 25 designated officials and resources of the Purchaser at Purchaser's selected location. This training shall cover a session on SOC operations and best practices for information security & general cyber and information security awareness on emerging trends.
   - The duration of each such yearly training session shall be of 3 to 5 days.
   - The standard contents of such training shall be documented and made available to all the users.
   - Two copies in hard and soft format shall be made available to the in-charge of every location. Changes to the same shall be updated periodically as and when required and the same shall be communicated to the respective sites.

3. **Technical Cybersecurity training**
   - The vendor will Conduct half yearly training through cyber security OEMs on provisioned OEM components and multiple emerging threat scenarios as per ICTA's requirement.
   - The biannual training shall be provided to 25 people each. The duration of each such half yearly training shall be at least 5 days
   - Training on SOC capability maturity model certification (CMM5) for 25 officers of ICTA & Beneficiary MDA's.
   - The contents of such trainings would need to be documented and made available to all the Purchaser for training
   - other officers of ICTA.
   - Provide one-time training & certification on provisioned OEM components to 25 members of the Purchaser's team.

4. **(c) Cyber security awareness training for field units**
   - The Vendor Shall conduct cybersecurity awareness training toRICTOs and teams deployed by the purchaser at various county & Subcounty offices (For Government ministries/departments/states). The trainings shall be conducted biannually at purchaser's location.
   - In case of urgent requirement of the Purchaser, more such training shall be conducted on demand. The duration of each such training shall be at least 3 days

Official Use Only
Official Use Only

The bidder should provide:

- Training plan
- Training materials
- Administrator guides
- User guides
- Practical exercises
- Assessment/evaluation materials
- OEM certificates, where applicable
- Knowledge-transfer records

2.5 Data Conversion and Migration

2.5.1 The Supplier MUST provide services and tools to perform the following Data Conversion and Migration Services: *[for example, specify:* ***volume of data; type, structure, and media of data; timing of conversion; quality assurance and validation methods****; etc.]*

Official Use Only
Official Use Only

2.6 Documentation Requirements

he vendor will be responsible for creation and maintenance of all the documentation and shared with the Purchaser as per mutually agreed format and periodicity. The documentation must be consistently updated throughout the contract period, following appropriate change management procedures and version control practices. It is recommended to adhere to international standards and best practices, such as ISO 27001, National Institute of Standards and Technology (NIST) 800-53 when creating the documentation. The documentation shall include but not be limited to the following:

(a) Design (HLD, LLD) and Architecture

(b) Installation and Configuration

(c) Operations manual for the SOC

(d) System administration

(e) Security Hardening manual

(f) Testing manual

(g) Troubleshooting Manual

(h) Standard Operating Procedure

(i) Crisis Management Plan and Manual

(j) Backup Plan and Manual

(k) ISO Compliance Documents

(l) SOC-CMM5 assessment and compliance within the first quarter of issue of first Work Order of Operational phase.

The vendor shall be responsible for maintaining and updating all the documents, related to the supplied components in the instance of but not limited to the following:

(a) Introduction of new ICT components or tools/ Change Management.

(b) Any configuration change impacting functionality, security, or interoperability.

(c) Policy changes issued by the Purchaser or the Government.

Official Use Only
Official Use Only

(d) Findings from audits or incident Root Cause Analysis. Failure to deliver, update, or maintain documentation shall be considered noncompliance to SLA penalties

2.7 Requirements of the Supplier's Technical Team

2.7.1 The Supplier MUST maintain a technical team of the following roles and skill levels during the Supply and Installation Activities under the Contract:

MANPOWER SUPPORT REQUIREMENTS FOR 24X7X365 OPERATIONS

a. The Vendor shall supply technical resources for all components and solutions, including, but not limited to SIEM, SOAR, Storage, Network, Cyber Security, System Administration, Forensics, Threat hunting, Threat detection, Incidence analysis and response etc., who possess the requisite experience stated in the RFP document. The VENDOR/CONTRACTOR shall ensure that the deployed product sets
are supported 24x7x365.
b. The Vendor is required to submit a comprehensive resource deployment plan as part of the technical Bid submission, outlining how technically qualified staff shall be allocated at SOC and DR locations to execute the project. The VENDOR/CONTRACTOR shall be responsible for the monitoring and management of the resources/manpower throughout the project.
c. The specific manpower requirements are outlined , which provide
only an indication of the minimum number of resources needed to undertake various activities as given in the scope of work. The VENDOR/CONTRACTOR bears the responsibility of allocating and supplying
adequate number of resources/manpower to fulfil the scope of work and ensure compliance to Service Level Agreements (SLAs).

Terms and Conditions for Resources/Manpower

Official Use Only
Official Use Only

d. The proposed resources/manpower shall be on the payroll of the vendor or the OEM (based on the
e. requirements outlined in Annex1) during the course of their deployment
f. (The personnel deployed by the vendor under this Contract/Agreement, under no circumstances, be considered employees of the Purchaser. The vendor shall have the sole responsibility for the supervision and control of the personnel deployed in the Project and for payment of such personnel's compensation, including salary, provident fund, withholding of income tax and other taxes, worker's compensation, employee and disability benefits and the like, and shall be responsible for all obligations of an employer, subject to Applicable Law.
g. The Vendor shall designate an experienced and qualified Project Manager as per (Annexx.1) as a single point of contact (SPOC) for the Purchaser.
h. During the Implementation phase, the vendor shall establish a project governance team which shall include the Manpower proposed as part of Technical Bid including Project Manager, designated Team Leads and required number of personnel within vendors's hierarchy in order to support the escalation matrix as evaluated in the TEC. The project Governance team shall continue to function for entire contract period. The project governance team shall be responsible for ensuring compliance, conducting reviews, overseeing the project, and providing status reports as defined in the operations manual or any status report as and when desired by the purchaser.
i. The Vendor shall, to the best of its efforts, avoid any change in the organisational structure proposed for execution of this contract or replacement of any human resource appointed. The vendor shall promptly inform the Purchaser in writing if any such change is necessary. In case of replacement of any human resource, the VENDOR/CONTRACTOR shall ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate handholding period and training for the incoming resource. However, for Deployment of resources as per CVs and deployment plan submitted as part of Technical Bid, penalties shall be applicable as specified.
j. The project governance team and resources shall be continued to be deployed post Go-Live according to the deployment plan shared as part of the Technical Bid, and their CVs submitted during the Technical Bid phase. Throughout the contract, these resources cannot be changed, replaced, or have their level of involvement in the services reduced for any reason. In exceptional circumstances, the Managed Service Provider (VENDOR/CONTRACTOR) is permitted to replace up to 20% of these resources per year after written confirmation from the Purchaser and after proper knowledge transfer.
k. Post implementation, during the Operational phase, project governance meetings shall be scheduled as defined in the operations manual or at a mutually agreed-upon interval with the Purchaser.
l. If the deployed resources don't possess the required skill set or if the resources are not able to deliver on the assigned tasks, the resources shall be replaced (with similar or higher skill set and experience as specified in the RFP) within 30 days of receiving such an intimation from the Purchaser (refer Section6)."The Resources are expected to work in a 24x7 security operations environment.

Official Use Only
Official Use Only

m. If a resource is not available at the place of duty for more than 3 consecutive days, the VENDOR/CONTRACTOR shall provide an alternative resource with similar or higher skill set and experience as specified in the RFP at no additional cost to the Purchaser (refer Section 6).
n. The VENDOR/CONTRACTOR shall be required to provide dedicated professional grade laptops from well-known OEMs with at least 8 Core latest gen 2.4 GHz CPU, 16 GB RAM and 1TB SSD, standalone MS Office professional (latest version) with perpetual license to the deployed resources as per need. The laptops shall not have any VENDOR/CONTRACTOR provided applications, MDM, DLP, Endpoint security or other endpoint solution of the VENDOR/CONTRACTOR. The resources shall install on their laptop, the security and ICT solutions provided by the Purchaser and only applications permitted by the purchaser shall be installed. The resources shall not connect these dedicated laptops anywhere outside Purchaser's network, without an explicit written permission from the Purchaser.
o. The VENDOR/CONTRACTOR shall provide atleast 25 number of latest dual screen desktop systems (with latest generation i9/AMD Ryzen 9 or higher, at least 64 GB RAM and 1TB SSD, standalone MS Office professional (latest version) with perpetual license) to be used as SOC workstations. The workstations shall have only the latest version of Windows Operating Systems and shall not have any other applications, VENDOR/CONTRACTOR provided applications, MDM, DLP, Endpoint security or any other endpoint solution of the VENDOR/CONTRACTOR. These desktop systems shall be installed with Purchaser provided EDR, UEM and shall be hardened as per Purchaser's policy.
p. Any MFPs, Printers/Scanners to be used by the VENDOR/CONTRACTOR deployed teams shall also be provided by the VENDOR/CONTRACTOR.
q. The VENDOR/CONTRACTOR shall be required to provide the documentary proof of the qualifications and experience of the manpower being provided by it during the selection process by the Purchaser.
r. All manpower shall report to the designated nodal officer(s) assigned by the Purchaser. The VENDOR/CONTRACTOR must ensure proper planning for backup manpower to comply with the SLAs. This backup manpower must possess equivalent qualifications and experience as the person(s) they shall replace.
s. VENDOR/CONTRACTOR/OEM shall furnish the proof of employment of the manpower on the payroll of the VENDOR/CONTRACTOR/OEM as and when requested by the Purchaser.
t. Prior to Go-Live, the VENDOR/CONTRACTOR shall carry out background checks of the resources identified to work on this project and submit the background check reports, along with copies of any of the

Official Use Only
Official Use Only

u. officially valid documents in respect of each such resource. The same process shall be followed post Go-Live in respect of any resource who may be replaced or added, prior to his/her deployment on the project. The Purchaser shall also extend necessary cooperation, which may extend to disclosure of income-tax Permanent Account Number and other identification details, professional history including directorships, disclosure regarding criminal prosecution if any and organisational affiliations, and shall require any resources as aforesaid to so cooperate, for such person to undergo security vetting by such government-designated agency as the Purchaser may communicate in writing. If the Purchaser communicates in writing the fact of a resource having been identified as unsuitable by such agency as aforesaid, at any point of time, the VENDOR/CONTRACTOR shall take action to promptly revoke all the access to the SOC and its DR locations on immediate basis and remove such resource from the project immediately in any case not later than 24 hours from the receipt of such communication.

v. The Purchaser shall have the authority to remove or cause to be removed any person employed at the Project site who carries out duties incompetently or negligently, from both in-person and virtual access to the Project resources.

w. If the Purchaser asks the VENDOR/CONTRACTOR to remove a person who is a member of the VENDOR/CONTRACTOR's staff or work force, stating the reasons, the VENDOR/CONTRACTOR shall ensure that the person leaves the site within seven days and has no further connection with the Services under this Contract. All the access to the deployed and integrated components for the said resource shall be revoked on an immediate basis by the VENDOR/CONTRACTOR.

x. The Purchaser reserve the right to change the quantity and location of deployed manpower during the contract period with a written notice, 60 days in advance at no additional cost to the Purchaser.

POST IMPLEMENTATAION, OPERATION, MAINTENANCE & INCIDENCE RESPONSE SUPPORT.

The Vendor under SOC Operation, Maintenance, Support, Incidence Response and MDA Support, will be responsible but not limited to offering the following responsibilities for a period of five years after Go-live and sign-off.

1. SECURITY OPERATIONS MONITORING AND MANAGEMENT

a) The Vendor shall provide monitoring and management services for all the provisioned infrastructure systems related to cyber security from the date of Operational Acceptance.

b) The Vendor shall be responsible for the operation and management of the entire security solutions in order to ensure confidentiality, integrity, availability and non-repudiation of the services on a 24x7x365 basis.

c) The vendor will be required to provide monitoring and management of activities including but not limited to the following:

i. Proactive monitoring, detection, and response to cybersecurity threats and incidents response;

ii. High availability and disaster recovery capabilities to maintain uninterrupted SOC operations; and Capacity Buil;ding, Training, Knowledge Transfer and Skilling.

Official Use Only
Official Use Only

Technical Implementataion Team

a) **Project Manager (1)**
   a. Master's degree in information technology / computer science, or IT discipline
   b. Minimum of 10 years' experience in IT with minimum 5 years proven delivery as a manager in charge of the project) in Project Management – (Provide CV.)
   c. Five (5) Years of Experience in managing IT Project Management, at least 3 NO Projects in similar entities.
   d. PMP or Prince 2 or other equivalent project management certifications.
   e. ITIL Service Management or other equivalent project management certifications.

b) **Cyber-Security engineers (2)**
   a. Degree in Engineering with Information Technology / Computer as specialization, Computer Science, or IT discipline
   b. Minimum of 7 years' experience in system security and Extensive knowledge of computer systems and networks through professional experience.
   c. Relevant Certifications in security
   d. 2 years of experience in similar occupations, such as network administrator and extensive knowledge of networks and active equipment installation through professional experience.
   e. . Must be certified Ethical Hacker Certified

The Engineers must hold professional- or expert-level security certifications relevant to the proposed solutions. The proposed personnel shall hold the stated certification or an equivalent certification demonstrating comparable competencies. The Proposer shall provide evidence of the certification and its relevance to the role.

Integration engineer (2)
   a. Degree in Engineering with Information Technology / Cybersecurity, / Computer as specialization, Computer Science, or IT discipline
   b. Minimum of 5 years' experience in security tools that includes integration of (SIEM, SOAR, API-based integrations, log source onboarding)
   c. Certification in proposed OEM

Lead Enterprise Security Architect (1)

Official Use Only
Official Use Only

a. Degree in Engineering, Computer Science, Cybersecurity Information Technology / Computer as specialization, Computer Science, or IT discipline.
b. Minimum of 10 years' experience in enterprise security architecture, including designing security reference architectures, threat modelling, and security control framework.
c. The Engineers MUST have Cloud Security and Cloud network Certified at Professional level.
d. The Engineers MUST have Information Security Architecture Certification or equivalent like CISPP+ISSAP or SABSA which are purpose-built for security architecture roles
e. The Engineers MUST have Information Security Architecture Certification or equivalent like CISPP+ISSAP, TOGAF or SABSA which are purpose-built for security architecture roles

Network engineers/administrator (1)

a. Degree in Engineering, Cybersecurity, Information Technology / Computer Science specialization, Computer Science, or IT discipline
b. 5 years of experience in similar occupations, such as network administrator and extensive knowledge of networks and active equipment installation through professional experience.
c. At least one Professional Level Security certification: CCNP Security, PCNSE (Palo Alto), Fortinet NSE 7, or Check Point CCSE or equivalent aligned to the Solution being proposed by the Bidder.

GOVSOC Retainer & Incidence Response Service Practice Leads Personel.

SOC Team Lead/Manager (1)

a) Bachelor's degree in ICT, Computer Science, Cybersecurity, Information Security or related field;
b) 8+ years ICT/Cybersecurity experience, 5+ years managing SOC/CSIRT/Incident Response operations
c) At least one of the following Certifications; CISSP, CISM, CRISC, GIAC, ISO 27001/22301 or equivalent

SOC Analyst (3 in No.)

a) Bachelor's degree/diploma in ICT, Cybersecurity, Computer Science or related field;
b) 5+ years cybersecurity/SOC experience, including hands-on monitoring, triage, investigation and incident response
c) At least one of the following Certifications; Security+, CySA+, GCIH, GCIA, CEH or equivalent

Official Use Only
Official Use Only

KEY DELIVERABLES OF VENDOR/CONTRACTOR

The Vendor shall be responsible for end-to-end provisioning, deployment, operation, and management of all supplied components, licenses, and manpower for entire contract duration.

(a) All the components supplied shall:

i. Be provided with full feature and functionality, with the required licensing with no restrictions/limitations for delivering on the required SLA at no additional cost to the Purchaser.
ii. Exhibit high scalability and be deployed on both on premises or ON=Cloud , unless stated otherwise with minimum N+1 high availability (Excluding standalone SOC tools) mode at each site of deployment.

(b) The Vendor must include Annual Maintenance Contracts (AMC), warranty coverage, and provision for office consumables to be used by the VENDOR/CONTRACTOR deployed team throughout the contract period.

(c) The Gross Total Value shall include the cost of hardware, software, licenses, manpower and other required components.

(d) The VENDOR/CONTRACTOR is required to provide a comprehensive breakdown of costs for each individual component, including AMC, warranty, and other associated expenses. This detailed breakdown shall contribute to price discovery and can be utilized by Purchaser for any future procurements, up to 25% of the total contract value.

(e) Bidder is free to quote a solution with higher capacity and capability, which exceeds the requirements provided in this RFP.

(f) The VENDOR/CONTRACTOR shall setup dashboard and alerts as per the requirement of Purchaser.

(g) In addition to O&M of the supplied solutions, the VENDOR/CONTRACTOR shall carry out SOC operational tasks, including but not limited to:

i. Incident Handling and Response
ii. Log monitoring
iii. Dashboard design and customization
iv. Query formulation
v. Correlation rule creation
vi. YARA rule configuration
vii. Snort rule development
viii. Filter and playbook design/implementation
ix. Threat detection and Threat hunting, security threat mitigation and other SOC-related activities.

Official Use Only
Official Use Only

(h) After the deployment of the supplied components and when they are prepared for Go-Live, the VENDOR/CONTRACTOR shall get a thorough review and assessment of the architecture and configuration through the respective Original Equipment Manufacturers (OEMs) and shall submit the same to the Purchaser for signoff prior to Go-Live.

(i) The VENDOR/CONTRACTOR shall integrate the supplied ITSM with all supplied components (Except standalone SOC tools). In addition, the ITSM shall also integrate with Purchaser services like NOC Services, Endpoint security, ZTA, NAC, DRM, DLP, NDR, SSO, SMS Gateway, Email etc.

(j) The SLAs for all purchaser supplied components and services shall be configured on the SOCMIS.

(k) The VENDOR/CONTRACTOR is responsible for ensuring complete automation of the entire solution stack, encompassing both the infrastructure and software aspects. This entails providing the necessary technology solutions for end-to-end automation and management as part of the comprehensive solution offering.

(l) All required Hardware, software, database and operating system licences etc. shall be offered as a part of the solution.

(m) The vendor will be required to provide monitoring and management of activities including but not limited to the following:

EXTENDED POST IMPLEMENTATION OPERATIONAL SUPPORT, MAINTENANCE AND INCIDENCE RESPONSE RETAINER SERVICES

Official Use Only
Official Use Only

Security Operations Monitoring and Management

The Contractor shall be responsible for the operation, administration, maintenance, and support of the GovSOC technologies supplied under this Contract (SOC hardware and devices, SIEM, SOAR, TIP, Anti-DDoS, FIM and ASM).
For existing Government systems and security technologies not supplied under this Contract (including the firewalls, NIPS, WAF, NDR, SSL off-loader, Anti-APT, DLP, DAM, PAM, AAA, server anti-malware/EDR and patch management tools listed in categories A to D below), the Contractor's responsibilities shall be limited to security monitoring, event analysis, incident detection, reporting, and coordination of response activities.
Direct administration, configuration changes, patching, maintenance, or remediation of such existing systems shall remain the responsibility of ICTA or the respective system owners, unless expressly included in the contractual scope. Any response action affecting these systems shall follow approved procedures and authorization arrangements. Where categories A to D below describe maintenance, patching, configuration or lifecycle activities for such systems, they shall be read as monitoring, identification, reporting and coordination with the system owner.

a. The Vendor shall provide monitoring and management services for all the provisioned infrastructure systems related to cyber security from the date of Operational Acceptance.
b. The Vendor shall be responsible for the operation and management of the GovSOC security solutions supplied under this Contract, and for the security monitoring of the existing systems within the limits stated above, to ensure confidentiality, integrity, availability and non-repudiation of the services on a 24x7x365 basis. The team will be required to provide monitoring and management of activities including but not limited to the following:-

Cat.	Category	Items Covered
A	**Perimeter & Network Security Tools**	DDoS, Firewall (IGW/DMZ), NIPS, WAF, NDR, SSL Off Loader
B	**Advanced Threat & Data Protection**	Anti-APT & TIP, Host-based DLP, Database Activity Monitoring
C	**Identity & Access Management**	PAM, AAA
D	**Platform, Patch & Vulnerability Support**	Server Security, Patch Management, Vulnerability Assessment
E	**Governance, Documentation & Reporting**	Operational documentation , knowledge management, incident & service records , SLA monitoring and periodic MIS Reporting for contracted services

A. Perimeter & Network Security Tools

Official Use Only
Official Use Only

A.1 DDoS Mitigation Solution

Monitoring & Operations

- 24x7x365 monitoring of inbound/outbound traffic for volumetric, protocol, and application-layer attacks.
- Real-time anomaly detection using traffic baselining and signature-based methods.
- Auto/manual mitigation via black-holing, rate limiting, or challenge-response mechanisms.
- Escalation handling and proactive threat alerts.
- Detection of a confirmed attack within 5 minutes, with mitigation initiated within 10 minutes of detection.

Incident Response

- Immediate response to DDoS attack events.
- Automated incident notification to all stakeholders, including users.
- Mitigation of false positives to ensure service continuity.
- Root Cause Analysis (RCA) and incident report for each attack.
- Generation of threat intelligence, collection of IOCs, blocking of IOCs on relevant security solutions, and sharing of IOCs with the Purchaser.
- Support during Disaster Recovery (DR) drills and large-scale simulations.

Maintenance & Lifecycle

- Regular patching and firmware updates of DDoS appliances.
- Regular signature updates, with prior intimation to all stakeholders.
- Backup and restore of configuration files.
- Health-check routines and redundancy/failover testing.

Reporting & Governance

- DDoS attack summary, mitigation effectiveness and false-positive rate included in the standard MIS reporting cadence.

A.2 IGW & DMZ Firewall Management

Monitoring & Operations

- Continuous firewall monitoring, including LAN error rates, CPU/memory utilization of data-plane and control-plane, and traffic levels on network interfaces.
- SNMP-based monitoring covering CPU, memory, physical/sub-interfaces and VLANs, with granular reporting and proactive alerting.
- Log file review, trend analysis, and correlation of traffic-flow data.
- Connection/session table monitoring to prevent drops.
- Recommendation of firewall rule/policy changes to ICTA, for implementation by the system owner, based on observed threats and incidents.

Official Use Only
Official Use Only

- Review of firewall policy-change logs and alerting on unauthorised or high-risk changes.

Incident Response

- If a NIC-net IP is continuously attacking and traffic is dropped, notify the ICTA user to remediate the affected system.
- If dropped traffic at the Data Centre exceeds 1% during an attack, notify the concerned ICTA official for further action.
- Escalate any unusual traffic pattern to the ICTA official.
- Generate threat intelligence, collect and block IOCs, and share with the Purchaser.
- Analysis and escalation to the system owner of firewall issues (connectivity, policy, VPN, performance, authentication, logging, HA) within defined SLAs.
- RCA report for major incidents.

Maintenance & Lifecycle

- Administration, configuration (including NAT, VPN and segmentation), patching, firmware updates, backup, failover testing and lifecycle management of the firewalls remain the responsibility of ICTA or the respective system owner. The Contractor shall monitor firewall health and security posture, integrate firewall logs with the SIEM, and report and escalate any required maintenance, patching or configuration action.

Reporting & Governance

- Secure access to logs, policies and performance statistics via protected web portals.
- Monthly health-check, compliance and SLA-adherence reports; capacity/trend analysis of resource utilization.
- Facilitate and support completion of third-party or internal audits, providing logs on request.

A.3 Network Intrusion Prevention System (NIPS)

Monitoring & Operations

- 24x7x365 availability monitoring; traffic profiling and monitoring of attack-logging and generic-deny rule logs.
- Monitoring of attack bandwidth utilization, and of CPU/memory utilization on data-plane and control-plane.
- Monitoring and subscribing to external threat-intelligence sources to evaluate new attacks.

Incident Response

- Define alert levels and incident-response levels; determine intrusion occurrence and restore NIPS availability.
- RCA for security events; analysis of network attacks and serious attack attempts.
- Generate threat intelligence, collect and block IOCs, share with the Purchaser.
- Coordinate with device/machine owners to clean/sanitize compromised endpoints identified via NIPS alerts.

Maintenance & Lifecycle

Official Use Only

- Regular signature upgrades per SOPs, with stakeholder intimation; testing/verification of triggered signatures for false positives with OEMs; fine-tuning and creation of custom/user-defined signatures.
- Regular patching and firmware updates; daily backups of all NIPS.
- Assessment of newly disclosed vulnerabilities; propose corrective/preventive actions.

