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.

Government of Kenya

Request for Bids
Information Systems
Design, Supply and Installation

(One-Envelope Bidding Process)

(Without Prequalification)

Procurement of:

Data Management Information System, Case Management System, Legislative Drafting Information Management System, Legal Opinion System and Correctional Services Management Information System

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

Project: **Kenya Digital Economy Acceleration Project**

Contract title: **Provision of Automation Services for Selected Ministries, Departments & Agencies in Three (3) Lots**

   LOT 1: Data Management Information System for Office of the Data Protection Commissioner; LOT 2: Case Management System, Legislative Drafting Information Management System, & Legal Opinion System for Office of the Attorney General; LOT 3: Correctional Services Management Information System for State Department for Correctional Services

Country: **Kenya**

Loan No