Reporting & Governance

- Scheduled reporting of intrusions and actions taken, via web-based access, aligned to the standard MIS reporting schedule rather than as an unscheduled "regular report."
- Signature-update turnaround SLA of 24 hours from OEM release for critical signatures.

A.4 Web Application Firewall (WAF)

Monitoring & Operations

- All protected websites/applications placed behind the WAF so that all requests are inspected whenever WAF services are enabled.
- Monitoring of WAF policy mode and effectiveness, and recommendation to the system owner of policy tuning, including the transition from learning mode to protection mode.
- 24x7x365 monitoring of HTTP/HTTPS traffic; reporting of false-positive/negative findings to the system owner.
- Monitoring of IP-reputation, rate-limiting, bot-protection and CAPTCHA events, and recommendation of custom rules to the system owner.
- Monitoring of WAF availability, load-balancer health checks, throughput and failover status.

Incident Response

- Detection, analysis and escalation of application-layer attacks (RFI, LFI, CSRF, etc.).
- Alert generation and analysis of blocked-request logs; incident reporting with payload/attacker detail.
- RCA and mitigation support post-incident.
- Generate threat intelligence, collect and block IOCs, share with the Purchaser.

Maintenance & Lifecycle

- Administration of the WAF, including signature and policy updates, OS/firmware patching, certificate updates and configuration backup, remains the responsibility of ICTA or the respective system owner. The Contractor shall monitor signature currency and platform health and escalate any required action.

Reporting & Governance

- Scheduled WAF activity, blocked-attack and policy-change report included in the standard MIS reporting cadence.

A.5 Network Detection and Response (NDR)

Official Use Only
Official Use Only

Ownership and administration of the NDR platform remain with ICTA or the respective system owner. The Contractor's role is SOC monitoring, detection analysis, incident-response coordination and reporting.

Monitoring & Operations

- 24x7x365 inspection of raw packet data and metadata to establish and continuously baseline normal network behavior.
- Filtering of IOCs and detection of insider abuse, data exfiltration, lateral movement and command-and-control communication that lacks a known signature.
- Use of approved integrations with the firewall and other security controls to request or trigger blocking of suspicious traffic, in accordance with approved playbooks and authorisation arrangements.

Incident Response

- Response actions on positive detection, in accordance with approved procedures and authorisations, such as isolating a compromised device or quarantining malicious traffic.
- RCA and incident reporting for confirmed detections, consistent with other tools in this Schedule.
- Generate threat intelligence, collect and block IOCs, and share with the Purchaser.

Maintenance & Lifecycle

- Updates to NDR detection models, software/OS, configuration backup and health checks are performed by the system owner. The Contractor shall monitor NDR health and detection-content currency and escalate any required action.

Reporting & Governance

- NDR detections, false-positive rate and response actions included in the standard MIS reporting cadence.

A.6 SSL Off Loader

Monitoring & Operations

- Secure intake of SSL keys/certificates from the user via a defined safe-handover mechanism; creation of filters/policies per application requirement.
- 24x7x365 monitoring of SSL/TLS traffic; continuous tuning for performance and security.
- Full certificate lifecycle management (procurement, installation, renewal, revocation), with advance user notification ahead of expiry.
- Enforcement of approved cipher suites, TLS versions and secure negotiation policies.

Incident Response

- Detection and alerting of handshake failures, expired/invalid certificates and insecure protocol use.
- Automatic mechanism to stop traffic flow through a malfunctioning filter.
- Incident reporting for SSL-related events, including possible downgrade or MITM attempts; RCA and remediation guidance.

Maintenance & Lifecycle

Official Use Only

- Regular updates to firmware/software and cryptographic libraries; periodic review of TLS configuration against current best practice (e.g., disabling deprecated protocols).
- Backup and restore of configuration, certificates and private keys; performance tuning to minimize latency at peak load.

Reporting & Governance

- Periodic certificate-inventory and expiry-status report included in the MIS reporting schedule.)

B. Advanced Threat & Data Protection

B.1 Anti-APT Solution & Threat Intelligence Platform

Monitoring & Operations

- 24x7x365 monitoring of network, endpoint and application-level activity for APT indicators; continuous tuning of detection policies.
- Integration/correlation with threat-intelligence feeds; customization of detection/behavioral rules for specific organizational assets.
- On-demand forensic analysis of suspicious files/packet streams.

Incident Response

- Real-time detection and blocking/quarantining of malicious files, processes and command-and-control (C2) communications.
- Alert correlation with SIEM/SOC for advanced triage; detailed incident reports covering attack-chain mapping, malware behavior and IOC/IoA data.
- Sandbox verdict-driven signature creation and enforcement, with a turnaround target of 30 minutes for automated analysis and 4 hours for manual/deep analysis.
- RCA including cyber forensics and coordinated post-incident mitigation; generate and share IOCs with the Purchaser.

Maintenance & Lifecycle

- Regular updates to signatures, heuristics and sandbox analysis engines; patching/upgrading of software, OS components and detection engines.
- Backup and restore of configuration, custom rules and detection profiles; health checks and performance optimization.

Reporting & Governance

- Anti-APT detections and sandbox activity summarized in the standard MIS reporting cadence. (

B.2 Host-based Data Leak Prevention (DLP)

Monitoring & Operations

- Continuous monitoring of Host-based DLP activity across all data-centre servers and user desktops.
- Recommendation to the system/data owner of DLP policy tuning to reduce false-positive/negative alerts.

Incident Response

- Triage of data-exfiltration and policy-violation alerts, with escalation to the relevant system/data owner.

Official Use Only
Official Use Only

- RCA and incident report for confirmed data-loss events; generate and share related IOCs where applicable.

Maintenance & Lifecycle

- DLP agent/OS patching and policy administration remain with the system owner. The Contractor shall monitor DLP agent coverage and policy compliance and escalate any gaps.

Reporting & Governance

- Periodic DLP incident and policy-violation summary included in the MIS reporting schedule

B.3 Database Activity Monitoring (DAM)

Monitoring & Operations

- Continuous monitoring of database access patterns, queries and user behavior.
- Integration of DAM alerts with the SIEM for correlation.

Incident Response

- Alert generation on abnormal or unauthorized database activity, with a defined escalation path to the database/application owner.
- RCA for confirmed unauthorized-access incidents.

Maintenance & Lifecycle

- Patching and version upgrades of the DAM platform itself, on the same cadence as other security tools in this Schedule.
- Maintain audit logs for compliance and forensic purposes.

Reporting & Governance

- Periodic DAM activity and exception report included in the MIS reporting schedule.

C. Identity & Access Management

C.1 Privileged Access Management (PAM)

Monitoring & Operations

- Monitoring of onboarding/de-provisioning of privileged identities and alerting on deviations from approved role-based access policies for critical infrastructure.
- Periodic review of privileged access against approved policies, with findings reported to ICTA.
- Continuous monitoring of session recordings and access logs for all privileged activity.

Incident Response

Official Use Only

- Defined response procedure for a suspected or confirmed compromised privileged account, including escalation to the PAM system owner for session termination and credential rotation, and incident reporting.
- RCA for privileged-access incidents; generate and share related IOCs where applicable.

Maintenance & Lifecycle

- PAM platform administration, backup, patching and integration maintenance remain the responsibility of ICTA or the system owner. The Contractor shall monitor PAM session and access logs through the SIEM, monitor integration health, and escalate any issue.

Reporting & Governance

- Periodic privileged-access review and exception report included in the MIS reporting schedule.

C.2 AAA — Authentication, Authorization, Accounting (50,000 concurrent users)

Monitoring & Operations

- Manage AAA policies for infrastructure- and application-level access control.
- Real-time monitoring of AAA logs and access attempts.
- Redundancy and scalability confirmed through periodic load/capacity testing against the 50,000-concurrent-user target, rather than a stated target alone.

Incident Response

- Defined response procedure for authentication anomalies (e.g., brute-force attempts, credential stuffing), including account lockout, alerting and escalation.
- RCA for confirmed authentication-based incidents.

Maintenance & Lifecycle

- Periodic configuration updates and log archiving.

Reporting & Governance

- Periodic AAA access and anomaly report included in the MIS reporting schedule

D. Platform, Patch & Vulnerability Support

D.1 Server Security (Anti-malware / EDR)

Monitoring & Operations

- Monitoring of anti-malware/EDR alerts and agent coverage across data-centre servers.
- Regular integrity checks and system-hardening reviews.

Incident Response

Official Use Only

- Triage of alerts and coordination with the system owner of the isolation of compromised servers, in accordance with approved procedures.
- RCA and incident report following any isolation event, rather than closing the incident at containment alone

Maintenance & Lifecycle

- Identification and reporting of missing OS patches against the system owner's patching windows (7 days for critical patches, 30 days for routine patches), and tracking of remediation status.
- Monitoring and reporting of compliance with organisational server-security baselines.

Reporting & Governance

- Server-security posture and patch-compliance summary included in the MIS reporting schedule.

D.2 Patch Management

Monitoring & Operations / Maintenance & Lifecycle

- Identification of missing patches across physical and virtual servers and reporting to the system owner, who remains responsible for patch testing and deployment.
- Tracking of the system owner's patch rollouts and verification of patch status after deployment.
- Reporting of patch compliance against the system owner's target timelines by severity: Critical (CVSS 9.0–10) 7 days; High (7.0–8.9) 15 days; Medium/Low next scheduled maintenance window.
- Immediate notification to the system owner of actively exploited (zero-day) vulnerabilities, with recommended mitigations.

Incident Response

- Coordinate with the incident-response function where a patch failure or rollback itself causes a service impact.

Reporting & Governance

- Patch-compliance and rollout report included in the MIS reporting schedule, per defined SLAs.

D.3 Vulnerability Assessment (VA)

Monitoring & Operations / Maintenance & Lifecycle

- Scheduled VA scans: quarterly for external-facing infrastructure, quarterly for internal infrastructure, plus ad-hoc scans following any major change.
- Maintain VA tooling and plugin updates; perform risk scoring for identified findings.

Incident Response

- Coordination of remediation with the system owner, tracking remediation against target timelines by severity: Critical 15 days, High 30 days, Medium 60 days, Low best-effort.

Reporting & Governance

- Risk report and remediation-status report submitted per the MIS reporting schedule.

Official Use Only

E. Governance, Documentation & Reporting

E.1 Documentation & Knowledge Management

- Deployment plan covering timelines, HLD/LLD, architecture layout diagrams, methodology, manpower schedule, test plans and acceptance criteria.
- Configuration, operation and maintenance manuals for every security solution; SOPs for every function of the proposed solutions.
- DR/BCP documentation (backup/restore process, failover testing, escalation contacts).
- Best-practice and continuous-enhancement report submitted to the Purchaser.
- Version-controlled updates reflecting infrastructure/policy changes; documentation format, media and copy count as decided by the Purchaser.
- All documentation to adhere to international standards (ISO/IEC 20000, ISO/IEC 27001, ITIL best practices).
- All documents, diagrams, manuals and SOPs created under this contract are the sole property of the Purchaser.
- Fixed annual documentation-review cycle, independent of ad-hoc updates triggered by an infrastructure or policy change.

E.2 MIS Reporting

- Daily: support-desk issue summary (logged/resolved/escalated), backup/restoration logs, rule-count changes per solution, device issues, uptime/availability summary.
- Weekly: issue/complaint trend analysis, systems-rebooted summary, OEM-logged issues, Data Centre spare-parts inventory, major/minor change summary, cyber-security incident summary, key-infrastructure health-check status, attacks-blocked summary.
- Monthly: component-wise availability/utilization, SLA-adherence report, Data Centre change summary, preventive/scheduled maintenance log, manpower attendance, capacity trend/forecast, attacks-blocked summary.
- Quarterly: SLA-adherence report, resource-utilization trends and recommendations, cyber-security posture review.
- On-demand/ad-hoc: incident-specific RCA, audit-compliance reports, regulatory submissions, or any other report requested by the Purchaser.
- Live dashboard / self-service reporting portal, in addition to the scheduled reports above.
- Fixed submission SLA: all periodic reports delivered within 2 business days of period end

SLA Reference Timelines for Incident Restoration

Service / Activity	Indicative SLA (Enhancement — subject to mutual agreement)
DDoS Mitigation	Detect confirmed attack within 5 minutes; begin mitigation within 10 minutes of detection.
Anti-APT / Sandbox	Automated verdict within 30 minutes; manual/deep analysis within 4 hours of submission.

Official Use Only
Official Use Only

NIPS / WAF Signature Currency (monitoring)	Notify the system owner of critical OEM signature releases within 24 hours and verify deployment status.
Patch-Compliance Monitoring	Report missing critical patches (CVSS 9.0–10) within 24 hours of detection; track remediation against the system owner's timelines (Critical 7 days; High 15 days; Medium/Low next maintenance window).
Vulnerability Remediation Tracking	Report findings within 2 business days of each scan; track and escalate remediation by the system owner (Critical 15 days; High 30 days; Medium 60 days; Low 90 days).
Server Patch-Compliance Reporting	Report patch-compliance status monthly; escalate overdue critical patches (more than 7 days) to ICTA.
Vulnerability Assessment Frequency	Quarterly external and internal scans, plus ad-hoc scans after any major change.
MIS Report Submission	All periodic reports (daily/weekly/monthly/quarterly) delivered within 2 business days of period end.

D. TECHNOLOGY SPECIFICATIONS – SUPPLY & INSTALL ITEMS

3.0 General Technical Requirements

3.0.1 Language Support: All information technologies must provide support for the ***English language of the end-user(s)***. Specifically, all display technologies and software must support the ISO *ISO/IEC 11801*

3.0.2 Electrical Power: All active (powered) equipment must operate on ***voltage range and frequency range****, e.g., 220v +/- 20v, 50Hz +/- 2Hz.* All active equipment must include power plugs standard in *Kenya*

3.0.3 Environmental: Unless otherwise specified, all equipment must operate in environments HVAC conditions in Kenya.

3.0.4 Safety:

3.0.4.1 Unless otherwise specified, all equipment must operate at noise levels no greater than *the recommended levels in Kenya*.

Official Use Only
Official Use Only

3.0.4.2 All electronic equipment that emits electromagnetic energy must be certified as meeting ***emission standard****s in Kenya,* or equivalent, emission standards.

3.1 Computing & Other Hardware Specifications

Technical requirements for active devices

The below minimum technical requirements given in this bid are for reference purpose. Bidders may propose similar, better, or equivalent solutions from any international respected equipment and service providers. The latest version of the product must be proposed.

NB: The Proposer must attach product data sheets that highlight the features matching each requirement/specification.

#	EQUIPMENT/ACCESSORIES DESCRIPTION	QNTY	SPECIFICATIONS OF MATERIALS & EQUIPMENT
	Modular Uninterruptible Power Supply (Ups) System		• Liquid Leak Alerting: Under-floor and drip-tray leak detection sensors integrated to BMS with SOC alerting. • Battery Runtime & Generator ATS: Minimum >=30 min runtime at full load (Best-in-Class: >=90 min, or >=30 min with auto-start generator, ATS <10 sec transfer, and >=24 hr fuel autonomy). • Power Efficiency & Monitoring: Energy efficiency >=94% at 50–100% load with SNMP monitoring (Best-in-Class: >=97%, Li-ion batteries, full remote alerting, 24x7 support). • Grid Waveform Compliance: Output compliant with the ITIC (CBEMA) curve for voltage sag/surge ride-through. • Power Distribution Redundancy: N+1 minimum redundancy with dual A+B feed distribution to all downstream racks • Battery Technology Lifecycle: Li-ion battery technology preferred for lifespan (8–10 yrs vs 3–5 yrs VRLA) and reduced footprint/thermal load.

Official Use Only
Official Use Only

			• Generator Failover Integration: Automatic Transfer Switch (ATS) with tested transfer time <10 sec; fuel autonomy >=24 hrs at full load for generator. • Infrastructure Integration & Certification: Integration with DCIM/BMS; remote firmware update capability; NEBS or IEC 62040 compliance. • Maintenance Bypass: Manual/static maintenance bypass switch enabling zero-downtime maintenance.
	SOC Analyst Workstations & Operations Floor		• Compute Hardware Spec: Core i7 / Ryzen 7 class, 32 GB RAM, 1 TB SSD, TPM 2.0 (Best-in-Class: >=64 GB RAM, >=2 TB NVMe, discrete GPU, 5-yr on-site warranty). • Analyst Multi-Display Setup: Dual 24" FHD (1920x1080) monitors (Best-in-Class: Triple 27" or dual 32" 4K, height-adjustable). • Floor Workspace & Ergonomics: Minimum >=4 m² per analyst, ergonomic desks, structured cabling, access control, CCTV (Best-in-Class: Biometric access, tray/raised-floor cabling). • Endpoint Data Exfiltration Prevention: Hardware root of trust (TPM 2.0) plus port-lockdown (USB disabled by policy) for data-exfiltration control. • Graphics Rendering Performance: Independent GPU output per monitor (not integrated-graphics splitting) to avoid rendering lag on SIEM dashboards. • Secure Console Switching: KVM-over-IP switching for analysts working across classified/unclassified networks (air-gapped consoles). • Ergonomic & Acoustic Standards: Compliance with ISO 9241 ergonomics standard and NC-40 or better acoustic rating for sustained shift work. • Workstation Power Resiliency: Individual desktop UPS or dual power rail to workstations, not just rack-level UPS. • Physical Asset Protection: Cable locks / chassis intrusion-detection switches reporting to asset management.
	Video Wall System (Display Panels)		• Display Resolution & Bezel: Narrow-bezel 55" FHD LCD, >=500 nits, bezel <=3.5 mm (Best-in-Class: 4K or fine-pitch LED <=P1.2, >=800 nits, seamless). • Continuous Operation & Life: 24x7 rated; >=50,000 hrs life; 3-yr on-site warranty (Best-in-Class: >=100,000 hrs, redundant PSU, 5-yr warranty).

Official Use Only
Official Use Only

			• Color Calibration: Factory colour calibration (Delta E < 3) for consistent geo/threat-map interpretation across panels. • Display Uniformity: Panel-to-panel brightness/colour uniformity <=3% variance for a seamless wall appearance • Panel Duty Cycle & Burn-in Protection: Rated for 24x7 continuous operation (commercial-grade, not consumer TV panels) with anti-burn-in technology. • Dual Power Feeds: Dual-input power per panel where budget allows, tied to UPS-A/UPS-B feeds. • Seismic & Vibration Mounting: VESA-compliant mounts rated for seismic/vibration tolerance where applicable.
	Video Wall System (Controller & Management)		• Multi-Source Processing Capability: Minimum >=8 inputs (HDMI/DP/IP), multi-window, FHD/4K support (Best-in-Class: >=32 inputs, 4K60, IP decoding). • System Resilience & Layout Control: Web/GUI layout management; preset layouts; RBAC (Best-in-Class: Hot-standby controller and SIEM/SOAR dashboard integration). • Display Processing Latency: End-to-end glass-to-glass latency <100 ms for real-time incident feeds (CCTV, live dashboards). • Network Interface Redundancy: Dual NIC with automatic failover for IP-based video distribution (AV-over-IP/NDI/SDVoE). • Modular Architecture Expansion: Modular, card-based architecture allowing input/output expansion without full controller replacement. • Access Control & Audit Logging: Role-based access control with audit logging of layout changes (who displayed what, when). • Content Protection & Chroma Subsampling: HDCP 2.2/2.3 compliance for protected content sources; 4K60 4:4:4 chroma support (not 4:2:0) for text legibility.
	Remote Monitoring Supervisor Tablets		• Display & Compute Performance: 10–11" FHD, 6 GB RAM, 128 GB storage, >=8 hr battery (Best-in-Class: >=12", >=8/256 GB, >=12 hr, LTE/5G). • Endpoint Security & Management: MDM enrolment; full-disk encryption; VPN; biometric/PIN lock (Best-in-Class: Per-app VPN, rugged rating IP65+, 3-yr warranty).

Official Use Only
Official Use Only

			• Physical Durability Rating: IP65/IP67 ingress rating and MIL-STD-810G shock/drop tolerance for field use. • Cellular & Wireless Redundancy: Dual-SIM or eSIM with automatic carrier failover; Wi-Fi 6/6E support. • Hardware-Backed Authentication: Hardware-backed biometric (not software-only) plus FIDO2/hardware token support for SOC dashboard MFA. • Power Management: Hot-swappable battery option for extended field shifts. • Classified Data Certification: Common Criteria or FIPS 140-2 certification for devices handling classified SOC data. • Automated Fleet Enrolment: Zero-touch enrolment (Android Enterprise/Apple DEP) for rapid fleet provisioning and remote wipe

Knowledge Transfer and Operational Readiness Acceptance Milestone

The Contractor shall successfully complete all training, knowledge transfer, competency assessment, documentation handover, and operational readiness activities before commencement of the Warranty and Support Period. The issuance of the Knowledge Transfer Completion Certificate shall constitute a contractual acceptance milestone confirming that ICTA has attained the operational capability to independently operate, administer, monitor and maintain the solution. The detailed acceptance requirements are set out in the table below.

Table: Knowledge Transfer and Operational Readiness Acceptance Milestone

Milestone	Activity	Detailed Acceptance Criteria	Verification Method	Documentation Required	Outcome
Training Delivery	Delivery of all contractual training programmes (SOC operations, platform administration, technical	✓ All planned training sessions completed in line with approved training plan			

Official Use Only
Official Use Only

	training, cybersecurity awareness, certification preparation)	✓ Coverage of all required modules across SIEM, SOAR, TIP, ASM, FIM, Anti-DdoS Minimum attendance achieved for designated personnel	Review of training sessions, attendance validation, trainer sign-off	Training plan, attendance registers, course materials, certification records	Training formally completed
Knowledge Transfer Execution	Hands-on mentoring, operational shadowing, administration workshops, SOP walkthroughs	✓ Government personnel actively participate in live operational activities ✓ Demonstrated exposure to real incident handling scenarios All SOPs, runbooks, and administrative procedures transferred and explained	Observation of sessions, mentorship logs, activity tracking	SOPs, runbooks, administration guides, KT logs, mentoring records	Knowledge transfer activities completed
Operational Competency Assessment	Evaluation of staff capability through practical exercises and scenarios	✓ Personnel independently execute key tasks: monitoring, alert triage, escalation, reporting, basic administration ✓ Successful completion of predefined operational scenarios ✓ No critical competency gaps identified	Practical assessments, scenario-based testing, evaluator scoring	Competency assessment reports, test results, evaluation matrix	Operational competency validated
Documentation Handover & Verification	Delivery and validation of all documentation	✓ Complete documentation set delivered (architecture, SOPs, DR procedures, admin manuals) ✓ Documentation reviewed for accuracy, completeness, and usability	Document review workshops, validation sessions	Approved documentation set, review sign-offs	Documentation formally accepted

Official Use Only
Official Use Only

		✓ Government confirms readiness for operational use			
Operational Readiness Validation	End-to-end validation of Government-led operations	✓ Government personnel operate the SOC platform independently for a defined period ✓ Successful execution of end-to-end workflows without vendor intervention ✓ Stable platform operations with no critical issues	Live operational monitoring, supervised independence period	Operational logs, performance reports, validation checklist	Operational readiness confirmed
Knowledge Transfer Acceptance Gateway	Formal review and approval	✓ Completion of training, KT, competency assessment, and documentation handover ✓ No critical findings or unresolved gaps All acceptance criteria formally met	Formal acceptance review meeting and audit	KT completion checklist, signed acceptance certificate	Knowledge Transfer Completion Certificate issued
Warranty Commencement	Start of warranty and support period	✓ Issuance of Knowledge Transfer Completion Certificate Confirmation of operational independence and readiness	Contractual confirmation and approval	Signed handover and acceptance documents	

Following successful completion of all contractual training, knowledge transfer, competency assessment and documentation handover requirements, the Contractor shall facilitate an Independent Operations Period during which designated ICTA personnel shall operate

Official Use Only
Official Use Only

the solution without direct vendor intervention. Successful completion of this milestone shall constitute the Knowledge Transfer Sign-off and shall be a contractual prerequisite for commencement of the Warranty and Support Period.

Official Use Only
Official Use Only

Knowledge Transfer Sign-off and Independent Operations Acceptance Milestone

MILESTONE	ACTIVITY	ACCEPTANCE CRITERIA	OUTCOME
Knowledge Transfer Completion	Completion of all training, mentoring, documentation handover, and operational coaching	All contractual training and documentation deliverables accepted	Knowledge transfer completed
Independent Operations Period	ICTA personnel operate the platform independently for a minimum period of 10–15 consecutive working days (or another period specified in the Contract), with the vendor providing only remote advisory support upon request	ICTA staff successfully perform routine monitoring, incident triage, response coordination, reporting, platform administration, and escalation without vendor intervention in normal operations	Operational competency demonstrated
Operational Readiness Assessment	Joint evaluation of ICTA's operational capability against agreed performance criteria	All critical operational tasks completed satisfactorily; no significant competency gaps identified	Operational readiness confirmed
Knowledge Transfer Sign-off	Formal certification by the Procuring Entity that ICTA personnel can independently operate and administer the platform	Successful completion of the independent operations period, competency assessment, and acceptance of all documentation	Knowledge Transfer Completion Certificate issued
Post-Implementation Commencement	Post-implementation support	Issuance of the Knowledge Transfer Completion Certificate	Warranty period begins

Official Use Only
Official Use Only

1. List of Related Services and Completion Schedule

The schedule below will define the completion schedule.

Items 1: Delivery of Hardware, SOC Analysts Compute, Hosting Servers and Storage requirements

*The schedule below defines the Related Services to be provided by the Contractor and their respective completion dates under the Contract. "**T**" refers to the **Effective Date of the Contract***

Service	Description of Service	Quantity[1]	Physical Unit	Place where Services shall be performed	Final Completion Date(s) of Services
1. Delivery, Installation, Inspection and Verification of GovSOC Compute and Related Equipment	a) Complete delivery of the SOC compute infrastructure, hosting servers, storage and other related equipment in accordance with the BoM and Technical Specifications. b) Installation of the complete hardware, including mounting in racks or workstations, where required, and power-on of the equipment. c) Physical and technical inspection and verification of the delivered equipment by the Purchaser. d) Submission of delivery documentation, equipment inventory, serial numbers and applicable manufacturer documentation. e) Installation and configuration of the software components specified in the BoM to support testing and UAT. f) Validation of basic functionality in accordance with the approved inspection and acceptance procedures.	1	Service	ICTA/SOC designated premises and other approved locations	**T + 12 weeks, or earlier**

Official Use Only
Official Use Only

2. Configuration, Integration and System Readiness	a) Configuration of the supplied GovSOC platforms, infrastructure and security technologies in accordance with the Technical Specifications. b) System integration of all Contractor/OEM-supplied platforms required for GovSOC readiness. c) Integration in accordance with applicable OEM requirements and approved technical specifications. d) Conduct of functional, integration and system-readiness testing in accordance with the approved test plan. e) Demonstration that the implemented solution performs in accordance with the approved technical requirements. f) Submission of configuration, integration and testing documentation. g) Written confirmation by the Purchaser of system readiness for operational onboarding.	1	Service	ICTA/GovSOC designated premises and approved ICT environments	**T + 26 weeks, or earlier**
3. Onboarding of ICTA CII, Devices and Related Documentation	a) Successful onboarding and integration of the agreed ICTA Critical Information Infrastructure (CII), devices, systems and other approved ICT assets. b) Configuration and validation of the required security data sources, logs, events and telemetry. c) Verification that required security logs, events and telemetry are being received, processed, correlated and monitored by the GovSOC solution. d) Completion of the agreed onboarding and integration activities. e) Updating of the asset inventory, integration records, operational procedures and other	1	Service	ICTA/GovSOC designated premises and approved ICT environments	**T + 33 weeks, or earlier**

Official Use Only

	relevant documentation. f) Conduct of onboarding validation and acceptance testing. g) Submission of the updated system, asset, integration and operational documentation for approval by the Purchaser.				
4. Training and Knowledge Transfer	a) Provision of SOC operational training to the designated ICTA personnel, including SOC operations, monitoring, incident handling and applicable security best practices. b) Provision of hands-on technical training through the relevant OEMs on the provisioned security technologies and components. c) Training on relevant emerging cyber-threat scenarios and use cases. d) Provision of agreed SOC capability maturity training/certification, where specified in the Technical Specifications. e) Provision of OEM product training and certification to designated ICTA personnel. f) Provision of cybersecurity awareness training to designated MDA teams in accordance with the Technical Specifications. g) Provision of training materials and documentation in the agreed formats. h) Submission of a training completion and knowledge-transfer report.	1	Service	ICTA/GovSOC premises, designated OEM training centres and other approved locations	**T + 26 weeks, or earlier**
5. Operational Support, Maintenance and Local Professional Support	Provision of the contracted support and maintenance services, including 24x7x365 operational support, real-time monitoring, threat hunting, threat detection, incident handling and response capabilities, together with local professional support, in accordance with the	1	Service	ICTA/GovSOC designated premises and approved remote locations	**Five (5) years from the date of Operational Acceptance**

Official Use Only

	Service Level Requirements and Technical Specifications.				
6. Operational Acceptance and Completion of Implementation	a) Completion of all contractual implementation deliverables. b) Completion of system commissioning and Operational Acceptance Tests. c) Resolution of Critical and High-priority defects and non-conformities, or implementation of an acceptable corrective action plan approved by the Purchaser. d) Submission and approval of final technical, operational, configuration, as-built and other contractual documentation. e) Completion of all agreed training and knowledge-transfer obligations. f) Demonstration that the GovSOC solution is operational and performs in accordance with the Contract. g) Issuance of the **Operational Acceptance Certificate** by the Purchaser.	1	Service	ICTA/GovSOC designated premises	**T + 35 weeks (Operational Acceptance)**
7	GovSOC SOC-CMM Compliance & Assessment and maintenance (Phase II)				Phase II

[1] If applicable.

The schedule below will define the respective **Training and Documentation Services** completion schedule.

Official Use Only
Official Use Only

Service	**Description of Service**	Quantity1	Physical Unit	Place where Services shall be performed	Final Completion Date(s) of Services
1	**AS Build Training on SOC Operations:** a) The vendor shall impart operational training to at least 20 designated officials and resources of the ICT Authority at a designated Accredited OEM center out of country. This training shall cover a session on SOC operations and best practices for information security & general cyber and information security awareness on emerging trends. The duration of each yearly training session shall be of 5 to 8 days. b) The standard contents of such training shall be documented and made available to all the users. Two copies in hard and soft format shall be made available to the in-charge of every location. Changes to the same shall be updated periodically as and when required and the same shall be communicated to the respective sites.	1	Service		T +9 Months, or earlier .

Official Use Only
Official Use Only

	Technical training: (i) Conduct a hands on technical training through cyber security OEMs on provisioned OEM components and multiple emerging threat scenarios as per Authority's 's requirement. (iii) Training on SOC capability maturity model certification (CMM5) for 20 officers of ICTA . (iv) The contents of such trainings would need to be documented and made available to all the Purchaser for training other officers of ICTA. (v) Provide one time training & certification on provisioned OEM components to 20 members of the ICTA's team.				

Official Use Only
Official Use Only

2	**Cyber security awareness training for MDA units:** (a) The Vendor Shall conduct cybersecurity awareness trainings to DCISOs and teams deployed by the purchaser at various Government ministries/departments/states. The trainings shall be conducted at purchaser's location. In case of urgent requirement of the Purchaser, more such training shall be conducted on demand. The duration of each such training shall be at least 3 days.				
3	**Five Year Support , Maintenance and Local professional support INCLUDING** 24x7x365 operations with real-time monitoring, Threat hunting, Threat detection, and incident handling response capabilities.	1	Service		T +9 Months, or earlier .
4	GovSOC SOC-CMM Compliance & Assessment and maintenance (Phase II)				Phase II

Official Use Only
Official Use Only

The schedule below will define the respective **Documentation** completion schedule.

The Vendor shall be responsible for creation and development of all the documentation and shared with the ICT Authority.

The documentation must be consistently updated throughout the contract period, following appropriate change management procedures and version control practices. It is recommended to adhere to international standards and best practices, such as ISO 27001, National Institute of Standards and Technology (NIST) 800-53 when creating the documentation. The documentation shall include but not be limited to the following:

i. Design (HLD, LLD) and Architecture
ii. Installation and Configuration
iii. Operations manual for the SOC
iv. System administration
v. Security Hardening manual
vi. Testing manual
vii. Troubleshooting Manual
viii. Standard Operating Procedure
ix. Crisis Management Plan and Manual
x. Backup Plan and Manual

COMPLETION REQUIREMENTS

Upon completion, the Contractor shall provide:

b) As-built drawings.
c) Operation Manuals.
d) Standard Operating Procedures (SOPs) and System Documentation.
e) Training Completion Records and Certification (where applicable).
f) **Knowledge Transfer Completion Certificate (Knowledge Transfer Sign-off), confirming successful operational competency assessment and independent operation of the platform by designated ICTA personnel.**
g) Testing and Commissioning Certificates for all supplied systems(all M&E installations)
h) Warranty Certificates.
i) Cleaning and handover documentation

Official Use Only
Official Use Only

3.2 Network and Communications Specifications *[If this has to be specified; As applicable]*

3.2.1 Local Area Network:

3.2.1.2 Cabling:

3.2.2 Wide-Area Network: Applicable as 3.2.1

3.2.2.1 Equipment and software: *[for example, specify:* ***protocols supported; performance levels; expandability; fault tolerance; administration, management, and security features****; etc.]*

3.2.2.2 Telecommunications Services: *[for example, specify:* ***media; capacity; protocols supported; performance levels; expandability; fault tolerance; administration, management, and security features****; etc.]*

3.2.3 Other Communications Equipment: *[for example, specify:* ***modems; facsimile devices; modem and facsimile servers****, etc.]*

3.2.4 Video Conferencing/Congress Equipment:

3.2.5.

3.3 Ancillary Hardware Specifications *[If this has to be specified; As applicable]*

3.3.1 Shared Data Storage Devices: *[specify:* ***disk; tape; optical storage devices, including capacities, interfaces, hardware-based administration/diagnostics/failover****, etc.]:*

3.3.2 Shared Output and Input Devices:

3.3.2.1 General Requirements: Unless otherwise specified, all shared output and input devices must be capable of handling A4 standard sized paper.

3.3.2.2 Printers: *[for example, specify:* ***high-speed, high-quality printer; standard-speed, high-quality printer; high-speed, large-format (A3) printer; color, high-quality printer, video and output devices****; etc.]*

3.3.2.3 Scanners: *[for example, specify:* ***scanner resolution; paper- / film-handling features; speed****; etc.]*

Official Use Only
Official Use Only

3.3.3 Power Conditioning Devices:

3.3.3.1 Uninterruptable Power Supplies: *[*

3.3.4 Specialized Furnishing/Equipment:

3.3.4.1 Equipment Cabinets/Racks:

3.3.4.2 Environment Control Equipment: *[for example, specify:* ***air conditioning units; humidity control equipment; etc****.]*

3.3.4.3 Physical Access Control Equipment: *[for example, specify:* ***door entry controls; intrusion detection; video surveillance****, etc.]*

3.3.4.3 Logical Access Control Equipment: *[for example, specify:* ***secure identity tokens; token readers****, etc.]*

3.4 Standard Software Specifications Included in the in the supplied equipment *as per Section 3.2.2*

3.4.1 System Software and System-Management Utilities:

3.4.1.1 Processing unit type 1: *[for example, specify:* ***operating system; back-up, optimization, anti-virus, and other utilities; systems administration, maintenance, and troubleshooting tools****; etc.]*

3.4.1.2 Processing unit type 2: *[for example, specify:* ***operating system; back-up, optimization, anti-virus, and other utilities; systems administration, maintenance, and troubleshooting tools****; etc.]*

3.4.1.3 Etc...

3.4.2 Networking and Communications Software: *[for example, specify:* ***protocols, media and equipment to be supported; network services, management and administration features; security and failure management features****; etc.]*

3.4.3 General-Purpose Software: *[for example, specify:* ***office automation software; programming tools and libraries****; etc.]*

3.4.4 Database Software and Development Tools: *[for example, specify:* ***database and database management feature; development tools and environments****; etc.]*

3.4.5 Business Application Software: *[for example, specify:* ***specific business functions to be supported in native code; application management feature; customization options and tools****; etc.]*

Official Use Only
Official Use Only

3.5 Consumables – Not Applicable

3.5.1 Printer Ink / Toner – Printer Type 1:

3.6 Other Non-IT Goods – Not Applicable

3.6.1 Workstation Desks:

3.6.2 Photocopiers:

3.6.3 Specialized Mechanical Systems – Datacenter *[for example, specify:* ***raised floor system, electrical distribution subsystem****, etc.]*

E. TESTING AND QUALITY ASSURANCE REQUIREMENTS

4.1 Inspections

4.1.1 Factory Inspections: *The equipment listed in Section 3 will be inspected before shipment.*

4.1.2 Inspections following delivery: The Purchaser shall inspect and verify delivered equipment at the delivery/installation site at Telposta Towers, 23rd Floor, Kenyatta Avenue, Nairobi, Kenya, before acceptance. The Supplier shall give at least five (5) working days' written notice of any proposed factory inspection. Inspection shall verify quantities, model/serial numbers, conformity with the specifications, completeness of accessories and applicable functional tests. The Supplier shall provide test records and bear its own costs of inspection and any factory visit requested as part of its Proposal. Non-conforming items shall be corrected or replaced by the Supplier at no additional cost before acceptance.

4.2 Pre-commissioning Tests

4.2.0 In addition to the Supplier's standard check-out and set-up tests, the Supplier (with the assistance of the Purchaser) must perform the mutually agreed tests on the System and its Subsystems before Installation/Commissioning.

4.2.1 *The list of Acceptance Tests will be provided during Equipment Commissioning*

4.2.2

4.2. N The Entire System: Pre-commissioning Tests for the entire System are: *as mututally agreed between the Supplier and the Purchaser.*

4.3 Operational Acceptance Tests

4.3.0 Pursuant to GCC Clause 27 and related SCC clauses, the Purchaser (with the assistance of the Supplier) will perform the mutually agreed tests on the System and its Subsystems following Installation to determine whether the System and

Official Use Only
Official Use Only

the Subsystems meet all the requirements mandated for Operational Acceptance.

#	Tool / Component	Functionality Expected	Test Scenario (What Was Tested)	Expected Result
1. SIEM — Security Information & Event Management				
	SIEM	Collects and normalizes logs from all defined sources	Connect all in-scope log sources (firewalls, servers, endpoints, network devices) and observe ingestion	All sources appear in SIEM; logs are parsed and normalized into a common, readable format
		Correlates related events and raises alerts	Simulate a multi-step attack (e.g. repeated failed logins followed by an unusual account login)	A single, consolidated alert is raised linking the related events, not multiple unrelated alerts
		Provides real-time dashboards and reports	View live dashboard during simulated activity; generate a scheduled report	Dashboard reflects activity in real time; report generates automatically without errors
		Retains and allows search of historical logs	Search for logs from a date within the required retention period	Historical logs are found and returned within an acceptable response time
2. SOAR — Security Orchestration, Automation & Response				
	SOAR	Automatically executes response playbooks	Trigger a test incident (e.g. malware alert) and observe the matching playbook	Playbook runs end-to-end (e.g. isolates host, notifies analyst) without manual steps
		Manages incident cases through their lifecycle	Create a case, assign it, update status, and close it	Case status, ownership and history are accurately tracked from open to close
		Integrates with SIEM and TIP for enriched response	Confirm an alert from SIEM arrives in SOAR already enriched with threat intel	Data flows automatically between systems; no manual re-entry of alert details
3. TIP — Threat Intelligence Platform				
	TIP	Ingests external and commercial threat feeds	Check that subscribed feeds are updating on schedule	New indicators appear in the platform automatically, matching feed update frequency
		Enriches indicators (IP, domain, file hash) on request	Submit a known indicator for a lookup	Platform returns reputation and context data within an acceptable response time
		Shares intelligence automatically with SIEM/SOAR	Confirm new indicators are pushed to SIEM/SOAR without manual upload	Indicators appear in SIEM/SOAR correlation rules automatically
4. Anti-DDoS				
	Anti-DDoS	Detects volumetric/application-layer attacks	Simulate a DDoS attack in the test environment	Attack is detected within the agreed SLA time
		Mitigates attacks automatically	Observe system response once an attack is detected	Malicious traffic is scrubbed/blocked while legitimate traffic continues unaffected
		Alerts SOC and produces a mitigation report	Review notification and report generated after the test attack	SOC is notified in real time; report clearly summarizes attack and action taken
5. FIM — File Integrity Monitoring (Phase II)				
	FIM	Detects unauthorized file/configuration changes	Modify a monitored file or folder on a protected system	Change is detected and alerted on in near real time, showing what changed and by whom

Official Use Only
Official Use Only

#	Tool / Component	Functionality Expected	Test Scenario (What Was Tested)	Expected Result
		Integrates alerts into the SIEM	Confirm the FIM alert appears in the SIEM console	Alert is visible and correlated alongside other security events
6. ASM — Attack Surface Management (Phase II)				
ASM		Discovers internet-facing and shadow-IT assets	Run an external attack-surface scan against the organization's domains	Known and previously unknown internet-facing assets are identified and listed
		Identifies exposures and misconfigurations	Review scan findings for exposed services, expired certificates, open ports	Exposures are accurately flagged and given a risk rating
		Feeds findings into SIEM/SOAR for triage	Confirm high-risk findings appear as alerts/cases for the SOC team	Findings are visible to analysts for triage without manual transfer
7. SOC Facility & Infrastructure				
22	UPS / Power Supply	Sustains operations through a power failure	Simulate a mains power outage	UPS takes over seamlessly and sustains systems for the required runtime
23	Analyst Workstations	Give analysts full access to SOC tools	Log in to a workstation and open SIEM, SOAR and TIP dashboards	All tools load correctly and are usable from the workstation
24	Video Wall System	Displays live SOC dashboards to the floor	Push live dashboards/feeds to the video wall	Video wall displays real-time data clearly, without lag or distortion
25	Remote Monitoring Tablets	Allow secure remote/mobile monitoring	Access SOC dashboards remotely via a supervisor tablet	Dashboards load securely with full visibility, matching the in-room view
8. Integrated SOC Workflows (End-to-End)				
All Tools (Integrated)		Supports a full detection-to-response workflow	Run a complete use case: detection → triage → escalation → response → closure	Workflow completes across all tools with no manual gaps or hand-off failures
		Meets day-to-day operational requirements	SOC analysts perform a live walkthrough of routine daily operations	Analysts confirm the system supports their workflow; formal user sign-off obtained

4.3.1 *The list of Acceptance Tests will be provided during Equipment Commissioning*

Note

Official Use Only
Official Use Only

F. SERVICE SPECIFICATIONS – RECURRENT COST ITEMS

5.1 Warranty Defect Repair

5.1.1 The Supplier MUST provide the following services under the Contract or, as appropriate under separate contracts (as specified in the request for proposals documents).

5.1.1.1 Warranty Defect Repair Service: *As per the contract.*

5.1.1.2 ...

5.2 Technical Support

5.2.1 The Supplier MUST provide the following services under the Contract or, as appropriate under separate contracts (as specified in the request for proposals documents).

The requirements will be listed in the contracts signed for technical support

5.

5.2.1.4 ....

5.3 Requirements of the Supplier's Technical Team

5.3.1 The Supplier MUST provide a technical team to cover the Purchaser's anticipated Post-Operational Acceptance Technical Assistance Activities Requirements (e.g., modification of the Information System to comply with changing legislation and regulations) with the roles and skill levels that are specified below. The minimum expected quantities of inputs by the Supplier's technical support team will be specified in the relevant System Inventory Tables for Recurrent Cost Items provided at the time of contract signing

5.3.2**GovSOC Operating Model and Staffing Requirements**

The Supplier shall provide one (1) SOC Team Lead/Manager three SOC Analysts (3) and an Open Source Platforms (Operating Systems) Expert dedicated and to support GovSOC operations.

Continuous 24×7×365 security monitoring and incident management shall be delivered through a hybrid operating model comprising the dedicated GovSOC personnel and the Supplier's remote SOC capabilities.

The Supplier shall provide additional remote technical and specialist support, as necessary, for threat hunting, incident response, platform administration, network security, and digital forensics, in accordance with the prescribed Service Level Agreements (SLAs).

Official Use Only
Official Use Only

The Supplier shall submit a staffing, shift coverage, and escalation plan demonstrating how continuous service availability, incident response timelines, and operational responsibilities will be maintained within the proposed contract price. The 25 SOC workstations shall constitute operational infrastructure capacity and shall not represent a requirement for simultaneous staffing.

Official Use Only
Official Use Only

Implementation Schedule

Notes on preparing the Implementation Schedule

The Implementation Schedule summarize when and where Installation, and Operational Acceptance should take place for all Subsystems and/or major components of the System, and for the overall System itself – as well as any other major Contract milestones.

***Note**: The delivery date is not presented in the Implementation Schedule. Under Incoterms 2010 for CIP, Delivery refers to the date when the Supplier delivers the goods to the first carrier at the port of embarkation, not to the arrival of the goods at the destination site. Delivery (shipment) date therefore varies according to the country of origin of the goods and the Supplier's chosen method of transport.*

The target dates need to be realistic and achievable in light of the capacity of both the average Supplier and the Purchaser to carry out their respective contract obligations. Also, the Purchaser must take care to ensure that the dates specified in the Schedule are consistent with any specified elsewhere in the request for proposals document, especially in the GCC/SCC (e.g., and/or times specified for the submission and acceptance of the Agreed Project Plan).

The work breakdown structure (deliverables) in the Implementation Schedule should be sufficiently detailed to facilitate careful management of the Contract – but not so detailed that it unnecessarily constrains Proposers from organizing the proposed work in the most efficient and effective manner.

To facilitate the procurement and the contract management processes, the Implementation Schedule, the System Inventory Tables and Price Schedules should be closely linked. In particular, the Implementation Schedule defines the major deliverable Subsystems. For each Subsystem there should be a corresponding System Inventory Table or Tables. These System Inventory Tables catalog the specific items (inputs) comprising the Subsystem, as well as the quantities of each item required (for the supply and install cost items as well as the recurrent cost items). For each System Inventory Table there should be a corresponding Price Schedule that closely mirrors the System Inventory Table. Careful development of these materials will greatly improve the changes of obtaining complete and comparable proposals (and ease the proposal evaluation process) as well as improving the likelihood that the Purchaser's and Supplier's interactions during contract execution are closely orchestrated (thus easing the burden of contract management and improving the likelihood of successful implementation of the Information System).

The sample tables comprise:

(a) An Implementation Schedule Table;

(b) A Site Table(s); and

(c) A Table of Holidays and other Non-Working Days.

Official Use Only
Official Use Only

The Purchaser should modify these tables, as required, to suit the particulars of the System (and Subsystems) to be supplied and installed. The sample text in the tables is illustrative only and should be modified or deleted as appropriate.

The timings stated in the Implementation Schedule should be specified in weeks from Contract Effectiveness. This will ease the maintenance of the request for proposals documents during the preparation and request for proposals processes.

Where appropriate, the Implementation Schedule should indicate the deliverables against which Liquidated Damages may be applied in the event of implementation delays arising from the actions of the Supplier (as governed by the SCC and GCC clause 28). These milestones should be kept to the essential minimum needed by the Purchaser to ensure contract discipline by the Supplier – but not so many that they unnecessarily strain the Purchaser-Supplier relationship upon which the successful implementation of the Information System will invariably depend.

The Site Table(s) catalog the physical location of the site(s) where the System is to be supplied, installed, and operated. The site(s) may consist of a number of branch offices in remote regions, different departments or offices in the same city, or a combination of these. The Purchaser must specify this information in sufficient detail so that Proposers can accurately estimate costs related to:

(a) Delivery and insurance;

(b) Installation, including cabling and inter-building communications, etc.

(c) Perform support services, such as warranty defect repair, maintenance, and other technical support services; and

(d) Other related Service obligations the successful Proposer will have to perform under the Contract, including related travel and subsistence costs.

This information will also help Proposers identify which site(s) may warrant a site visit during the period they are preparing their proposals. If the System presents complex installation challenges, site layout drawings should be included in the Background and Informational Materials Section.

Official Use Only
Official Use Only

Table of Contents: Implementation Schedule

A. Implementation Schedule Table 257

B. Site Table(s) 258

C. Table of Holidays and Other Non-Working Days 259

Official Use Only
Official Use Only

A. IMPLEMENTATION SCHEDULE TABLE

*[Specify **desired installation and acceptance dates for all items in Schedule below, modifying the sample line items and sample table entries as needed.]***

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (Proposer to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
0	Project Plan	- -	- -		- -	W_	no
1	Subsystem 1	1	___		- -	- -	- -
:	etc.						
x	Operational Acceptance of the System as an integrated whole	- -	all sites		- -	W__	yes
y	Recurrent Cost Items	y	- -				
z	etc.						

Note: Refer to the System Inventory Table(s) for the specific items and components that constitute the Subsystems or item. Refer to the Site Table(s) below for details regarding the site and the site code.

- - indicates not applicable. "Indicates repetition of table entry above.

Official Use Only
Official Use Only

B. SITE TABLE(S)

[Specify: ***the detailed information regarding the site(s) at which the System is to be operated]***

Site Code	Site	City / Town / Region	Primary Street Address	Drawing Reference No. (if any)
HQ	Headquarters			
R1	Region 1			
R1.1	Region 1 Head Office			
R1.2	ABC Branch Office			
R1.3	DEF Branch Office			

Official Use Only
Official Use Only

C. TABLE OF HOLIDAYS AND OTHER NON-WORKING DAYS

[Specify: ***the days for each month for each year that are non-working days, due to Holidays or other business reasons (other than weekends).]***

Holiday / Observance	**2027 Date**	**2028 Date**	**Day of Week (2027 / 2028)**	**Status / Impact on Contract Schedule**	**Holiday / Observance**
Holiday / Observance	**2027 Date**	**2028 Date**	**Day of Week (2027 / 2028)**	**Status / Impact on Contract Schedule**	**Holiday / Observance**
New Year's Day	January 1, 2027	January 1, 2028	Friday / Saturday *(Observed Mon, Jan 3)*	Official Non-Working Day	**New Year's Day**
Eid al-Fitr *(Subject to moon sighting)*	March 9, 2027	February 26, 2028	Tuesday / Saturday *(Observed Mon, Feb 28)*	Official Non-Working Day (Gazetted)	**Eid al-Fitr** *(Subject to moon sighting)*
Good Friday	March 26, 2027	April 14, 2028	Friday / Friday	Official Non-Working Day	**Good Friday**
Easter Monday	March 29, 2027	April 17, 2028	Monday / Monday	Official Non-Working Day	**Easter Monday**
Eid al-Adha *(Subject to moon sighting)*	May 16, 2027	May 5, 2028	Sunday *(Observed Mon, May 17)* / Friday	Official Non-Working Day (Gazetted)	**Eid al-Adha** *(Subject to moon sighting)*
Madaraka Day	June 1, 2027	June 1, 2028	Tuesday / Thursday	Official Non-Working Day	**Madaraka Day**
Mazingira Day *(formerly Huduma Day)*	October 10, 2027	October 10, 2028	Sunday *(Observed Mon, Oct 11)* / Tuesday	Official Non-Working Day	**Mazingira Day** *(formerly Huduma Day)*

Official Use Only
Official Use Only

Holiday / Observance	2027 Date	2028 Date	Day of Week (2027 / 2028)	Status / Impact on Contract Schedule	Holiday / Observance
Mashujaa Day	October 20, 2027	October 20, 2028	Wednesday / Friday	Official Non-Working Day	**Mashujaa Day**
Jamhuri Day	December 12, 2027	December 12, 2028	Sunday *(Observed Mon, Dec 13)* / Tuesday	Official Non-Working Day	**Jamhuri Day**
Christmas Day	December 25, 2027	December 25, 2028	Saturday *(Observed Mon, Dec 27)* / Monday	Official Non-Working Day	**Christmas Day**
Boxing Day	December 26, 2027	December 26, 2028	Sunday *(Observed Tue, Dec 28)* / Tuesday	Official Non-Working Day	**Boxing Day**

Official Use Only
Official Use Only

System Inventory Tables

Notes on preparing the System Inventory Tables

The System Inventory Tables detail:

(a) for each Subsystem (Deliverable) indicated in the Implementation Schedule, the Information Technologies, Materials, and other Goods and Services that comprise the System to be supplied and/or performed by the Supplier;

(b) the quantities of such Information Technologies, Materials, and other Goods and Services;

(c) the sites and the location of each on a specific site (e.g., building, floor, room, department, etc.)

(d) the cross references to the relevant section of the Technical Requirements where that item is described in greater detail

The Purchaser should modify these tables, as required, to suit the particulars of the System (and Subsystems) to be supplied and installed. The sample text provided for various sections of the tables is illustrative only and should be modified or deleted as appropriate.

There are two sample formats given for the System Inventory Tables: one for the Supply and Installation cost items and the second for Recurrent Cost Items needed (if any).

Official Use Only
Official Use Only

Table of Contents: System Inventory Tables

System Inventory Table (Supply and Installation Cost Items) *[insert: identifying number]*.....263

System Inventory Table (Recurrent Cost Items) *[insert: identifying number] – Warranty Period*.....264

Official Use Only
Official Use Only

SYSTEM INVENTORY TABLE (SUPPLY AND INSTALLATION COST ITEMS) *[INSERT: IDENTIFYING NUMBER]*

Line item number: *[specify:* ***relevant line item number from the Implementation Schedule (e.g., 1.1)*** *]*

[as necessary for the supply and installation of the System, specify: ***the detailed components and quantities in the System Inventory Table below for the line item specified above, modifying the sample components and sample table entries as needed.*** *Repeat the System Inventory Table as needed to cover each and every line item in the Implementation Schedule that requires elaboration.]*

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
1.	Subsystem 1		- -	- -
1.1	_____			- -
:				
2.	Subsystem 2			- -
2.1	_____			- -
:				

Note: - - indicates not applicable. " indicates repetition of table entry above.

Official Use Only
Official Use Only

SYSTEM INVENTORY TABLE (RECURRENT COST ITEMS) *[INSERT: IDENTIFYING NUMBER] –*

Note: - - indicates not applicable. " indicates repetition of table entry above.

Official Use Only
Official Use Only

Background and Informational Materials

Official Use Only
Official Use Only

Table of Contents: Background and Informational Materials

A. Background.....267

0.1 ... The Purchaser.....267
0.2 ... The Purchaser's Business Objectives for the Information System.....268

B. Informational Materials 268

0.3 ... The Legal, Regulatory, and Normative Context for the Information System 268
0.4 ... Existing Information Systems / Information Technologies Relevant to the Information System.....268
0.5 ... Available Training Facilities to Support the Implementation of the Information System.....268
0.6 ... Site Drawings and Site Survey Information Relevant to the Information System .268

Official Use Only
Official Use Only

Background and Informational Materials

A. BACKGROUND

0.1 The Purchaser -

0.1.1 The Government of Kenya, through the Information and Communications Technology Authority (ICTA), is implementing the Kenya Digital Economy Acceleration Project (KDEAP), financed by the World Bank. This procurement supports the establishment and operationalization of the Government Security Operations Centre (GovSOC) through the supply, installation, integration, testing, commissioning and support of the technology system described in this RFP.

0.1.3 Overview of Purchaser's Project Management and Decision Making Arrangment

Overview of the Purchaser's Project Management and Decision-Making Arrangements

1. Project Governance Framework

The Purchaser,ICT Authority , shall establish a structured project governance framework to oversee the successful implementation of the Supply, Installation, Configuration, Testing, Commisioning and Support of the Government Security Operations Centre (GOVSoc) under the Government of Kenya's **Digital Economy Accelaration Programme (KDEAP)**. The governance framework shall ensure effective planning, coordination, monitoring, and decision-making throughout the implementation of the Contract.

ICTA, as Purchaser and implementing agency, shall administer the Contract through its designated Contract Manager. The designated representative shall coordinate implementation, review deliverables, monitor progress and service levels, record issues and escalate matters requiring a decision by the authorised Project Coordinator. Contractual acceptance shall be issued only by the officer authorised under the Contract. The Supplier shall submit progress, incident and service-level reports to the ICTA CIT chairperson in accordance with the Contract

The project seeks to expand high-speed broadband connectivity to public higher education institutions to support digital learning, research, innovation, administration, and collaboration, thereby contributing to the Government's Digital Economy Agenda and the national objective of improving access to quality higher education.

The governance framework shall provide:

- Strategic oversight and policy direction.

Official Use Only
Official Use Only

- Technical supervision of broadband infrastructure deployment and service delivery.
- Effective contract administration.
- Financial and procurement oversight.
- Risk and quality management.
- Stakeholder coordination.
- Timely decision-making and issue resolution.

The governance structure shall comprise the following levels:

- Project Steering Committee (PSC)
- Project Implementation Unit (PIU)
- Technical Committee (TWC)
- Contract Management Team
- Institution Implementation Teams
- Proposer Project Team

0.2 The Purchaser's Business Objectives for the Information System – NOT APPLICABLE

B. INFORMATIONAL MATERIALS

0.3 The Legal, Regulatory, and Normative Context for the Information System – NOT APPLICABLE

0.4 Existing Information Systems / Information Technologies Relevant to the Information System – NOT APPLICABLE

0.5 Available Training Facilities to Support the Implementation of the Information System – NOT APPLICABLE

0.6 Site Drawings and Site Survey Information Relevant to the Information System – NOT APPLICABLE

Official Use Only
Official Use Only

PART 3 – CONDITIONS OF CONTRACT AND CONTRACT FORMS

Official Use Only
Official Use Only

SECTION VIII - GENERAL CONDITIONS OF CONTRACT

Official Use Only
Official Use Only

Table of Clauses

A. Contract and Interpretation 273

1 ..... Definitions 273
2 ..... Contract Documents 281
3 ..... Interpretation 281
4 ..... Notices 283
5 ..... Governing Law 285
6 ..... Fraud and Corruption 285

B. Subject Matter of Contract 285

7 ..... Scope of the System 285
8 ..... Time for Commencement and Operational Acceptance 286
9 ..... Supplier's Responsibilities 287
10 ... Purchaser's Responsibilities 293

C. Payment 295

11 ... Contract Price 295
12 ... Terms of Payment 296
13 ... Securities 297
14 ... Taxes and Duties 298

D. Intellectual Property 299

15 ... Copyright 299
16 ... Software License Agreements 300
17 ... Confidential Information 302

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System 303

18 ... Representatives 303
19 ... Project Plan 306
20 ... Subcontracting 308
21 ... Design and Engineering 309
22 ... Procurement, Delivery, and Transport 312
23 ... Product Upgrades 314
24 ... Implementation, Installation, and Other Services 315
25 ... Inspections and Tests 315
26 ... Installation of the System 316
27 ... Commissioning and Operational Acceptance 317

F. Guarantees and Liabilities 321

28 ... Operational Acceptance Time Guarantee 321
29 ... Defect Liability 322
30 ... Functional Guarantees 325
31 ... Intellectual Property Rights Warranty 325
32 ... Intellectual Property Rights Indemnity 326
33 ... Limitation of Liability 329

Official Use Only
Official Use Only

G. Risk Distribution 329

34. ... Transfer of Ownership 329
35. ... Care of the System 329
36. ... Loss of or Damage to Property; Accident or Injury to Workers; Indemnification 331
37. ... Insurances 332
38. ... Force Majeure 334

H. Change in Contract Elements 336

39. ... Changes to the System 336
40. ... Extension of Time for Achieving Operational Acceptance 341
41. ... Termination 341
42. ... Assignment 348

I. Settlement of Disputes 348

43. ... Settlement of Disputes 348

J. Cyber Security 351

44. ... Cyber Security 351

Official Use Only
Official Use Only

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 Purchaser and the Supplier, together with the Contract Documents referred to therein. The Contract Agreement and the Contract Documents shall constitute the Contract, and the term "the Contract" shall in all such documents be construed accordingly.

(ii) **"Contract Documents"** means the documents specified in Article 1.1 (Contract Documents) of the Contract Agreement (including any amendments to these Documents).

(iii) **"Contract Agreement"** means the agreement entered into between the Purchaser and the Supplier using the form of Contract Agreement contained in the Sample Contractual Forms Section of the request for proposals documents and any modifications to this form agreed to by the Purchaser 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 request for proposals documents.

(vii) **"Implementation Schedule"** means the Implementation Schedule in Section VII of the request for proposals documents.

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

Official Use Only
Official Use Only

(ix) **"Procurement Regulations"** refers to the edition **specified in the SCC** of the World Bank "Procurement Regulations for IPF Borrowers".

(x) **"**request for proposals **document"** refers to the document issued by the Purchaser on the subject procurement process.

(xi) "**Sexual Exploitation and Abuse" "(SEA)"** means the following:

Sexual Exploitation is defined as any actual or attempted abuse of position of vulnerability, differential power or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially or politically from the sexual exploitation of another.

Sexual Abuse is defined as the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions.

(xii) **"Sexual Harassment" "(SH)"** is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature by the Supplier's Personnel with other Supplier's or Purchaser's personnel.

(b) entities

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

(ii) **"Purchaser's Personnel"** means all staff, labor and other employees of the Project Manager and of the Purchaser engaged in fulfilling the Purchaser's obligations under the Contract; and any other personnel identified as Purchaser's Personnel, by a notice from the Purchaser to the Supplier;

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

(iv) **"Supplier"** means the firm or Joint Venture whose proposal to **perform** the **Contract** has

Official Use Only
Official Use Only

been accepted by the Purchaser and is named as such in the Contract Agreement.

(v) **"Supplier's Representative"** means any person **nominated** by the Supplier and named as such in the Contract Agreement or otherwise approved by the Purchaser in the manner provided in GCC Clause 18.2 (Supplier's Representative) to perform the duties delegated by the Supplier.

(vi) **"Supplier's Personnel"** means all personnel whom the Supplier utilizes in the execution of the Contract, including the staff, labor and other employees of the Supplier and each Subcontractor; and any other personnel assisting the Supplier in the execution of the Contract;

(vii) **"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, is subcontracted directly or indirectly by the Supplier.

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

(ix) **"The World Bank"** (also called "The Bank") means the International Bank for Reconstruction and Development (IBRD) or the International Development Association (IDA).

(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

Official Use Only
Official Use Only

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 by the 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 Purchaser, pursuant to GCC Clause 19, based on the requirements of the Contract and the Preliminary Project Plan included in the Supplier's proposal. The "Agreed Project Plan" is the version of the Project Plan approved by the Purchaser, in accordance with GCC Clause 19.2. Should the Project Plan conflict with the Contract in any way, the relevant provisions of the Contract, including any amendments, shall prevail.

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

Official Use Only
Official Use Only

(viii) "System Software" means Software that provides the operating and management instructions for the 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 such in Appendix 4 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 Agreement and such other Software as the parties may agree in writing to be Standard Software.

(xii) "Custom Software" means Software identified as such in Appendix 4 of the Contract Agreement and 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

Official Use Only
Official Use Only

(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 Purchaser 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 Purchaser's expense under the Contract and identified as such in Appendix 5 of the Contract Agreement and such other Materials as the parties may agree in writing to be Custom Materials. Custom Materials includes Materials 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, extract or re-utilize data from, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit or provide access electronically, broadcast, display, enter into computer memory, or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or to authorize or assign others to do so.

(xviii) "Supplier's Equipment" means all equipment, tools, apparatus, or things of every kind required in or 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 Purchaser in accordance with

Official Use Only
Official Use Only

the current edition Incoterms specified in the Contract.

(ii) "Installation" means that the System or a Subsystem as specified in the Contract is ready for Commissioning 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 Clause 27.1 (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 Subsystem, 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 Purchaser of the System (or any Subsystem(s) where the Contract provides for acceptance of the System in parts), in accordance with GCC Clause 27.3 (Operational Acceptance).

(e) place and time

(i) "Purchaser's Country" is the **country named in the SCC.**

(ii) "Supplier's Country" is the country in which the Supplier is legally organized, as named in the Contract Agreement.

(iii) **Unless otherwise specified in the SCC** "Project Site(s)" means the place(s) in the Site Table in the

Official Use Only
Official Use Only

Technical Requirements Section for the supply and installation of the System.

(iv) "Eligible Country" means the countries and territories eligible for participation in procurements financed by the World Bank as defined in the Procurement Regulations.

(v) "Day" means calendar day of the Gregorian Calendar.

(vi) "Week" means seven (7) consecutive Days, beginning the day of the week as is customary in the Purchaser's Country.

(vii) "Month" means calendar month of the Gregorian Calendar.

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

(ix) "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 Subsystem(s).

(x) "Contract Period" is the time period during which this Contract governs the relations and obligations of the Purchaser 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 the terms set out in the Contract**.**

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

(xii) "The Coverage Period" means the Days of the Week and the hours of those Days during which

Official Use Only
Official Use Only

maintenance, operational, and/or technical support services (if any) must be available.

(xiii) 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, either under this 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 **Unless otherwise specified in the SCC**, all Contract Documents and related correspondence exchanged between Purchaser and Supplier shall be written in the language of the request for proposals document (English)**,** 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 governing language under GCC Clause 3.1.1 above, the translation of such documents into the governing language shall prevail in matters of interpretation. The originating party, with respect to such documents shall bear the costs and risks of such translation.

3.2 Singular and Plural

The singular shall include the plural and the plural the singular, except where the context otherwise requires.

3.3 Headings

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

3.4 Persons

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

Official Use Only
Official Use Only

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 Purchaser and Supplier with respect to the subject matter of Contract and supersedes all communications, negotiations, and agreements (whether written or 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 the Contract is performed. All employees, representatives, or Subcontractors engaged by the Supplier in connection with the performance of the Contract shall be under the complete control of the Supplier and shall not be deemed to be employees of the Purchaser, and nothing contained in the Contract or in any subcontract awarded by the Supplier shall be construed to create any contractual relationship between any such employees, representatives, or Subcontractors and the Purchaser.

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 Purchaser for the fulfillment of the provisions of the Contract and shall designate one of such firms to act as a leader with authority to bind the Joint Venture. The composition or

Official Use Only
Official Use Only

constitution of the Joint Venture shall not be altered without the prior consent of the Purchaser.

3.10 Nonwaiver

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 Contract or 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 characteristics or in purpose or utility from its components. The Origin of Goods and Services is distinct from the nationality of the Supplier and 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 shall be sent, pursuant to GCC Clause 4.3 below, by personal delivery, airmail post, special courier, facsimile, electronic mail, or other electronic means, 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

Official Use Only
Official Use Only

by notice sent by airmail post or special courier, except as otherwise specified in the Contract.

4.1.2 Any notice sent by airmail 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 postal authorities or courier service for transmission by airmail or special courier.

4.1.3 Any notice delivered personally or sent by facsimile, electronic mail, or EDI shall be deemed to have been delivered 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 and other communication to be given under the Contract.

4.3 Pursuant to GCC Clause 18, notices from/to the Purchaser 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 Purchaser or Supplier may give and receive notices at their fallback addresses. The address of the Project Manager and the fallback address of the Purchaser are as **specified in 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.

Official Use Only
Official Use Only

5. Governing Law

5.1 The Contract shall be governed by and interpreted in accordance with the laws of the country **specified in the SCC**.

5.2 Throughout the execution of the Contract, the Supplier shall comply with the import of goods and services prohibitions in the Purchaser's Country when

(a) as a matter of law or official regulations, the Borrower's country 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, the Borrower's Country 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 Bank requires compliance with the Bank's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures as set forth in the WBG's Sanctions Framework, as set forth in the Appendix 1 to the GCC.

6.2 The Purchaser 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 procurement 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.

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

Official Use Only
Official Use Only

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 proposal, 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 thereafter proceed 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 for Operational Acceptance of such Subsystem(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).

Official Use Only
Official Use Only

9. Supplier's Responsibilities

9.1 The Supplier shall conduct all activities with due care and diligence, in accordance with the Contract and with the 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 their respective callings and supervisory staff who are competent to adequately supervise the work at hand. The Supplier shall ensure that its Subcontractors carryout the work on the Information System in accordance with the Contract, including complying with relevant environmental and social requirements and the obligations set out in GCC Clause 9.9.

The Supplier shall at all times take all reasonable precautions to maintain the health and safety of the Supplier's Personnel employed for the execution of the Contract at the Project Site/s in the Purchaser's country where the Contract is executed.

If **required in the SCC**, the Supplier shall submit to the Purchaser for its approval a health and safety manual which has been specifically prepared for the Contract.

The health and safety manual shall be in addition to any other similar document required under applicable health and safety regulations and laws.

The health and safety manual shall set out any applicable health and safety requirement under the Contract,

(a) which may include:

(i) the procedures to establish and maintain a safe working environment;

(ii) the procedures for prevention, preparedness and response activities to be implemented in the case of an emergency event (i.e. an unanticipated incident, arising from natural or man-made hazards);

(iii) the measures to be taken to avoid or minimize the potential for community exposure to water-borne, water-based, water-related, and vector-borne diseases,

(iv) the measures to be implemented to avoid or minimize the spread of communicable diseases; and

Official Use Only
Official Use Only

(b) any other requirements stated in the Purchaser's Requirements.

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 Purchaser and on the basis of information that the Supplier could have obtained from a visual inspection of the site (if access to the site was available) and of other data readily available to the Supplier relating to the System as at the date twenty-eight (28) days prior to proposal 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 under its 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 the Purchaser's Country that are necessary for the performance of the Contract, including, without limitation, visas for the Supplier's Personnel and entry permits for all imported Supplier's Equipment. The Supplier shall acquire all other permits, approvals, and/or licenses that are not the responsibility of the Purchaser 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 the Purchaser's Country. 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 Purchaser from and against any and all liabilities, damages, claims, fines, penalties, and expenses of whatever nature arising or resulting from the violation of such laws by the Supplier or its personnel, including the Subcontractors and their personnel, but without prejudice to GCC Clause 10.1. The Supplier shall not indemnify the Purchaser to the extent that such liability, damage, claims, fines, penalties, and

Official Use Only
Official Use Only

expenses were caused or contributed to by a fault of the Purchaser.

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

9.7 Pursuant to paragraph 2.2 e. of the Appendix 1 to the General Conditions of Contract, the Supplier shall permit and shall cause its agents (where declared or not), subcontractors, subconsultants, service providers, suppliers, and personnel, to permit, the Bank and/or persons appointed by the Bank to inspect the site and/or the accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have such accounts, records and other documents audited by auditors appointed by the Bank. The Supplier's and its Subcontractors' and subconsultants' attention is drawn to GCC Clause 6.1 (Fraud and Corruption) which provides, inter alia, that acts intended to materially impede the exercise of the Bank's inspection and audit rights constitute a prohibited practice subject to contract termination (as well as to a determination of ineligibility pursuant to the Bank's prevailing sanctions procedures).

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

9.9 **Code of Conduct**

The Supplier shall have a Code of Conduct for the Supplier's Personnel employed for the execution of the Contract at the Project Site/s.

The Supplier shall take all necessary measures to ensure that each such personnel is made aware of the Code of Conduct including specific behaviors that are prohibited, and understands the consequences of engaging in such prohibited behaviors.

These measures include providing instructions and documentation that can be understood by such personnel, and seeking to obtain that person's signature acknowledging receipt of such instructions and/or documentation, as appropriate.

The Supplier shall also ensure that the Code of Conduct is visibly displayed in the Project Site/s as well as, as applicable, in areas outside the Project Site/s accessible to the local

Official Use Only
Official Use Only

community and any project affected people. The posted Code of Conduct shall be provided in languages comprehensible to the Supplier's Personnel, Purchaser's Personnel and the local community.

The Supplier's Management Strategy and Implementation Plans, if applicable, shall include appropriate processes for the Supplier to verify compliance with these obligations.

9.10 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.

9.11 The Supplier, including its Subcontractors, shall comply with all applicable safety obligations. The Supplier shall at all times take all reasonable precautions to maintain the health and safety of the Supplier's Personnel employed for the execution of Contract at the Project Site/s.

9.12 Training of Supplier's Personnel

The Supplier shall provide appropriate training to relevant Supplier's Personnel on any applicable environmental and social aspect of the Contract, including appropriate sensitization on prohibition of SEA, health and safety.

As stated in the Purchaser's Requirements or as instructed by the Project Manager, the Supplier shall also allow appropriate opportunities for the relevant personnel to be trained on any applicable environmental and social aspects of the Contract by the Purchaser's Personnel and/or other personnel assigned by the Purchaser.

The Supplier shall provide training on SEA and SH, including its prevention, to any of its personnel who has a role to supervise other Supplier's Personnel.

9.13 Stakeholder engagements

The Supplier shall provide relevant contract- related information, as the Purchaser and/or Project Manager may reasonably request to conduct contract stakeholder engagement. "Stakeholder" refers to individuals or groups who:

(a) are affected or likely to be affected by the Contract; and

(b) may have an interest in the Contract.

Official Use Only
Official Use Only

The Supplier may also directly participate in contract stakeholder engagements, as the Purchaser and/or Project Manager may reasonably request.

9.14 Forced Labor

The Supplier, including its Subcontractors, shall not employ or engage forced labour. Forced labour consists of any work or service, not voluntarily performed, that is exacted from an individual under threat of force or penalty, and includes any kind of involuntary or compulsory labour, such as indentured labour, bonded labour or similar labour-contracting arrangements.

No persons shall be employed or engaged who have been subject to trafficking. Trafficking in persons is defined as the recruitment, transportation, transfer, harbouring or receipt of persons by means of the threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power, or of a position of vulnerability, or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purposes of exploitation.

9.15 Child Labor

The Supplier, including its Subcontractors, shall not employ or engage a child under the age of 14 unless the national law specifies a higher age (the minimum age).

The Supplier, including its Subcontractors, shall not employ or engage a child between the minimum age and the age of 18 in a manner that is likely to be hazardous, or to interfere with, the child's education, or to be harmful to the child's health or physical, mental, spiritual, moral, or social development.

The Supplier, including its Subcontractors, shall only employ or engage children between the minimum age and the age of 18 after an appropriate risk assessment has been conducted by the Supplier with the Project Manager's consent. The Supplier shall be subject to regular monitoring by the Project Manager that includes monitoring of health, working conditions and hours of work.

Work considered hazardous for children is work that, by its nature or the circumstances in which it is carried out, is likely to jeopardize the health, safety, or morals of children. Such work activities prohibited for children include work:

Official Use Only
Official Use Only

(a) with exposure to physical, psychological or sexual abuse;

(b) underground, underwater, working at heights or in confined spaces;

(c) with dangerous machinery, equipment or tools, or involving handling or transport of heavy loads;

(d) in unhealthy environments exposing children to hazardous substances, agents, or processes, or to temperatures, noise or vibration damaging to health; or

(e) under difficult conditions such as work for long hours, during the night or in confinement on the premises of the employer.

9.16 Non-Discrimination and Equal Opportunity

The Supplier shall not make decisions relating to the employment or treatment of personnel for the execution of the Contract on the basis of personal characteristics unrelated to inherent job requirements. The Supplier shall base the employment of personnel for the execution of the Contract on the principle of equal opportunity and fair treatment, and shall not discriminate with respect to any aspects of the employment relationship, including recruitment and hiring, compensation (including wages and benefits), working conditions and terms of employment, access to training, job assignment, promotion, termination of employment or retirement, and disciplinary practices.

Special measures of protection or assistance to remedy past discrimination or selection for a particular job based on the inherent requirements of the job shall not be deemed discrimination. The Supplier shall provide protection and assistance as necessary to ensure non-discrimination and equal opportunity, including for specific groups such as women, people with disabilities, migrant workers and children (of working age in accordance with GCC Clause 9.15).

9.17 Personnel Grievance Mechanism

The Supplier shall have a grievance mechanism for personnel employed in the execution of the Contract to raise workplace concerns. The grievance mechanism shall be proportionate to the nature, scale, risks and impacts of the Contract. The grievance mechanism may utilize existing grievance mechanisms, provided that they are properly

Official Use Only
Official Use Only

designed and implemented, address concerns promptly, and are readily accessible to such personnel.

9.18 Security of the Project Site

If stated in the SCC, the Supplier shall be responsible for the security at the Project Site/s including providing and maintaining at its own expense all lighting, fencing, and watching when and where necessary for the proper execution and the protection of the locations, or for the safety of the owners and occupiers of adjacent property and for the safety of the public.

In making security arrangements, the Supplier shall be guided by applicable laws and any other requirements that may be stated in the Purchaser's Requirements.

The Supplier shall (i) conduct appropriate background checks on any personnel retained to provide security; (ii) train the security personnel adequately (or determine that they are properly trained) in the use of force (and where applicable, firearms), and appropriate conduct towards the Supplier's Personnel, Purchaser's Personnel and affected communities; and (iii) require the security personnel to act within the applicable Laws and any requirements set out in the Purchaser's Requirements.

The Supplier shall not permit any use of force by security personnel in providing security except when used for preventive and defensive purposes in proportion to the nature and extent of the threat.

9.19 Recruitment of Persons

The Supplier shall not recruit, or attempt to recruit, either on limited time or `permanent basis or through any other contractual agreement, staff and labor from amongst the Purchaser's Personnel.

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

10. Purchaser's Responsibilities

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

10.2 The Purchaser 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

Official Use Only
Official Use Only

provide such resources, information, and decision making may constitute grounds for Termination pursuant to GCC Clause 41.3.1 (b).

10.3 The Purchaser shall be responsible for acquiring and providing legal and physical possession of the site and access to it, and for providing possession of and access to all other areas reasonably required for the proper execution of the Contract.

10.4 If requested by the Supplier, the Purchaser shall use its best endeavors to assist the Supplier in obtaining in 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 undertakings require the Supplier or Subcontractors or the Supplier's Personnel, 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, Agreed Project Plan, or other parts of the Contract, the Purchaser shall use its best endeavors to assist the Supplier in obtaining such services in a timely and expeditious manner.

10.6 The Purchaser 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 where provision of such items is explicitly identified in the Contract as being the responsibility of the Supplier. Delay by the Purchaser may result in an appropriate extension of the Time for Operational Acceptance, at the Supplier's discretion.

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

10.8 The Purchaser will designate appropriate staff for the training courses to be given by the Supplier and shall make

Official Use Only
Official Use Only

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 Purchaser 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 after Operational Acceptance. However, this shall not limit in any way the Supplier's responsibilities after the date of Operational Acceptance otherwise specified in the Contract.

10.10 The Purchaser 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 Purchaser, save those to be incurred by the Supplier with respect to the performance of the Operational Acceptance Test(s), in accordance with GCC Clause 27.2.

10.12 **Unless otherwise specified in the SCC** the Purchaser shall have no other Purchaser 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 other clauses 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.

Official Use Only
Official Use Only

12. Terms of Payment

12.1 The Supplier's request for payment shall be made to the Purchaser in writing, accompanied by an invoice describing, 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 Purchaser herein shall be deemed to constitute acceptance by the Purchaser of the System or any Subsystem(s).

12.3 Payments shall be made promptly by the Purchaser, but in no case later than forty five (45) days after submission of a valid invoice by the Supplier. In the event that the Purchaser fails to make any payment by its respective due date or within the period set forth in the Contract, the Purchaser 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 made in 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 the Purchaser's Country shall be made to the Supplier through an irrevocable letter of credit opened by an authorized bank in the Supplier's Country and will be payable on presentation of the appropriate documents. It is agreed that the letter of credit will be subject to Article 10 of the latest revision of *Uniform Customs and Practice for Documentary Credits*, published by the International Chamber of Commerce, Paris.

12.6 **As specified in the SCC**, if the Supplier fails to perform its cyber security obligations under the Contract, an assessed amount, as determined by the Project Manager, may be withheld until the obligation has been performed.

Official Use Only
Official Use Only

13. Securities

13.1 Issuance of Securities

The Supplier shall provide the securities specified below in favor of the Purchaser at the times and in the amount, manner, and form specified below.

13.2 Advance Payment Security

13.2.1 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.

13.2.2 The security shall be in the form provided in the request for proposal document or in another form acceptable to the Purchaser. The amount of the security shall be reduced in proportion to the value of the System executed by 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 Purchaser. **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 Clause 12.1.

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

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 the request for proposal document, or it shall be in another form acceptable to the Purchaser.

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

Official Use Only
Official Use Only

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 the Purchaser's country, the Supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the Purchaser's country. Any duties, such as importation or customs duties, and taxes and other levies, payable in the Purchaser's country for the supply of Goods and Services from outside the Purchaser's country are the responsibility of the Purchaser unless these duties or taxes have been 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 Purchaser. 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 the Purchaser's country, and only if these taxes, levies and/or duties are also excluded from the Contract Price in Article 2 of the Contract Agreement and the Price Schedule it refers to.

14.3 If any tax exemptions, reductions, allowances, or privileges may be available to the Supplier in the Purchaser's Country, the Purchaser 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 proposal submission in the Purchaser's Country (also called "Tax" in this GCC Clause 14.4). If any Tax rates are increased or decreased, a new Tax is introduced, an existing Tax is

Official Use Only
Official Use Only

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 Subcontractors, or their employees in connection with 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 Purchaser agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause 16, except that additional copies of Standard Materials may be made by the Purchaser for use within the scope of the project of which the System is a part, in the event that the Supplier does not deliver copies within thirty (30) days from receipt of a request for such Standard Materials.

15.3 The Purchaser'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 Purchaser. The Supplier shall do and execute or arrange for the doing and executing of each necessary act, document, and thing (as legally sufficient) that the Purchaser may consider necessary or desirable to perfect the right, title, and interest of the Purchaser in and to those rights. In respect of such Custom Software and Custom Materials, the Supplier shall ensure that the holder of a moral right in such an item does not assert it, and the Supplier shall, if requested to do so by the Purchaser and

Official Use Only
Official Use Only

where permitted by applicable law, ensure that the holder of such 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 Purchaser, the Supplier hereby grants to the Purchaser license to access and use the Software, including all inventions, designs, and marks embodied in the Software.

Such license to access and use the Software shall:

(a) be:

(i) nonexclusive;

(ii) fully paid up and irrevocable (except that it shall terminate if the Contract terminates under GCC Clauses 41.1 or 41.3);

(iii) **unless otherwise specified in the SCC** valid throughout the territory of the Purchaser's Country;

(iv) **unless otherwise specified in the SCC** subject to NO additional restrictions.

(b) 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 proposal), plus a backup computer(s) of the same or similar capacity, if the primary is(are) inoperative, and during a reasonable transitional period when use is being transferred between primary and backup;

(ii) used or copied for use on or transferred to a replacement computer(s), (and use on the original and replacement computer(s) may be simultaneous during a reasonable transitional period) provided that, if the Technical Requirements and/or the Supplier's proposal 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 backup computer(s) by

Official Use Only
Official Use Only

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 safekeeping or backup purposes;

(v) customized, adapted, or combined with other computer software for use by the Purchaser, provided that derivative software incorporating any substantial part of the delivered, restricted Software shall be subject to same restrictions as are set forth in this Contract;

(vi) **unless otherwise specified in the SCC,** disclosed to, and reproduced for use by, support service suppliers and their subcontractors, to the extent reasonably necessary to the performance of their support service contracts, subject to the same restrictions as are set 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 Purchaser 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, 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 Purchaser and the Supplier, Purchaser 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.

Official Use Only
Official Use Only

17. Confidential Information

17.1 **Unless otherwise specified in the SCC,** the "Receiving Party" (either the Purchaser 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 Purchaser or the Purchaser'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 Purchaser to the extent reasonably required for the Subcontractor to perform its work under the Contract; and

(b) the Purchaser 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 abides 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 Purchaser 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 Purchaser's prior written consent, use any Confidential Information received from the Purchaser for any purpose other than those that are required for the performance of the Contract.

Official Use Only
Official Use Only

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;

(d) is being provided to the Bank.

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.

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, the Purchaser shall appoint and notify the Supplier in writing of the name of the Project Manager. The Purchaser 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 Purchaser 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 Purchaser pursuant to GCC Clause 4.

Official Use Only
Official Use Only

18.2 Supplier's Representative

18.2.1 If the Supplier's Representative is not named in the Contract, then within fourteen (14) days of the Effective Date, the Supplier shall appoint the Supplier's Representative and shall request the Purchaser 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 Purchaser does not object to the appointment within fourteen (14) days, the Supplier's Representative shall be deemed to have been approved. If the Purchaser 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 shall normally 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 Purchaser's prior written consent, which shall not be unreasonably withheld. If the Purchaser consents to such an action, 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 Purchaser's Project Manager and staff, act within their own authority, and abide by directives issued by the Purchaser that are consistent with the terms of the Contract. The Supplier's Representative is responsible for managing the activities of the Supplier's Personnel.

18.2.5 The Supplier's Representative may, subject to the approval of the Purchaser (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

Official Use Only
Official Use Only

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 thereby 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 Clause 18.2.5 shall be deemed to be an act or exercise by the Supplier's Representative.

18.3 Removal of Supplier's Personnel

18.3.1 The Project Manager may require the Supplier to remove (or cause to be removed) the Supplier's Representative or any other person employed by the Supplier in the execution of the Contract, who:

(a) persists in any misconduct or lack of care;

(b) carries out duties incompetently or negligently;

(c) fails to comply with any provision of the Contract;

(d) persists in any conduct which is prejudicial to safety, health, or the protection of the environment;

(e) based on reasonable evidence, is determined to have engaged in Fraud and Corruption during the execution of the Contract;

(f) has been recruited from the Purchaser's Personnel;

(g) engages in any other behaviour which breaches the Code of Conduct, as applicable;

If appropriate, the Supplier shall then promptly appoint (or cause to be appointed) a suitable replacement with equivalent skills and experience.

Notwithstanding any requirement from the Project Manager to remove or cause to remove any person, the Supplier shall take immediate action as appropriate in response to any violation of (a) through (g) above. Such immediate action shall include removing (or causing to be removed) from work on the System, any person Employed by the Supplier in the execution of the Contract who engages in (a), (b), (c), (d), (e) or (g) above or has been recruited as stated in (f) above.

Official Use Only
Official Use Only

18.3.2 If any representative or person employed by the Supplier is removed in accordance with GCC Clause 18.3.1, the Supplier shall, where required, promptly appoint a suitable replacement with equivalent skills and experience.

19. Project Plan

19.1 In close cooperation with the Purchaser and based on the Preliminary Project Plan included in the Supplier's proposal, 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.

19.2 **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 Purchaser. Such submission to the Purchaser shall include any applicable environmental and social management plan to manage environmental and social risks and impacts. The Purchaser 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 the Project Plan and resubmit to the Purchaser. The Purchaser shall, within five (5) days of resubmission of the Project Plan, notify the Supplier of any remaining non-conformities. This procedure shall be repeated as necessary until the Project Plan is free from non-conformities. When the Project Plan is free from non-conformities, the Purchaser shall provide confirmation in writing to the Supplier. This approved Project Plan ("the Agreed Project Plan") shall be contractually binding on the Purchaser and the Supplier.

19.3 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 39 and 40.

19.4 The Supplier shall undertake to supply, install, test, and commission the System in accordance with the Agreed Project Plan and the Contract.

Official Use Only
Official Use Only

19.5 **Unless otherwise specified in the SCC**, the Supplier shall submit to the Purchaser Monthly Progress Reports 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 Purchaser and/or actions to be taken by the Purchaser in the next reporting period;

(vi) status of compliance to environmental and social requirements, as applicable;

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

19.6 The Supplier shall submit to the Purchaser other (periodic) reports as specified in the SCC.

19.7 Immediate Reporting requirement

The Supplier shall inform the Project Manager immediately of any allegation, incident or accident in Project Site/s, which has or is likely to have a significant adverse effect on the environment, the affected communities, the public, Purchaser's Personnel or Supplier's Personnel. This includes, but is not limited to, any incident or accident causing fatality or serious injury; significant adverse effects or damage to private property; any cyber security incidents as **specified in the SCC**; or any allegation of SEA and/or SH. In case of SEA and/or SH, while maintaining confidentiality as appropriate, the type of allegation (sexual exploitation, sexual abuse or sexual harassment), gender and age of the person who experienced the alleged incident should be included in the information.

The Supplier, upon becoming aware of the allegation, incident or accident, shall also immediately inform the Purchaser of any such incident or accident on the

Official Use Only
Official Use Only

Subcontractors' or suppliers' premises relating to the Contract which has or is likely to have a significant adverse effect on the environment, the affected communities, the public, Purchaser's Personnel or Supplier's Personnel. The notification shall provide sufficient detail regarding such incidents or accidents.

The Supplier shall provide full details of such incidents or accidents to the Project Manager within the timeframe agreed with the Purchaser.

The Purchaser shall require its Subcontractors to immediately notify it of any incidents or accidents referred to in this Sub- Clause.

20. Subcontracting

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 Purchaser. 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 Purchaser for its approval in sufficient time so as not to impede the progress of work on the System. Submision by the Supplier, for addition of any Subcontractor not named in the Contract, shall also include the Subcontractor's declaration in accordance with Appendix 2 to the GCC- Sexual exploitation and Abuse (SEA) and/or Sexual Harassment (SH) Performance Declaration. Approval by the Purchaser 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 so listed, or subcontract an item not so listed, it must seek the Purchaser'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 Contract Agreement, the Supplier may employ such Subcontractors as it may select, provided: (i) the Supplier notifies the Purchaser in writing at least twenty-eight (28) days prior to

Official Use Only
Official Use Only

the proposed mobilization date for such Subcontractor, including by providing the Subcontractor's declaration in accordance with Appendix 2 to the GCC- Sexual exploitation and Abuse (SEA) and/or Sexual Harassment (SH) Performance Declaration; and (ii) by the end of this period either the Purchaser has granted its approval in writing or fails to respond. The Supplier shall not engage any Subcontractor to which the Purchaser has objected in writing prior to the end of the notice period. The absence of a written objection by the Purchaser 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 Purchaser of Subcontractors not listed in the Contract Agreement, nothing in this Clause, however, shall limit the rights and obligations of either the Purchaser or Supplier as they are specified in GCC Clauses 20.1 and 20.2, or in Appendix 3 of the Contract Agreement.

20.4 The Supplier shall ensure that its Subcontractors comply with the relevant ES requirements and the obligations set out in GCC Clause 9.9.

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 Contract or, 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 inaccurate information furnished in writing to the Supplier by or on behalf of the Purchaser.

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 Purchaser, by giving a notice of such disclaimer to the Project Manager.

Official Use Only
Official Use Only

21.2 Codes and Standards

Wherever references are made in the Contract to codes and standards in accordance with which the Contract shall 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 proposal submission shall apply. During Contract execution, any changes in such codes and standards shall be applied after approval by the Purchaser and shall be treated in accordance with GCC Clause 39.3.

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

21.3.1 **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 such documents 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 shall be 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 approval, but not to those furnished to the Project Manager for its review only.

21.3.2 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 copy of 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, then the document shall be deemed to have been approved by the Project Manager.

21.3.3 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.

21.3.4 If the Project Manager disapproves the document, the Supplier shall modify the document and resubmit it for

Official Use Only
Official Use Only

the Project Manager's approval in accordance with GCC Clause 21.3.2. If the Project Manager approves the 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 out in GCC Clauses 21.3.2 through 21.3.4 shall be repeated, as appropriate, until the Project Manager approves such documents.

21.3.5 If any dispute occurs between the Purchaser and the Supplier in connection with or arising out of the disapproval by the Project Manager of any document and/or any modification(s) to a document that cannot be settled between the parties within a reasonable period, then, in case the Contract Agreement includes and names an Adjudicator, such dispute may be referred to the Adjudicator for determination in accordance with GCC 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 shall proceed 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 Purchaser has not given notice under GCC Clause 43.1.2, then the Supplier shall be reimbursed by the Purchaser for any additional costs incurred by reason of such instructions and shall be relieved of such responsibility or liability in connection with the dispute and the execution of the instructions as the Adjudicator shall decide, and the Time for Achieving Operational Acceptance shall be extended accordingly.

21.3.6 The Project Manager's approval, with or without modification of the document furnished by the Supplier, shall not 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 or inaccurate information furnished in writing to the Supplier by or on behalf of the Purchaser.

21.3.7 The Supplier shall not depart from any approved document unless the Supplier has first submitted to the Project Manager an amended document and obtained

Official Use Only
Official Use Only

the Project Manager's approval of the document, pursuant to the provisions 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 Purchaser'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 Purchaser, which consent shall not be unreasonably withheld.

22.4 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 Purchaser'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 terms and conditions used in the specification of prices in the Price Schedules, including the terms and conditions of the associated Incoterms.

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.

22.5 **Unless otherwise specified in the SCC,** the Supplier will provide the Purchaser with shipping and other documents, as specified below:

22.5.1 For Goods supplied from outside the Purchaser's Country:

Upon shipment, the Supplier shall notify the Purchaser and the insurance company contracted by the Supplier

Official Use Only
Official Use Only

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 Purchaser 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 total amount;

(b) usual transportation documents;

(c) insurance certificate;

(d) certificate(s) of origin; and

(e) estimated time and point of arrival in the Purchaser's Country and at the site.

22.5.2 For Goods supplied locally (i.e., from within the Purchaser's country):

Upon shipment, the Supplier shall notify the Purchaser by cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Purchaser 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.

22.6 Customs Clearance

(a) The Purchaser will bear responsibility for, and cost of, customs clearance into the Purchaser's country in accordance the particular Incoterm(s) used for Goods supplied from outside the Purchaser's country in the Price Schedules referred to by Article 2 of the Contract Agreement.

(b) At the request of the Purchaser, the Supplier will make available a representative or agent during the process of customs clearance in the Purchaser's country for goods supplied from outside the Purchaser's country. In the event of delays in

Official Use Only
Official Use Only

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 Clause 40;

(ii) the Contract Price shall be adjusted to compensate the Supplier for any additional storage charges 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 proposal and still to be delivered, the Supplier shall be obligated to offer to the Purchaser the latest versions of the available Information Technologies having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC Clause 39 (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 Purchaser any cost reductions and additional and/or improved support and facilities that it offers to other clients of the Supplier in the Purchaser's Country, pursuant to GCC Clause 39 (Changes to the System).

23.3 During performance of the Contract, the Supplier shall offer to the Purchaser 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 the Purchaser's Country, 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 its proposal.

23.4 **Unless otherwise specified in the SCC,** during the Warranty Period, the Supplier will provide at no additional cost to the Purchaser all new versions, releases, and updates for all Standard Software that are used in the System, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in the Purchaser's country, and

Official Use Only
Official Use Only

no later than twelve (12) months after they are released in the country of origin of the Software.

23.5 The Purchaser 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 continue to 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 Purchaser receives a production-ready copy of a subsequent version, release, or update. The Purchaser shall use all reasonable endeavors to implement any new version, release, or update as soon as practicable, subject to the 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 with the 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 advance by the parties (including, but not restricted to, any prices submitted by the Supplier in the Recurrent Cost Schedules of its proposal) and shall not exceed the prevailing rates charged by the Supplier to other purchasers in the Purchaser's Country for similar services.

25. Inspections and Tests

25.1 The Purchaser 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 conformity to the Contract at the point of delivery and/or at the Project Site.

25.2 The Purchaser or its representative shall be entitled to attend any such inspections and/or tests of the components, provided that the Purchaser shall bear all costs and expenses incurred in connection with such attendance, including but not limited to all inspection agent fees, travel, and related expenses.

Official Use Only
Official Use Only

25.3 Should the inspected or tested components fail to conform to the Contract, the Purchaser 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 Purchaser.

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 the other 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 parties within 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.

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 with the Technical Requirements, the SCC and the Agreed Project Plan, the Supplier shall so notify the Purchaser in writing.

26.2 The Project Manager shall, within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 26.1, either issue an Installation Certificate in the form specified in the Sample Contractual Forms Section in the request for proposals document, stating that the System, or major component or Subsystem (if Acceptance by major component or Subsystem is specified pursuant to the SCC for GCC Clause 27.2.1), has achieved Installation by 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

Official Use Only
Official Use Only

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 carry out retesting of the System or Subsystem and, when in the Supplier's opinion the System or Subsystem is ready for Commissioning and Operational Acceptance Testing, notify the Purchaser in writing, in accordance with GCC Clause 26.1. The procedure set out in this GCC Clause 26.2 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 defects and/or deficiencies within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 26.1, or if the Purchaser puts the System or a Subsystem into 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 Purchaser put the System into production operation, as the case may be.

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) shall be 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 Purchaser 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

Official Use Only
Official Use Only

Purchaser (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 meets the standard of performance quoted in the Supplier's proposal, including, but not restricted to, the functional and technical 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 Purchaser's discretion, Operational Acceptance Tests may also be performed on replacement Goods, upgrades and new version releases, and Goods that are added or field-modified after Operational Acceptance of the System.

27.2.2 If for reasons attributable to the Purchaser, 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 by the Purchaser and the Supplier, the Supplier shall be deemed to have fulfilled its obligations with respect to 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 the System, 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 Purchaser within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause 27.2.2 above; or

Official Use Only
Official Use Only

(c) the Purchaser 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 Purchaser 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 a notice to the Project Manager requesting the issue of an Operational Acceptance Certificate.

27.3.3 After consultation with the Purchaser, 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 other reasons 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 Purchaser, and the Purchaser, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Supplier shall notify the Purchaser of its request for Operational Acceptance Certification, in accordance with GCC Clause 27.3.3. The Purchaser 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 out in this GCC Clause 27.3.4 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, then either:

Official Use Only
Official Use Only

(a) the Purchaser may consider terminating the Contract, pursuant to GCC Clause 41.2.2;

or

(b) if the failure to achieve Operational Acceptance within the specified time period is a result of the failure of the Purchaser 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.

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 pursuant to 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

Official Use Only
Official Use Only

shall issue an Operational Acceptance Certificate within fourteen (14) days after the fittings and/or furnishings have been 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 Purchaser 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 Purchaser 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 of ten (10) percent of the Contract Price (exclusive of Recurrent Costs if any). Once the Maximum is reached, the Purchaser may consider termination of the Contract, pursuant to GCC Clause 41.2.2.

28.3 **Unless otherwise specified in the SCC,** liquidated damages payable under GCC Clause 28.2 shall apply only to 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

Official Use Only
Official Use Only

remedies the Purchaser may have under the Contract for other delays.

28.4 If liquidated damages are claimed by the Purchaser for the System (or Subsystem), the Supplier shall have no further liability whatsoever to the Purchaser 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 and liabilities under the Contract.

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 Requirements or 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 with respect 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 the Contract are new, unused, and incorporate all recent improvements in design that materially affect the System's or 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 Operational Acceptance 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,

Official Use Only
Official Use Only

engineering, Materials, and workmanship of the Information Technologies and other Goods supplied or of the Services provided by the Supplier, the Supplier shall promptly, in consultation and agreement with the Purchaser 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 to the 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 any damage to the System arising out of or resulting from any of the following causes:

(a) improper operation or maintenance of the System by the Purchaser;

(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 Purchaser, 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

(b) any designs, specifications, or other data designed, supplied, or specified by or on behalf of the Purchaser or any matters for which the Supplier has disclaimed responsibility, in accordance with GCC Clause 21.1.2.

29.8 The Purchaser shall give the Supplier a notice promptly following the discovery of such defect, stating the nature of any such defect together with all available evidence. The Purchaser shall afford all reasonable opportunity for the Supplier to inspect any such defect. The Purchaser 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.

Official Use Only
Official Use Only

29.9 The Supplier may, with the consent of the Purchaser, 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 System caused 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 Purchaser may give the Supplier notice requiring that tests of the defective part be made by the Supplier immediately upon completion of such remedial work, whereupon the Supplier shall carry out such tests.

If such part fails the tests, the Supplier shall carry out further repair, replacement, or making good (as the case may be) until that part of the System passes such tests. The tests shall be agreed upon by the Purchaser 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 Purchaser 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 Purchaser in connection with such work shall be paid to the Purchaser by the Supplier or may be deducted by the Purchaser 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, the Warranty 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 Purchaser because of such defect and/or making good of such defect.

29.12 Items substituted for defective parts of the System during the Warranty Period shall be covered by the Defect Liability 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 Purchaser may choose to retain physical possession of any replaced defective information storage devices.

29.13 At the request of the Purchaser and without prejudice to any other rights and remedies that the Purchaser may have

Official Use Only
Official Use Only

against the Supplier under the Contract, the Supplier will offer all possible assistance to the Purchaser 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 Purchaser of the benefit of any warranties given by such producers or licensors to 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 Purchaser'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 governs how technical conformance of the System 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 Purchaser upon completion of the necessary changes, modifications, and/or additions and shall request the Purchaser to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance.

30.3 If the System (or Subsystem[s]) fails to achieve Operational Acceptance, the Purchaser 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 result from this failure.

31. Intellectual Property Rights Warranty

31.1 The Supplier hereby represents and warrants that:

(a) the System as supplied, installed, tested, and accepted;

(b) use of the System in accordance with the Contract; and

Official Use Only
Official Use Only

(c) copying of the Software and Materials provided to the Purchaser in accordance with the Contract

do not and will not infringe any Intellectual Property Rights held by any third party and that it has all necessary rights or at its sole expense shall have secured in writing all transfers of rights 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 Purchaser 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 Purchaser 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 Purchaser 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 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 Purchaser'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 thereby in association or combination with any other goods or 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.

Official Use Only
Official Use Only

32.3 Such indemnities shall also not apply if any claim of infringement:

(a) is asserted by a parent, subsidiary, or affiliate of the Purchaser's organization;

(b) is a direct result of a design mandated by the Purchaser's Technical Requirements and the possibility of such infringement was duly noted in the Supplier's Proposal; or

(c) results from the alteration of the System, including the Materials, by the Purchaser or any persons 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 Purchaser arising out of the matters referred to in GCC Clause 32.1, the Purchaser shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Purchaser'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 Purchaser within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify the Purchaser within the twenty-eight (28) days, the Purchaser shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Purchaser 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 reasonable expenses incurred in so doing.

32.5 The Purchaser 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 costs incurred 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 Property Rights 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 Purchaser or any persons (other than the Supplier) contracted by the

Official Use Only
Official Use Only

Purchaser, except to the extent that such losses, liabilities, and costs arise as a result of the Supplier's breach of GCC Clause 32.8.

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 Purchaser or any other person contracted by the Purchaser, 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 a parent, 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 Purchaser or any persons contracted by the Purchaser.

32.8 If any proceedings are brought or any claim is made against the Supplier arising out of the matters referred to in GCC Clause 32.5, the Supplier shall promptly give the Purchaser notice of such proceedings or claims, and the Purchaser 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 Purchaser 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 Purchaser 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 Purchaser's request, afford all available assistance to the Purchaser in

Official Use Only
Official Use Only

conducting such proceedings or claim and shall be reimbursed by the Purchaser 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 Purchaser, 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 Purchaser; and

(b) the aggregate liability of the Supplier to the Purchaser, 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 Purchaser 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 Goods shall be transferred to the Purchaser at the time of Delivery or otherwise under terms that may be agreed upon 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) Clause 16 (Software License Agreements), and any elaboration in the Technical Requirements.

34.3 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.

35. Care of the System

35.1 The Purchaser shall become responsible for the care and custody of the System or Subsystems upon their Delivery. The Purchaser shall make good at its own cost any loss or damage that may occur to the System or Subsystems from

Official Use Only
Official Use Only

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), excepting such 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) (insofar 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 Supplier could not reasonably foresee, or if reasonably foreseeable could not reasonably make provision for or insure against, insofar 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 Purchaser 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 Purchaser, or any such matter for which the Supplier has disclaimed responsibility in accordance with GCC Clause 21.1.2,

the Purchaser 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 Purchaser 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 Purchaser in accordance with GCC Clause 39. If the Purchaser does not request the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Purchaser shall either request a change in accordance with GCC Clause 39, excluding the performance of that part of the System thereby lost, destroyed, or damaged, or, where the loss or damage affects a substantial part of the System, the Purchaser shall terminate the Contract pursuant to GCC Clause 41.1.

35.3 The Purchaser shall be liable for any loss of or damage to any Supplier's Equipment which the Purchaser has

Official Use Only
Official Use Only

authorized to locate within the Purchaser'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 the Purchaser's Country.

36.2 Subject to GCC Clause 36.3, the Supplier shall indemnify and hold harmless the Purchaser 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 Purchaser or its employees or officers may suffer as a result of the death or injury of any person or loss of or damage to any property (other than 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 Purchaser, its contractors, employees, officers, or agents.

36.3 If any proceedings are brought or any claim is made against the Purchaser that might subject the Supplier to liability under GCC Clause 36.2, the Purchaser shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in the Purchaser'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 Purchaser within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify the Purchaser within the twenty-eight (28) day period, the Purchaser shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Purchaser 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 reasonable expenses incurred in so doing.

36.4 The Purchaser shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from any and all losses, liabilities, and costs (including

Official Use Only
Official Use Only

losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of the death or personal injury of any person or loss of or damage to property of the Purchaser, 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.

36.5 If any proceedings are brought or any claim is made against the Supplier that might subject the Purchaser to liability under GCC Clause 36.4, the Supplier shall promptly give the Purchaser notice of such proceedings or claims, and the Purchaser 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 Purchaser 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 Purchaser 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 Purchaser's request, afford all available assistance to the Purchaser in conducting such proceedings or claim and shall be reimbursed by the Purchaser for all reasonable expenses incurred in so doing.

36.6 The party entitled to the benefit of an indemnity under this GCC Clause 36 shall take all reasonable measures to 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 Purchaser, who should not unreasonably withhold such approval.

(a) Cargo Insurance During Transport

Official Use Only
Official Use Only

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 Purchaser's personnel) and loss of or damage to property (including the Purchaser's property and any Subsystems that have been accepted by the Purchaser) occurring in connection with the supply and installation of the Information System.

(d) Automobile Liability Insurance

In accordance with the statutory requirements prevailing in the Purchaser's Country, 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.

(e) Other Insurance (if any), as **specified in the SCC.**

37.2 The Purchaser 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 be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause 37.1 except for Cargo Insurance During Transport. All insurer's rights of subrogation against such co-insured for losses or claims arising out of the performance of the Contract shall be waived under such policies.

37.3 The Supplier shall deliver to the Purchaser certificates of insurance (or copies of the insurance policies) as evidence that the required policies are in full force and effect.

Official Use Only
Official Use Only

37.4 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.

37.5 If the Supplier fails to take out and/or maintain in effect the insurance referred to in GCC Clause 37.1, the Purchaser may take out and maintain in effect any such insurance and may from time to time deduct from any amount due the Supplier under the Contract any premium that the Purchaser shall have paid to the insurer or may otherwise recover such amount as a debt due from the Supplier.

37.6 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 shall be paid to the Supplier. The Purchaser 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 Purchaser's interest is involved, the Supplier shall not give any release or make any compromise with the insurer without the prior written consent of the Purchaser. With respect to insurance claims in which the Supplier's interest is involved, the Purchaser shall not give any release 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 Purchaser 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 warlike 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 de jure or de facto authority or

Official Use Only
Official Use Only

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 Contract by 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 Achieving Operational 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.

Official Use Only
Official Use Only

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 nonperformance 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 more than sixty (60) days or an aggregate period of more than one hundred and twenty (120) days on account of one or 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 Purchaser 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 Purchaser to make 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 Purchaser 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.

A Change may involve, but is not restricted to, the substitution of updated Information Technologies and

Official Use Only
Official Use Only

related Services in accordance with GCC Clause 23 (Product Upgrades).

39.1.2 The Supplier may from time to time during its performance of the Contract propose to the Purchaser (with a copy to the Project Manager) any Change that the Supplier considers necessary or desirable to improve the quality or efficiency of the System. The Purchaser may at its discretion approve or reject any Change proposed by the Supplier.

39.1.3 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.

39.1.4 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 request for proposals document.

39.1.5 Moreover, the Purchaser and Supplier will agree, during development of the Project Plan, to a date prior to the scheduled date for Operational Acceptance, after which the Technical Requirements for the System shall be "frozen." Any Change initiated after this time will be dealt with after Operational Acceptance.

39.2 Changes Originating from Purchaser

39.2.1 If the Purchaser 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; and

Official Use Only
Official Use Only

(f) any additional documents as **specified in the SCC**.

39.2.2 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 Purchaser shall do one of the following:

(a) accept the Supplier's estimate with instructions to the Supplier to proceed with the preparation of the Change Proposal;

(b) advise the Supplier of any part of its Change Estimate Proposal that is unacceptable and request the Supplier to review its estimate;

(c) advise the Supplier that the Purchaser does not intend to proceed with the Change.

39.2.3 Upon receipt of the Purchaser'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 Purchaser and Supplier has not reached agreement in accordance with GCC Clause 39.2.6, then GCC Clause 39.2.7 shall apply.

39.2.4 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 inequitable, the parties to the Contract shall agree on other specific rates to be used for valuing the Change.

39.2.5 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 become binding 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 the Change Proposal. If

Official Use Only
Official Use Only

the Purchaser accepts the Supplier's objection, the Purchaser shall withdraw the proposed Change and shall notify the Supplier in writing of its 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.

39.2.6 Upon receipt of the Change Proposal, the Purchaser and the Supplier shall mutually agree upon all matters contained in the Change Proposal. Within fourteen (14) days after such agreement, the Purchaser shall, if it intends to proceed with the Change, issue the Supplier a Change Order. If the Purchaser is 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 Purchaser 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 its Change Estimate Proposal submitted in accordance with GCC Clause 39.2.2.

39.2.7 If the Purchaser 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 party under 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 including the 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

Official Use Only
Official Use Only

39.2.7. However, should the Purchaser choose not to proceed or the Purchaser 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 Purchaser 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 during the performance of the Contract. 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 Purchaser may incur in implementing the value engineering proposal; and

(c) a description of any effect(s) of the change on performance/functionality.

The Purchaser 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 Purchaser; or

(c) improves the quality, efficiency, safety or sustainability of the systems; or

(d) yields any other benefits to the Purchaser,

without compromising the necessary functions of the systems.

If the value engineering proposal is approved by the Purchaser and results in:

(a) a reduction of the Contract Price; the amount to be paid to the Supplier shall be the percentage specified 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.

Official Use Only
Official Use Only

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 Clause 39 (Change in the Information System);

(b) any occurrence of Force Majeure as provided in GCC Clause 38 (Force Majeure);

(c) default of the Purchaser; 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 Manager a notice of a claim for an extension of the time for achieving Operational Acceptance, together with particulars of 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 Purchaser and the Supplier shall agree upon the period of such extension. In the event that the Supplier does not accept the Purchaser's estimate of a fair and reasonable time extension, the Supplier shall be entitled to refer the matter to the provisions for the Settlement of 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 Purchaser's Convenience

41.1.1 The Purchaser may at any time terminate the Contract for any reason by giving the Supplier a notice of 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

Official Use Only
Official Use Only

(a) cease all further work, except for such work as the Purchaser 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 Purchaser pursuant to GCC Clause 41.1.2 (d) (ii) below;

(c) remove all Supplier's Equipment from the site, repatriate the Supplier's 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 Purchaser the parts of the System executed by the Supplier up to the date of termination;

(ii) to the extent legally possible, assign to the Purchaser all right, title, and benefit of the Supplier to the System, or Subsystem, as at the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(iii) deliver to the Purchaser 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 Purchaser shall pay to the Supplier 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 Personnel;

(c) any amount to be paid by the Supplier to its Subcontractors in connection with the

Official Use Only
Official Use Only

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 Purchaser, 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 therefore to the Supplier, referring to this GCC Clause 41.2:

(a) if the Supplier becomes bankrupt or insolvent, 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 Contract or any right or interest therein in violation of the provision of GCC Clause 42 (Assignment); or

(c) if the Supplier, in the judgment of the Purchaser has engaged in Fraud and Corruption, as defined in paragraph 2.2 a. of the Appendix 1 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:

(a) has abandoned or repudiated the Contract;

Official Use Only
Official Use Only

(b) has without valid reason failed to commence work on the System promptly;

(c) 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;

(d) 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 Purchaser that the Supplier can attain Operational Acceptance of the System by the Time for Achieving Operational Acceptance as extended;

then the Purchaser 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 thirty (30) days of its receipt of such notice, then the Purchaser 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:

(a) cease all further work, except for such work as the Purchaser 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 Purchaser pursuant to GCC Clause 41.2.3 (d) below;

(c) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(d) to the extent legally possible, assign to the Purchaser all right, title and benefit of the Supplier to the System or Subsystems as at the

Official Use Only
Official Use Only

date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(e) deliver to the Purchaser 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 Purchaser 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 Purchaser thinks appropriate, the Purchaser 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 due the Purchaser 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 Purchaser completes the System, the cost of completing the System by the Purchaser shall be 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 Purchaser 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 Clause 41.2.5, the Supplier shall pay the balance to the Purchaser, and if such excess is less than the sums due the Supplier under GCC Clause 41.2.5, the Purchaser shall pay the balance to the Supplier. The Purchaser 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

Official Use Only
Official Use Only

41.3.1 If:

(a) the Purchaser 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 Purchaser 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 Purchaser to remedy the same, as the case may be. If the Purchaser 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 Purchaser, including but not limited to the Purchaser'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 Purchaser of such events, and if the Purchaser 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 obligations under the Contract for any reason attributable to the Purchaser within twenty-eight (28) days of the said notice, the Supplier may by a further notice to the Purchaser referring to this GCC Clause 41.3.1, forthwith terminate the Contract.

41.3.2 The Supplier may terminate the Contract immediately by giving a notice to the Purchaser to that effect, referring to this GCC Clause 41.3.2, if the Purchaser becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or,

Official Use Only
Official Use Only

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 Purchaser 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 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 Purchaser pursuant to Clause 41.3.3 (d) (ii);

(c) remove all Supplier's Equipment from the site and repatriate the Supplier's Personnel from the site.

(d) In addition, the Supplier, subject to the payment specified in GCC Clause 41.3.4, shall:

(i) deliver to the Purchaser the parts of the System executed by the Supplier up to the date of termination;

(ii) to the extent legally possible, assign to the Purchaser all right, title, and benefit of the Supplier to the System, or Subsystems, as of the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the Supplier and its Subcontractors;

(iii) to the extent legally possible, deliver to the Purchaser 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 41.3.1 or 41.3.2, the Purchaser shall pay to the Supplier all payments specified in GCC Clause 41.1.3 and reasonable compensation for all loss, except for

Official Use Only
Official Use Only

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 Clause 41.3.

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 Purchaser to the Supplier, account shall be taken of any sum previously paid by the Purchaser to the Supplier under the Contract, including any advance payment paid **pursuant to the SCC.**

42. Assignment

42.1 Neither the Purchaser nor the Supplier shall, without the express prior written consent of the other, assign to any third party the Contract or any part thereof, or any right, benefit, obligation, or interest therein or thereunder, 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

43. Settlement of Disputes

43.1 Adjudication

43.1.1 If any dispute of any kind whatsoever shall arise between the Purchaser and the Supplier in connection with 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

Official Use Only
Official Use Only

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 Appendix 2 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 Clause 43.2.1.

43.1.2 The Adjudicator shall give his or her decision in writing to both parties within twenty-eight (28) days of the dispute 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 Purchaser or the Supplier within fifty-six (56) days of such reference, the decision shall become final and binding upon the Purchaser and the Supplier. Any decision that has become final and binding shall be implemented by the parties forthwith.

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 Purchaser and the Supplier.

43.1.4 Should the Adjudicator resign or die, or should the Purchaser 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 Purchaser 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

Official Use Only
Official Use Only

43.2.1 If

(a) the Purchaser 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 Purchaser 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 Purchaser or the Supplier acts within the following fourteen (14) days,

then either the Purchaser or the Supplier may act to give notice to the other party, with a copy for information to the Adjudicator in case 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 Purchaser shall pay the Supplier any monies due the Supplier.

Official Use Only
Official Use Only

J. CYBER SECURITY

44. Cyber Security

44.1 **Pursuant to the SCC**, the Supplier, including its Subcontractors/ suppliers/ manufacturers shall take all technical and organizational measures necessary to protect the information technology systems and data used in connection with the Contract. Without limiting the foregoing, the Supplier, including its Subcontractors/ suppliers/ manufacturers, shall use all reasonable efforts to establish, maintain, implement and comply with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or data used in connection with the Contract.

Official Use Only
Official Use Only

APPENDIX 1

Fraud and Corruption

(Text in this Appendix shall not be modified)

1. Purpose

1.1 The Bank's Anti-Corruption Guidelines and this annex apply with respect to procurement under Bank Investment Project Financing operations.

2. Requirements

2.1 The Bank requires that Borrowers (including beneficiaries of Bank financing); bidders (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, observe the highest standard of ethics during the procurement process, selection and contract execution of Bank-financed contracts, and refrain from Fraud and Corruption.

2.2 To this end, the Bank:

a. Defines, for the purposes of this provision, the terms set forth below as follows:

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:

(a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation 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

(b) acts intended to materially impede the exercise of the Bank's inspection and audit rights provided for under paragraph 2.2 e. below.

Official Use Only
Official Use Only

b. Rejects a proposal for award if the Bank 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;

c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring misprocurement, if the Bank determines at any time that representatives of the Borrower or of a recipient of any part of the proceeds of the loan engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the Borrower having taken timely and appropriate action satisfactory to the Bank to address such practices when they occur, including by failing to inform the Bank in a timely manner at the time they knew of the practices;

d. Pursuant to the Bank's Anti-Corruption Guidelines, and in accordance with the Bank's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a Bank-financed contract, financially or in any other manner;[1] (ii) to be a nominated[2] sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a Bank-financed contract; and (iii) to receive the proceeds of any loan made by the Bank or otherwise to participate further in the preparation or implementation of any Bank-financed project;

e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by a Bank loan, requiring (i) bidders (applicants/proposers), consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents, personnel, permit the Bank to inspect[3] 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 Bank.

---

1 For the avoidance of doubt, a sanctioned party's ineligibility to be awarded a contract shall include, without limitation, (i) applying for pre-qualification, expressing interest in a consultancy, and bidding, 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 A nominated sub-contractor, nominated consultant, nominated manufacturer or supplier, or nominated service provider (different names are used depending on the particular bidding document) is one which has been: (i) included by the bidder in its pre-qualification application or bid because it brings specific and critical experience and know-how that allow the bidder to meet the qualification requirements for the particular bid; or (ii) appointed by the Borrower.

3 Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the Bank or persons appointed by the Bank 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 thereof 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 thereof as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

Official Use Only
Official Use Only

Official Use Only
Official Use Only

APPENDIX 2

Sexual Exploitation and Abuse (SEA) and/or Sexual Harassment (SH) Performance Declaration for Subcontractors

[The following table shall be filled in by each subcontractor proposed by the Supplier, that was not named in the Contract]

Subcontractor's Name: *[insert full name]*

Date: *[insert day, month, year]*
Contract reference *[insert contract reference]*
Page *[insert page number]* of *[insert total number]* pages

SEA and/or SH Declaration
We: ☐ (a) have not been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations. ☐ (b) are subject to disqualification by the Bank for non-compliance with SEA/ SH obligations. ☐ (c) had been subject to disqualification by the Bank for non-compliance with SEA/ SH obligations, and were removed from the disqualification list. An arbitral award on the disqualification case has been made in our favor.
[If (c) above is applicable, attach evidence of an arbitral award reversing the findings on the issues underlying the disqualification.]
Period of disqualification: From: _____ To: _____

Name of the Subcontractor_____

Name of the person duly authorized to sign on behalf of the Subcontractor_____

Title of the person signing on behalf of the Subcontractor_____

Signature of the person named above_____

Date signed _____ day of _____, _____

Countersignature of authorized representative of the Supplier:

Signature: _____

Date signed _____ day of _____, _____

Official Use Only
Official Use Only

SECTION IX - SPECIAL CONDITIONS OF CONTRACT

Table of Clauses

A. Contract and Interpretation 359

Definitions (GCC Clause 1).....359
Notices (GCC Clause 4).....359

B. Subject Matter of Contract 359

Scope of the System (GCC Clause 7).....359
Time for Commencement and Operational Acceptance (GCC Clause 8) 361
Supplier's Responsibilities (GCC Clause 9).....361

C. Payment.....361

Contract Price (GCC Clause 11).....361
Terms of Payment (GCC Clause 12) 361
Securities (GCC Clause 13).....364

D. Intellectual Property 364

Copyright (GCC Clause 15).....364
Software License Agreements (GCC Clause 16).....365
Confidential Information (GCC Clause 17).....365

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System 365

Representatives (GCC Clause 18) 365
Project Plan (GCC Clause 19) 365
Design and Engineering (GCC Clause 21) 368
Product Upgrades (GCC Clause 23).....368
Inspections and Tests (GCC Clause 25) 369
Commissioning and Operational Acceptance (GCC Clause 27) 369

F. Guarantees and Liabilities.....370

Operational Acceptance Time Guarantee (GCC Clause 28) 370
Defect Liability (GCC Clause 29) 371
Functional Guarantees (GCC Clause 30).....372

G. Risk Distribution.....373

Insurances (GCC Clause 37).....373

H. Change in Contract Elements.....374

Changes to the System (GCC Clause 39) 374

I. Settlement of Disputes.....374

Settlement of Disputes (GCC Clause 43) 374

J. Cyber Security.....375

Official Use Only
Official Use Only

Cyber Security (GCC Clause 44).....375

Official Use Only
Official Use Only

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 of Contract. For the purposes of clarity, any referenced GCC clause numbers are indicated in the left column of the SCC.

A. CONTRACT AND INTERPRETATION

Definitions (GCC Clause 1)

GCC 1.1 (a) (ix)	The applicable edition of the Procurement Regulation is dated: **Revised Fifth Edition, September 2023**
GCC 1.1 (b) (i)	The Purchaser is: **The Information and Communications Technology Authority**
GCC 1.1 (b) (ii)	The Project Manager : will be named by the Employer and communicated to the successful Bidder prior to Contract Signing.
GCC 1.1 (e) (i)	The Purchaser's Country is: **Kenya**
GCC 1.1 (e) (x)	**There are no Special Conditions associated with GCC 1.1 (e) (x).**
GCC 1.1 (e) (xiii)	The Post-Warranty Services Period is 24 months starting with the completion of the 36-month Warranty Period, to align with five year support and licensing requirement and overall contract duration

Notices (GCC Clause 4)

GCC 4.3	Address of the Project Manager: *will be communicated by the Employer to the successful Bidder prior to Contract Signing* Fallback address of the Purchaser: **ICT Authority, 12th Floor, Telposta Towers, P.O. Box 27150 – 00100, Nairobi, Kenya**

B. SUBJECT MATTER OF CONTRACT

Scope of the System (GCC Clause 7)

GCC 7.3	The recurrent-cost items under this Contract are limited to the licences, subscriptions, renewals, maintenance, operational support and resident support expressly listed in Section VII and the Price Schedules. Each item shall state its quantity, coverage period, service obligation and payment

Official Use Only
Official Use Only

	basis. The thirty-six (36) month warranty is included in the Contract Price and shall not be charged as a separate recurrent cost. No recurrent cost not identified in the Price Schedules shall be payable unless introduced by a contract amendment in accordance with the Contract *[specify: **the recurrent cost items/services that are included in the Contract; also provide cross reference to the place in the Technical Requirements where each item/service is specified in detail.**]* ***[Note**: The requirements in terms of recurrent cost items should be defined here, reflected in the Recurrent Cost Table for the Warranty period, and elaborated in the Technical Requirements. See also notes to SCC Clause 29.4 regarding services that are not typically included in commercial warranties.* *If the Purchaser expects that wear and tear on System components will necessitate routine replacement of such components, and if Purchaser technical staff will perform these repair and replacement tasks, the Purchaser may wish to consider adding the following clause to the SCC that obligates the Supplier to stock and/or provide certain spare parts.]* The Supplier agrees to supply spare parts required for the operation and maintenance of the System, as stated below, for *[insert: **number of years**]* years beginning with Operational Acceptance. Moreover, the price of such spare parts shall be those specified in the spare parts price schedule submitted by the Suppler as part of its Proposal. These prices shall include the purchase price for such spare parts and other costs and expenses (including the Supplier's fees) relating to the supply of spare parts. *[list **the spare parts needs,** or reference **the line items in the Spare Parts Price Schedule in the Supplier's Proposal**, if the Supplier is the source of the identity of the spares, i.e., reflecting its own understanding of its own technologies.]* **[*Note:** The need to ensure the availability of spare parts sources, above and beyond those the Supplier would routinely and implicitly need to perform under its defect liability and/or maintenance responsibilities, generally is not a major issue for the Information Technologies available in the market today. A System is likely to become obsolete long before it begins to develop physical defects.]*

Official Use Only
Official Use Only

Time for Commencement and Operational Acceptance (GCC Clause 8)

GCC 8.1	The Supplier shall commence work on the System within: **14** days from the Effective Date of the Contract.

Supplier's Responsibilities (GCC Clause 9)

GCC 9.1	"health and safety manual is required"
GCC 9.8	The following sustainable procurement contractual provisions, apply: **None**
GCC 9.18	The Supplier **is required** to make security arrangements for the Project Site/s.

C. PAYMENT

Contract Price (GCC Clause 11)

GCC 11.2	Adjustments to the Contract Price shall be as follows: **Not Applicable**

Terms of Payment (GCC Clause 12)

GCC 12.1	Subject to the provisions of GCC Clause 12 (Terms of Payment), the Purchaser 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 Ten percent (10%) of the entire Contract Price, exclusive of all Recurrent Costs, shall be paid against receipt of a claim accompanied by the Advance Payment Security specified in GCC Clause 13.2.

Official Use Only
Official Use Only

	[Note: (b) 30% on Delivery, Installation, Inspection, verification of conformity of SOC Compute and related Equipment Thirty percent (30%) of the Contract Price shall become payable upon successful delivery, installation and verification of the SOC compute infrastructure and associated equipment specified in the Contract. Payment shall be subject to: i) delivery of the equipment in the quantities and specifications stipulated in the Contract; ii) physical and technical inspection and verification by purchaser; iii) submission of delivery notes, equipment inventory, serial numbers and applicable manufacturer documentation; and iv) confirmation by purchaser that the delivered equipment conforms to the contractual requirements. (c) 20% on Configuration, Integration and system readiness i) completion of the agreed configuration and integration activities; ii) successful completion of the approved functional and integration tests; iii) demonstration that the implemented solution performs in accordance with the approved technical requirements; iv) submission of configuration, integration and test documentation; and v) written approval by the purchaser confirming system readiness for operational onboarding. (d) 15% on Onboarding of Purchaser's CII/Devices and Documentation Fifteen percent (15%) of the Contract Price shall become payable upon successful onboarding and integration of the agreed Purchaser's Critical Information Infrastructure (CII), devices and other approved ICT assets. Payment shall be subject to: a) successful onboarding of the agreed devices, systems and data sources; b) verification that the required security logs, events and telemetry are being received, processed and monitored by the SOC solution; c) completion of agreed onboarding activities; and d) submission and approval of updated system, asset, integration and operational documentation; e)Ten percent (10%) of the Contract Price shall become payable upon successful completion of the agreed training and knowledge-transfer programme. The training shall cover, as applicable SOC operations, administration, monitoring, incident handling, use of the implemented security technologies and relevant Original Equipment Manufacturer (OEM) functionality. Payment shall be subject to:

Official Use Only
Official Use Only

	i) completion of the approved training programme; ii) training of the agreed number and categories of ICTA personnel and any additional nominated personnel; iii) submission of training materials and attendance/completion records; and iv) submission and acceptance of a training completion and knowledge-transfer report by the purchaser. ***[Note:*** *Some Contracts may involve considerable "Services other than Training" (and services other than software customization). For instance, there could be the digitization of maps using the procured Geographical Information System (GIS), or the scanning, indexing and conversion of paper documents, or the conversion or migration of existing electronic data sets. In these cases, payment may be keyed to acceptance of intermediate deliverables or completion of service delivery phases defined in the project implementation schedule, rather than merely to the passage of time, as illustrated. In designing this type of payment terms, the Purchaser has an obligation to balance and ensure consistency between its own interest to pay only against value received, the supplier's need for a reasonable cash flow, the design of the project implementation schedule, the specification of service milestones and even the process for acceptance testing of intermediate deliverables (when milestones completion would be subject to such testing).]* (e) 15% on Operational Acceptance The remaining fifteen percent (15%) of the Contract Price shall become payable upon Operational Acceptance of the SOC solution. Operational Acceptance shall be subject to: i) successful completion of all contractual deliverables and acceptance tests; ii) successful commissioning of the SOC solution; iii) resolution of all Critical and High-priority defects and non-conformities, or agreement with the purchaser on an acceptable corrective action plan for any outstanding items; iv) submission and approval of the final technical, operational, configuration, as-built and other contractual documentation; e) completion of all agreed training and knowledge-transfer obligations; and v) issuance of a Operational Acceptance Certificate by the purchaser.
GCC 12.3	The Purchaser shall pay to the Supplier interest on the delayed payments at a rate of: **prevailing Central Bank of Kenya (CBK) base rate plus 3% per annum.**

Official Use Only
Official Use Only

GCC 12.4	The Supplier will invoice the Purchaser in the currency used in the Contract Agreement and the Price Schedules it refers to, for Goods and Services supplied locally, and the conversion between this currency and **Kenya Shillings** for payment purposes - in case the two currencies are different - will be made as of the actual payment date using the exchange rate found in **Central Bank of Kenya**
GCC 12.6	**There are no Special Conditions of Contract applicable to GCC Clause 12.6**

Securities (GCC Clause 13)

GCC 13.3.1	The Performance Security shall be denominated in **Kenya Shillings or equivalent in any freely convertible currency** for an amount equal to **8** percent of the Contract Price, excluding any Recurrent Costs.
GCC 13.3.2	The Performance Security shall be in the form of an **Unconditional Bank Guarantee** issued by a commercial bank licensed and operating in Kenya or a foreign bank counter-guaranteed by a reputable bank in Kenya using the Performance Security Form contained in **Section X - Contract Forms**
GCC 13.3.4	During the Warranty Period (i.e., after Operational Acceptance of the System), the Performance Security shall be reduced to **2.5** percent of the Contract Price, excluding any Recurrent Costs.

D. INTELLECTUAL PROPERTY

Copyright (GCC Clause 15)

GCC 15.3	**There are no Special Conditions of Contract applicable to GCC Clause 15.3**
GCC 15.4	**There are no Special Conditions of Contract applicable to GCC Clause 15.4**
GCC 15.5	**There are no Special Conditions of Contract applicable to GCC Clause 15.5**

Official Use Only
Official Use Only

Software License Agreements (GCC Clause 16)

GCC 16.1 (a) (iv)	**There are no Special Conditions of Contract applicable to GCC Clause 16.1 (a) (iv)**
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 16.2	**There are no Special Conditions of Contract applicable to GCC Clause 16.2**

Confidential Information (GCC Clause 17)

GCC 17.1	**There are no Special Conditions of Contract applicable to GCC Clause 17.1**

E. SUPPLY, INSTALLATION, TESTING, COMMISSIONING, AND ACCEPTANCE OF THE SYSTEM – NOT APPLICABLE

Representatives (GCC Clause 18)

GCC 18.1	***There are no Special Conditions of Contract applicable to GCC Clause 18***
GCC 18.2.2	***There are no Special Conditions of Contract applicable to GCC Clause 18.2.2***

Project Plan (GCC Clause 19)

GCC 19.1	Chapters in the Project Plan shall address the following subject**:** ***(a) Project Organization and Management Plan, including quality assurance, configuration management, problem escalation and resolution, etc.*** ***(b) Systems Development Methodology Plan***

Official Use Only
Official Use Only

	(c) Delivery and Installation Plan ***(d) Integration and Data Migration Plan*** ***(e) Training Plan*** ***(f) Documentation Plan*** ***(g) Verification, Validation and Testing Plan*** ***(h) Technical Support Plan, including Warranty Services*** ***(i) Task, Time, and Resource Schedules;*** Further details regarding the required contents of each of the above chapters are contained in the Technical Requirements,
GCC 19.6	***The Supplier shall submit to the Purchaser:*** ***(i) monthly inspection and quality assurance reports*** ***(ii) monthly training participants test results*** (iii) ***monthly log of service calls and problem resolutions*** (iv) *" Monthly report on status of compliance to cyber security risks management, and any foreseeable cyber security risk and mitigation".]*
GCC 19.7	*[As appropriate, specify cyber security incidents to be immediately reported; if not applicable, state: "There are no Special Conditions of Contract applicable to GCC Clause 19.7".]* The Supplier shall notify ICTA of a cybersecurity incident affecting the GovSOC Information System within fifteen (15) minutes of discovery for a Critical incident, within thirty (30) minutes for a High incident, within four (4) hours for Medium incident and one(1) business day for a Low incident. Notification shall be made through the designated ICTA incident-reporting channel and shall include, to the extent known, the time detected, affected systems, severity, indicators, containment actions and support required. The Supplier shall preserve relevant logs and evidence, cooperate with ICTA and competent authorities as directed, provide regular updates for Critical and High incidents, and submit a root-cause and corrective-action report within five (5) business days after containment Cybersecurity incidents requiring immediate notification shall include, but shall not be limited to: - Secure configuration and hardening: Any unauthorized or material change to security configurations, hardening controls, access-

Official Use Only
Official Use Only

	control policies, or security baselines, or any discovery of a configuration that materially weakens the security of the solution. - Identity and privileged-access management: Any compromise, unauthorized use, suspected misuse, or unauthorized escalation of administrative, privileged, service, or user accounts. - Encryption and authentication standards: Any compromise, bypass, unauthorized disabling, misconfiguration, or material weakness affecting encryption, certificates, keys, authentication or authorization mechanisms. - Firmware and vulnerability management: Discovery or exploitation of a critical/high-risk vulnerability, malicious firmware, unauthorized firmware modification, or evidence that firmware or software has been compromised. - Security updates during warranty and support: Any failure to apply, delay in applying, or inability to provide a required security update or critical vulnerability remediation within the agreed SLA. - Logging and incident notification: Any unauthorized alteration, deletion, suppression, disabling or loss of security logs, monitoring functions, audit trails, or security alerts, including any failure of mechanisms required to detect or report security incidents. - Protection of management-plane traffic: Any interception, unauthorized access, manipulation, redirection, exposure or compromise of management-plane traffic or management interfaces. - Cloud-service and data-location requirements, where applicable: Any unauthorized access to, disclosure, transfer, processing, storage or relocation of GovSOC-related data outside the approved cloud service, jurisdiction or agreed data-location requirements. - Handover of credentials and configurations: Any loss, unauthorized disclosure, compromise or unauthorized retention of credentials, encryption keys, configurations, network diagrams, system documentation or other security-sensitive information required to be handed over to the Purchaser. - Removal of default passwords and undocumented remote access: Any discovery of default or weak credentials, hidden accounts, undocumented remote-access mechanisms, backdoors,

Official Use Only
Official Use Only

	unauthorized support accounts or other undocumented means of accessing the WLAN solution. The Supplier shall cooperate fully with the Purchaser in incident investigation, containment, eradication, recovery and post-incident review, and shall preserve relevant logs and evidence. Immediate notification shall not relieve the Supplier of its obligations to provide a detailed incident report and implement agreed corrective and preventive measures**.**

Design and Engineering (GCC Clause 21)

GCC 21.3.1	***There are no Special Conditions of Contract applicable to GCC Clause 21.3.1.*** ***[Note:*** *If necessary and appropriate, specify the Controlling Technical Documents (i.e., document that must be approved by the Purchaser's Project Manager before any relevant downstream work can be undertaken by the Supplier).]* *[If appropriate, insert "The Supplier shall prepare and furnish to the Project Manager the following documents for which the Supplier must obtain the Project Manager's approval before proceeding with work on the System or any Subsystem covered by the documents. [state* ***"none"*** *or specify, for example:* ***(*) detailed site surveys;*** ***(*) final Subsystem configurations;*** ***(*) etc.*** *]]"*

Product Upgrades (GCC Clause 23)

GCC 23.4	***There are no Special Conditions of Contract applicable to GCC Clause 23.4.*** *[**Note**: Mandating that all new versions, releases, and updates of Standard Software will be passed on for free during the Warranty Period is a comprehensive requirement, the benefits of which must be balanced against the perceived costs in the mind of the successful Proposer at the time of proposal submission. To require the Supplier to provide for free only new releases and updates, but agreeing that it would be reimbursed for the supply of complete new versions might be more cost-effective. For*

Official Use Only
Official Use Only

	example, this may be particularly appropriate when the Purchaser would not benefit from costs of migrating its business applications to an entirely new version of the underlying database system if such a version came out during a three Warranty Period. Another approach may be to shorten the time period during which updates, etc., would have to be supplied for free, for example, to only the first year of the Warranty Period; or alternatively, a more narrow set of Standard Software could be covered. *Also, note that the GCC only specifies the obligations "to provide" software updates. If the Purchaser needs to have the Supplier perform installation and configuration services associated with software updates, this needs to be clearly stated in the relevant service specifications in the Technical Requirements and text added to this SCC indicating the need for the Supplier to maintain such a service capacity: e.g., "The Supplier must maintain a service capacity to promptly deliver, provide, install and configure the provided versions, releases, and updates for all Standard Software that are used in the System at no additional cost to the Purchaser."]*

Inspections and Tests (GCC Clause 25)

GCC 25	***There are no Special Conditions of Contract applicable to GCC Clause 25.*** *[**Note**: Purchasers may wish to consider employing qualified inspectors to inspect and certify the Information Technologies, Materials, and other Goods prior to shipment. This can minimize the number of cases where the Purchaser receives shipped goods that do not conform to the Technical Requirements and shorten the repair or replacement time.]*

Commissioning and Operational Acceptance (GCC Clause 27)

GCC 27.2.1	***There are no Special Conditions of Contract applicable to GCC Clause 27.2.1.*** *[**Note**: Few aspects of Information Technology procurement are more critical to the successful implementation of a System than the specification of Operational Acceptance Tests. It is imperative that the Purchaser prepare the specification for these tests as carefully as the overall specification of the System itself. The description should be sufficiently comprehensive, unambiguous, and verifiable to result in proper operation of the System with*

Official Use Only
Official Use Only

	minimal confusion or controversy between the Purchaser and its management, the Supplier, and any users. *In addition, where the Contract covers the Installation and acceptance testing of a number of Subsystems, the nature of the acceptance tests required for each Subsystem, and for the final tests to be carried out on the entire System once all Subsystems have been completed, needs to be clearly specified here and/or in the Technical Requirements and which party bears responsibility for correcting any defects discovered during the final tests of the entire System needs to be identified.]*

F. GUARANTEES AND LIABILITIES

Operational Acceptance Time Guarantee (GCC Clause 28)

GCC 28.2	*In accordance with GCC Clause 28, if the Supplier fails to achieve Operational Acceptance of the Facilities (or any part thereof where sectional completion is applicable) by the respective Time for Completion specified in the Implementation Schedule, the Supplier shall pay to the Purchaser Liquidated Damages (LDs) at the rate of 0.5% of the Contract Price (or the applicable Subsystem/Milestone price as identified in the Implementation Schedule) per complete week of delay. The total aggregate amount of Liquidated Damages for delay under this Clause shall not exceed 10% of the final Contract Price.* *Once the maximum cap of* 10% *is reached, the Purchaser may consider termination of the Contract pursuant to GCC Clause 41.* *he Implementation Schedule shall explicitly designate the specific milestones subject to Liquidated Damages for delay. For the purposes of this Contract, the following milestones are identified as LD Milestones:* 1. *Milestone 1: Delivery and Site Acceptance of Core Hardware/Software (Target Date: T + 12 weeks)* 2. *Milestone 2: Completion of System Integration and Testing (Target Date: T + 26 weeks)* 3. *Milestone 3: Achievement of Operational Acceptance (Target Date: T + 35 weeks)* *SLA Response Times and Service Credit Mechanism (24/7 Support Services): For the continuous 24/7 operational and support services, the Supplier shall meet the Service Level Agreement (SLA) response and resolution times set forth below. Failure to meet these response times shall*

Official Use Only
Official Use Only

	trigger Service Credits, which shall be deducted from the subsequent month's maintenance/support fee or invoiced amount.
GCC 28.3	***There are no Special Conditions of Contract applicable to GCC Clause 28.3.*** *[**Note**: Establishing more milestones for liquidated damages may provide a somewhat greater degree of control and assurances regarding the pace of the implementation of the System. However, this will come at a price of increased complexity of Contract management and increased perceptions of financial risks on the part of Proposers. This most likely will lead to higher proposal prices. In most cases, Operational Acceptance should be the most appropriate financial control for ensuring the timeliness of implementation, since it captures the impact of earlier delays and is, in the final analysis, the milestone that truly matters. Whatever milestones are selected, it is critical that the Implementation Schedule precisely specify what Subsystems or other components are covered and when the milestone is set. These, of course, can be refined and revised through the Agreed Project Plan.]*

Defect Liability (GCC Clause 29)

GCC 29.1	***There are no Special Conditions of Contract applicable to GCC Clause 29.1.*** *[**Note**: Software is never completely error or "bug" free. Thus, the Purchaser may wish to refine or to limit the Supplier's warranty obligations. Properly done, this can reduce Proposer's perceptions of financial risk and help lower proposal prices. However, the Purchaser should balance the potential savings against the risks to reliable and effective operation of the System and the related costs to the Purchaser. These tradeoffs are very specific to the type of the System and its uses. These tradeoffs are also changing very rapidly with technological development. Accordingly, the World Bank recommends that Purchaser's consult experts in the relevant areas for an up-to-date assessment of the risks and the most appropriate text to express any such exceptions and limitations.]*
GCC 29.4	***There are no Special Conditions of Contract applicable to GCC Clause 29.4.***

Official Use Only
Official Use Only

	[Note: *When defining the Warranty period, Purchasers should be careful to recognize that services such as resident engineer support, new software releases and end-user help desk support are not typically included in commercial warranties and should be priced separately in the Recurrent Cost Table].*
GCC 29.10	***There are no Special Conditions of Contract applicable to GCC Clause 29.10*** ***[Note:*** *Typically, the Purchaser should develop a set of response times for different degrees of seriousness of the defects and/or categories of IT and/or specific Subsystems. The most appropriate and economical set of response times are highly dependent on the specific System, its use, and the relevant conditions in the Purchaser's Country.* *The GCC specifies that the Supplier must commence work on warranty defects within a maximum of two weeks; else the Purchaser may contract-in such services at the Supplier's expense. The Purchaser may wish to shorten or lengthen this period in the SCC. The time specified must strike a reasonable balance between the response time the typical qualified Supplier can physically achieve and the importance of maintaining continued System operation. If too short a time period is specified, Suppliers will need to protect themselves by adding a contingency to their proposal prices.]*

Functional Guarantees (GCC Clause 30)

GCC 30	***There are no Special Conditions of Contract applicable to GCC Clause 30.*** *[**Note**: In the event that Information Systems and Technologies would have to conform to other calendar system(s), here would be the place to specify related requirements in addition to, or in variation of, the requirements in GCC clause 30.2.]*
GCC 32	***There are no Special Conditions of Contract applicable to GCC Clause 32.*** *Insert:* ***necessary and appropriate clauses,*** *or state* ***"There are no Special Conditions of Contract applicable to GCC Clause 32."]***

Official Use Only
Official Use Only

G. RISK DISTRIBUTION

Insurances (GCC Clause 37)

GCC 37.1 (c)	*The Supplier shall obtain Third-Party Liability Insurance in the amount KES 20,000,000 (or USD 150,000) per occurrence with an UNLIMITED number of occurrences throughout the Contract and DLP. with deductible limits of no more than KES 1,000,000 (One Million Kenya Shillings) or equivalent in a freely convertible currency per claim.* *The insured Parties shall be jointly:* ***(i) The Information and Communications Technology Authority (ICTA) / Ministry (the Purchaser), and (ii) The Supplier (including its sub-contractors)****.* *The Insurance shall cover the period from* ***the Effective Date of the Contract*** *until* ***the issuance of the Operational Acceptance Certificate****.*
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 Purchaser's legal department.* *For example:* *The Supplier shall obtain Worker's Compensation Insurance in accordance with the statutory requirements of [insert:* ***the Purchaser's Country*** *]. Specifically: [insert****: requirements*** *]. 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*** *].* *The Supplier shall obtain Purchaser's Liability Insurance in accordance with the statutory requirements of [insert:* ***the Purchaser's Country*** *]. Specifically: [insert:* ***requirements*** *]. 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 Contract or its completion*** *].]*

Official Use Only
Official Use Only

H. CHANGE IN CONTRACT ELEMENTS

Changes to the System (GCC Clause 39)

GCC 39.2.1	***[Specify any additional requirements as appropriate]*** ***[If the contract has been assessed to present potential or actual cyber security risks, the following must be added]: "(f) sufficient information to enable assessment of cyber security risks."]***
GCC 39.4	**Value Engineering** The Purchaser **will not** consider a Value Engineering Proposal.

I. SETTLEMENT OF DISPUTES

Settlement of Disputes (GCC Clause 43)

GCC 43.1.4	The Appointing Authority for the Adjudicator is: The Registrar, **Nairobi Centre for International Arbitration** The hourly rate shall be determined in accordance with the prevailing fee schedule of the Nairobi Centre for International Arbitration (NCIA).
GCC 43.2.3	If the Supplier is from outside the Purchaser's Country arbitration proceedings shall be conducted in accordance with the rules of arbitration of ***UNCITRAL*** These rules, in the version in force at the time of the request for arbitration, will be deemed to form part of this Contract. If the Supplier is a national of the Purchaser's Country, any dispute between the Purchaser and a Supplier arising in connection with the present Contract shall be referred to arbitration in accordance with the laws of the Purchaser's country.

Official Use Only
Official Use Only

J. CYBER SECURITY

Cyber Security (GCC Clause 44)

GCC 44.1	Cyber Security ***applies***

Official Use Only
Official Use Only

SECTION X - CONTRACT FORMS

Notes to the Purchaser on preparing the Contract Forms

Performance Security: Pursuant to GCC Clause 13.3, the successful Proposer is required to provide the Performance Security within twenty-eight (28) days of notification of Contract award.

Advance Payment Security: Pursuant to Clause 13.2, the successful Proposer 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 Purchaser 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 Purchaser wishes to amend the recommended procedures and/or certificates, it may propose alternatives for the approval of the World Bank before release of the request for proposals document to potential Proposers.

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 request for proposals document unaltered. If the Purchaser wishes to amend the recommended procedures and/or certificates, it may propose alternatives for the approval of the World Bank before release of the request for proposals document.

Notes to Proposers on working with the Sample Contractual Forms

The following forms are to be completed and submitted by the successful Proposer following receipt of the Letter of Acceptance from the Purchaser: (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 Proposer's Proposal Price Schedules are attached to the Agreement. These contain corrections and adjustments to the Supplier's Proposal prices to correct errors, adjust the Contract Price to reflect – if applicable - any extensions to Proposal validity beyond the last day of original Proposal validity plus 56 days, etc.
- Performance Security: Pursuant to GCC Clause 13.3, the successful Proposer is required to provide the Performance Security in the form

Official Use Only
Official Use Only

contained in this section of this request for proposals document and in the amount specified in accordance with the SCC.

- Advance Payment Security: Pursuant to GCC Clause 13.2, the successful Proposer is required to provide a bank guarantee for the full amount of the Advance Payment - if an Advance Payment is specified in the SCC for GCC Clause 12.1 - in the form contained in this section of this request for proposals document or another form acceptable to the Purchaser. If a Proposer wishes to propose a different Advance Payment Security form, it should submit a copy to the Purchaser promptly for review and confirmation of acceptability before the proposal submission deadline.

The Purchaser 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 request for proposals document for the information of Proposers.

Official Use Only
Official Use Only

Table of Contract Forms

Notification of Intention to Award **379**

Beneficial Ownership Disclosure Form **383**

Letter of Acceptance **385**

1. Contract Agreement **386**

Appendix 1. Supplier's Representative 390
Appendix 2. Adjudicator 391
Appendix 3. List of Approved Subcontractors 392
Appendix 4. Categories of Software 393
Appendix 5. Custom Materials 394
Appendix 6. Revised Price Schedules 395
Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments 396

2. Performance and Advance Payment Security Forms **397**

2.1 ... Performance Security Form (Bank Guarantee) 398
2.2 ... Advance Payment Security Bank Guarantee 400

3. Installation and Acceptance Certificates **402**

3..... Installation and Acceptance Certificates 402
3.1 ... Installation Certificate 403
3.2 ... Operational Acceptance Certificate 404

4. Change Order Procedures and Forms **405**

4.1 ... Request for Change Proposal Form 406
4.2 ... Change Estimate Proposal Form 408
4.3 ... Estimate Acceptance Form 409
4.4 ... Change Proposal Form 410
4.5 ... Change Order Form 412
4.6 ... Application for Change Proposal Form 414

Official Use Only
Official Use Only

NOTIFICATION OF INTENTION TO AWARD

[This Notification of Intention to Award shall be sent to each Proposer that submitted a Proposal, unless the Proposer has previously received notice of exclusion from the process *Proposer.]*

[Send this Notification to the Proposer's Authorized Representative named in the Proposer Information Form]

For the attention of Proposer'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 Proposers. The Notification must be sent to all Proposers simultaneously. This means on the same date and as close to the same time as possible.]

DATE OF TRANSMISSION: This Notification is sent by: *[specify **email / fax**]* on *[specify **date**]* (local time)

Notification of Intention to Award

Purchaser: *[insert **the name of the Purchaser**]*

Project: *[insert **name of project**]*

Contract title: *[insert the **name of the contract**]*

Country: *[insert **country where RFP is issued**]*

Loan No. /Credit No. / Grant No.: *[insert **reference number for loan/credit/grant**]*

RFP No: *[insert RFP **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 in relation to the evaluation of your Proposal, and/or

b) submit a Procurement-related Complaint in relation to the decision to award the contract.

Official Use Only
Official Use Only

1. The successful Proposer

Name:	[*insert name of successful Proposer*]
Address:	[*insert address of the successful Proposer*]
Contract price:	[*insert contract price of the successful Proposer*]
Total combined score:	[*insert the total combined score of the successful Proposer*]

2. Other Proposers *[INSTRUCTIONS: insert names of all Proposers that submitted a Proposal, Proposal prices as read out and evaluated, technical scores and combined scores.]*

Name of Proposer	Technical Score (If applicable)	Proposal price	Evaluated Proposal Cost	Combined Score
[*insert name*]	[*insert Technical score*]	[*insert Proposal price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Proposal price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Proposal price*]	[*insert evaluated cost*]	[*insert combined score*]

3. Reason/s why your Proposal was unsuccessful *[Delete if the combined score already reveals the reason]*

[INSTRUCTIONS; State the reason/s why this Proposer's Proposal was unsuccessful. Do NOT include: (a) a point by point comparison with another Proposer's Proposal or (b) information that is marked confidential by the Proposer in its Proposal.]

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 Proposal. 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 Proposer, contact details; and address the request for debriefing as follows:

Official Use Only
Official Use Only

Attention: [*insert full name of person, if applicable*]

Title/position: [*insert title/position*]

Agency: [*insert name of Purchaser*]

Email address: [*insert email address*]

Fax number: [*insert fax number or state "not applicable"*]

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 Proposer, 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 Purchaser*]

Email address: [*insert email address*]

Fax number: [*insert fax number or state "not applicable"*]

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.

For more information see the "Procurement Regulations for IPF Borrowers (Procurement Regulations) (Annex III)." You should read these provisions before preparing and submitting your complaint. In addition, the World Bank's Guidance "How to make a Procurement-related Complaint" provides a useful explanation of the process, as well as a sample letter of complaint.

Official Use Only
Official Use Only

In summary, there are four essential requirements:

1. You must be an 'interested party'. In this case, that means a Proposer who submitted a Proposal 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 Purchaser:

Signature: _____

Title/position: [*insert* ***title/position***]

Agency: [*insert* ***name of Purchaser***]

Email address: [*insert* ***email address***]

Telephone number: [insert ***telephone number]***

Official Use Only
Official Use Only

BENEFICIAL OWNERSHIP DISCLOSURE FORM

INSTRUCTIONS TO PROPOSERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE FORM

This Beneficial Ownership Disclosure Form ("Form") is to be completed by the successful Proposer. In case of joint venture, the Proposer 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 Proposer is any natural person who ultimately owns or controls the Proposer by 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 Proposer*

RFP No.: *[insert **number of RFP process**]*
Request for Proposals No.: *[insert **identification**]*

To: **[***insert **complete name of Purchaser***]**

In response to your request in the Letter of Acceptance *dated [insert date of letter of Acceptance]* to furnish additional information on beneficial ownership: *[select one option as applicable and delete the options that are not applicable]*

(i) we hereby 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 Proposer (Yes / No)

Official Use Only
Official Use Only

[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 Proposer

OR

(iii) 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 Proposer 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 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 Proposer]"

Name of the Proposer: *[*insert* ***complete name of the Proposer***]

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

Title of the person signing the Proposal: [*insert* ***complete title of the person signing the Proposal***]

Signature of the person named above: _____

Date signed *[insert* ***ordinal number****]* day of *[insert* ***month****], [insert* ***year****]*

[*] In the case of the Proposal submitted by a Joint Venture specify the name of the Joint Venture as Proposer. In the event that the Proposer is a joint venture, each reference to "Proposer" in the Beneficial Ownership Disclosure Form (including this Introduction thereto) shall be read to refer to the joint venture member.

[**] Person signing the Proposal shall have the power of attorney given by the Proposer. The power of attorney shall be attached with the Proposal Schedules.

Official Use Only
Official Use Only

LETTER OF ACCEPTANCE

Purchaser: *[insert **the name of the Purchaser**]*

Project: *[insert **name of project**]*

Contract title: *[insert the **name of the contract**]*

Country: *[insert **country where RFP is issued**]*

Loan No. /Credit No. / Grant No.: *[insert **reference number for loan/credit/grant**]*

RFP No: *[insert RFP **reference number from Procurement Plan**]*

Date: *[insert **Date**]*

To: *[insert **Name of Proposer**]*

This is to notify you that your Proposal dated *[insert **Date**]* for execution of the *[insert **brief description of the Information System**]* for the Contract Price in the aggregate of *[insert **amount in figures**]* (*[insert **amount in words**]*), as corrected and modified in accordance with the Instructions to Proposers is hereby accepted by our Agency.

You are requested to furnish (i) the Performance Security within 28 days in accordance with the Conditions of Contract, using for that purpose one of the Performance Security Form*s* and (ii) the additional information on beneficial ownership in accordance with ITP 47.1 within eight (8) Business days using the Beneficial Ownership Disclosure Form, included in Section X, - Contract Forms, of the request for proposals document.

Authorized Signature: _____

Name and Title of Signatory: *[insert **Name and Title**]*

Name of Agency: *[insert **Purchaser Name**]*

Attachment: Contract Agreement

Official Use Only
Official Use Only

1. CONTRACT AGREEMENT

THIS CONTRACT AGREEMENT is made

the *[insert: **ordinal number**]* day of *[insert: **month**], [insert: **year].***

BETWEEN

(1) *[insert: **Name of Purchaser**],* a *[insert: **description of type of legal entity**, for example, an agency of the Ministry of . . . **]*** of the Government of *[insert: **country of Purchaser**],* or corporation incorporated under the laws of *[insert: **country of Purchaser**]* and having its principal place of business at *[insert**: address of Purchaser**]* (hereinafter called "the Purchaser"), and

(2) *[insert: **name of Supplier**],* a corporation incorporated under the laws of *[insert: **country of Supplier**]* and having its principal place of business at *[insert: **address of Supplier**]* (hereinafter called "the Supplier").

WHEREAS the Purchaser desires to engage the Supplier to supply, install, achieve Operational Acceptance of, and support the following Information System *[insert: **brief description of the Information System**]* ("the System"), and the Supplier has agreed to such engagement upon and subject to the terms and conditions appearing below in this Contract Agreement.

NOW IT IS HEREBY AGREED as follows:

Article 1. Contract Documents

1.1 Contract Documents (Reference GCC Clause 1.1 (a) (ii))

The following documents shall constitute the Contract between the Purchaser 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 proposal and original Price Schedules

(f) Code of Conduct for Supplier's Personnel

Official Use Only
Official Use Only

(g) *[Add here:* ***any other documents*** *]*

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, provided that 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 Clause 1)

Capitalized words and phrases used in this Contract Agreement shall have the same meanings as are ascribed to them in the General Conditions of Contract.

Article 2.

Contract Price and Terms of Payment

2.1 Contract Price (Reference GCC Clause 1.1(a)(viii) and GCC Clause 11)

The Purchaser hereby 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 of: *[insert:* ***amount of foreign currency A in words*** *],* *[insert:* ***amount in figures*** *],* plus *[insert:* ***amount of foreign currency B in words*** *], [insert:* ***amount in figures],*** plus *[insert:* ***amount of foreign currency C in words*** *], [insert****: amount in figures*** *], [insert:* ***amount of local currency in words*** *], [insert:* ***amount in figures],*** as specified in the Grand Summary Price Schedule.

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.

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 Purchaser and the Supplier;

(b) The Supplier has submitted to the Purchaser the performance security and the advance payment security, in accordance with GCC Clause 13.2 and GCC Clause 13.3;

(c) The Purchaser has paid the Supplier the advance payment, in accordance with GCC Clause 12;

Official Use Only
Official Use Only

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.

Article 4. 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.

APPENDIXES

Appendix 1. Supplier's Representative
Appendix 2. Adjudicator *[if there is no Adjudicator, state **"not applicable"**]*
Appendix 3. List of Approved Subcontractors
Appendix 4. Categories of Software
Appendix 5. Custom Materials
Appendix 6. Revised Price Schedules (if any)
Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments

IN WITNESS WHEREOF the Purchaser and the Supplier have caused this Agreement to be duly executed by their duly authorized representatives the day and year first above written.

For and on behalf of the Purchaser

Signed:

in the capacity of *[insert: **title or other appropriate designation**]*

in the presence of

For and on behalf of the Supplier

Official Use Only
Official Use Only

Signed:

in the capacity of *[insert: **title or other appropriate designation**]*

in the presence of

CONTRACT AGREEMENT

dated the *[insert: **number**]* day of *[insert: **month**], [insert: **year**]*

BETWEEN

*[insert: **name of Purchaser**],* "the Purchaser"

and

*[insert: **name of Supplier**],* "the Supplier"

Official Use Only
Official Use Only

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.*** *]*

Official Use Only
Official Use Only

Appendix 2. Adjudicator

In accordance with GCC Clause 1.1 (b) (vi), the agreed-upon Adjudicator is:

Name: *[insert:* ***name*** *]*
Title: *[insert:* ***title*** *]*
Address: *[insert:* ***postal address*** *]*
Telephone: *[insert:* ***telephone*** *]*

In accordance with GCC Clause 43.1.3, the agreed-upon fees and reimbursable expenses are:

Hourly Fees: *[insert:* ***hourly fees*** *]*
Reimbursable Expenses: *[list:* ***reimbursables*** *]*

Pursuant to GCC Clause 43.1.4, if at the time of Contract signing, agreement has not been reached between the Purchaser and the Supplier, an Adjudicator will be appointed by the Appointing Authority named in the SCC.

Official Use Only
Official Use Only

Appendix 3. List of Approved Subcontractors

The Purchaser has approved use of the following Subcontractors nominated by the Supplier for carrying out the item or component of the System indicated. Where more than one Subcontractor is listed, the Supplier is free to choose between them, but it must notify the Purchaser of its choice sufficiently in advance of the time when the subcontracted work needs to commence to give the Purchaser reasonable time for review. In accordance with GCC Clause 20.1, the Supplier is free to submit proposals for Subcontractors for additional items from time to time. No subcontracts shall be placed with any such Subcontractors for additional items until the Subcontractors have been approved in writing by the Purchaser and their names have been added to this list of Approved Subcontractors, subject to GCC Clause 20.3.

[specify: ***item, approved Subcontractors, and their place of registration that the Supplier proposed in the corresponding attachment to its proposal and that the Purchaser approves that the Supplier engage during the performance of the Contract. Add additional pages as necessary.]***

Item	Approved Subcontractors	Place of Registration

Official Use Only
Official Use Only

Appendix 4. Categories of Software

The following table assigns each item of Software supplied and installed under the Contract to one of the three categories: (i) System Software, (ii) General-Purpose Software, or (iii) Application Software; and to one of the two categories: (i) Standard Software or (ii) Custom Software and to one of the two categories: (i) Proprietary or (ii) Open Source.

	(select one per title)			(select one per title)		(select one per title)	
Title	System	General-Purpose	Application	Standard	Custom	Proprietary	Open Source
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							
[insert Title]							

Official Use Only
Official Use Only

Appendix 5. Custom Materials

The follow table specifies the Custom Materials the Supplier will provide under the Contract.

Custom Materials
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*
*[insert **Title and description**]*

Official Use Only
Official Use Only

Appendix 6. Revised Price Schedules

The attached Revised Price Schedules (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the Price Schedules contained in the Supplier's Proposal. These Revised Price Schedules reflect any corrections or adjustments to the Supplier's proposal price, pursuant to the ITP Clauses 30.3 and 38.2.

Official Use Only
Official Use Only

Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments

The attached Contract amendments (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the relevant clauses in the GCC, SCC, Technical Requirements, or other parts of this Contract as defined in GCC Clause 1.1 (a) (ii).

Official Use Only
Official Use Only

2. PERFORMANCE AND ADVANCE PAYMENT SECURITY FORMS

Official Use Only
Official Use Only

2.1 Performance Security Form (Bank Guarantee)

(Bank Guarantee)

[The bank, as requested by the successful Proposer, shall fill in this form in accordance with the instructions indicated]

[Guarantor letterhead or SWIFT identifier code]

*[insert: **Bank's Name, and Address of Issuing Branch or Office**]*

Beneficiary: *[insert: **Name and Address of Purchaser**]*

Date: *[insert: **date**]*

PERFORMANCE GUARANTEE No.: *[insert: **Performance Guarantee Number**]*

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*

We have been informed that on *[insert: **date of award**]* you awarded Contract No. *[insert: **Contract number**]* for *[insert: **title and/or brief description of the Contract**]* (hereinafter called "the Contract") to *[insert: **complete name of Supplier which in the case of a joint venture shall be in the name of the joint venture**]* (hereinafter called "the Applicant"). Furthermore, we understand that, according to the conditions of the Contract, a performance guarantee is required.

At the request of the Applicant, we as Guarantor hereby irrevocably undertake to pay you any sum(s) not exceeding *[insert: **amount(s)**[1] **in figures and words**]* such sum being payable in the types and proportions of currencies which the Contract Price is payable upon receipt by us of 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 or reasons for their demand or the sum specified therein.

On the date of your issuing, to the Supplier, the Operational Acceptance Certificate for the System, the value of this guarantee will be reduced to any sum(s) not exceeding *[insert: **amount(s)**[1] **in figures and words**]*. This remaining guarantee shall expire no later than *[insert: **number** and select: **of months/of years** (of the Warranty Period that needs to be covered by the remaining guarantee)]* from the date of the Operational Acceptance Certificate for the System,[2] and any demand for payment under it must be received by us at this office on or before that date.

---

[1] *The bank shall insert the amount(s) specified and denominated in the SCC for GCC Clauses 13.3.1 and 13.3.4 respectively, either in the currency(ies) of the Contract or a freely convertible currency acceptable to the Purchaser.*

[2] *In this sample form, the formulation of this paragraph reflects the usual SCC provisions for GCC Clause 13.3. However, if the SCC for GCC Clauses 13.3.1 and 13.3.4 varies from the usual provisions, the paragraph, and possibly the previous paragraph, need to be adjusted to precisely reflect the provisions specified in the SCC.*

Official Use Only
Official Use Only

This guarantee is subject to the Uniform Rules for Demand Guarantees, (URDG) 2010 Revision, ICC Publication No. 758, except that the supporting statement under 15 (a) is hereby excluded.

_____

[Signature(s)]

*[**Note**: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.]*

Official Use Only
Official Use Only

2.2 Advance Payment Security Bank Guarantee

[Guarantor letterhead or SWIFT identifier code]

Beneficiary: *[insert: **Name and Address of Purchaser**]*

Date: ***[insert date of issue]***

ADVANCE PAYMENT GUARANTEE No.: *[insert: **Advance Payment Guarantee Number**]*

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*

We have been informed that on *[insert: **date of award**]* you awarded Contract No. *[insert: **Contract number**]* for *[insert: **title and/or brief description of the Contract**]* (hereinafter called "the Contract") to *[insert: **complete name of Supplier, which in the case of a joint venture shall be the name of the joint venture**]* (hereinafter called "the Applicant").

Furthermore, we understand that, according to the conditions of the Contract, an advance payment in the sum of *[insert: **amount in numbers and words, for each currency of the advance payment**]* is to be made to the Supplier against an advance payment guarantee.

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 *[insert **amount in figures**] ([insert **amount in words**])*[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 accompanying or identifying the demand, stating either that the Applicant:

(a) has used the advance payment for purposes other than toward delivery of Goods; 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.

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

[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 Purchaser.*

Official Use Only
Official Use Only

credited to the Applicant on its account number *[insert **number**]* at *[insert **name and address of Applicant's bank**]*.

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, has been certified for payment, or on the *[insert **day**]* day of *[insert **month**]*, *[insert **year**]*, whichever is earlier. Consequently, any demand for payment under this guarantee must be received by us at this office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees (URDG) 2010 Revision, ICC Publication No.758, except that the supporting statement under Article 15(a) is hereby excluded.

_____

[signature(s)]

*[**Note**: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.]*

Official Use Only
Official Use Only

3. INSTALLATION AND ACCEPTANCE CERTIFICATES

3. Installation and Acceptance Certificates

Official Use Only
Official Use Only

3.1 Installation Certificate

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

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 Purchaser*** *]* (hereinafter the "Purchaser") 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 letter 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 Purchaser

Signed:

Date:

in the capacity of: *[state:* ***"Project Manager"*** *or specify a higher level authority in the Purchaser's organization]*

Official Use Only
Official Use Only

3.2 Operational Acceptance Certificate

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

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 Purchaser*** *]* (hereinafter the "Purchaser") 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 Purchaser hereby 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 letter 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 Purchaser

Signed:_____

Date: *[insert:* ***date*** *]*

in the capacity of: *[state:* ***"Project Manager"*** *or specify a higher level authority in the Purchaser's organization]*

Official Use Only
Official Use Only

4. CHANGE ORDER PROCEDURES AND FORMS

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

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 Purchaser.

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

4.1 Request for Change Proposal Form
4.2 Change Estimate Proposal Form
4.3 Estimate Acceptance Form
4.4 Change Proposal Form
4.5 Change Order Form
4.6 Application for Change Proposal Form

Official Use Only
Official Use Only

4.1 Request for Change Proposal Form

(Purchaser's Letterhead)

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

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 letter.

1. Title of Change: *[insert:* ***title*** *]*
2. Request for Change No./Rev.: *[insert:* ***number*** *]*
3. Originator of Change: *[select* ***Purchaser / 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.

Official Use Only
Official Use Only

(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 its 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 Purchaser

Signed:

Date:

in the capacity of: *[state:* ***"Project Manager"*** *or specify a higher level authority in the Purchaser's organization]*

Official Use Only
Official Use Only

4.2 Change Estimate Proposal Form

(Supplier's Letterhead)

Date: *[insert:* ***date*** *]*

Loan/Credit Number: *[insert:* ***loan or credit number from RFP*** *]*

RFP: *[insert:* ***title and number of RFP*** *]*

Contract: *[insert:* ***name of System or Subsystem and number of Contract*** *]*

To: *[insert:* ***name of Purchaser 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 specify a other higher level authority in the Supplier's organization]*

Official Use Only
Official Use Only

4.3 Estimate Acceptance Form

(Purchaser's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

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: *[insert: **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 Purchaser

Signed:

Date:

in the capacity of: *[state: **"Project Manager"** or specify a higher level authority in the Purchaser's organization]*

Official Use Only
Official Use Only

4.4 Change Proposal Form

(Supplier's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contract**]*

To: *[insert: **name of Purchaser and address**]*

Attention: *[insert: **name and title**]*

Dear Sir or Madam:

In response to your Request for Change Proposal No. *[insert: **number],*** we hereby submit our proposal as follows:

1. Title of Change: *[insert: **name**]*
2. Change Proposal No./Rev.: *[insert: **proposal number/revision**]*
3. Originator of Change: *[select: **Purchaser / 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**]*

Official Use Only
Official Use Only

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 Purchaser
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 specify a other higher level authority in the Supplier's organization **]***

Official Use Only
Official Use Only

4.5 Change Order Form

(Purchaser's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

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. Originator of Change: *[select: **Purchaser / 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 Purchaser

Signed: _____

Date*: [insert **date**]*

in the capacity of: *[state: **"Project Manager"** or higher level authority in the Purchaser's organization]*

Official Use Only
Official Use Only

For and on behalf of the Supplier

Signed:_____

Date: *[insert **date**]*

in the capacity of: *[state **"Supplier's Representative"** or specify a higher level authority in the Supplier's organization]*

Official Use Only
Official Use Only

4.6 Application for Change Proposal Form

(Supplier's Letterhead)

Date: *[insert: **date**]*

Loan/Credit Number: *[insert: **loan or credit number from RFP**]*

RFP: *[insert: **title and number of RFP**]*

Contract: *[insert: **name of System or Subsystem and number of Contrac**t]*

To: *[insert: **name of Purchaser 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 the System.

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 specify a higher level authority in the Supplier's organization]*

Official Use Only
Official Use Only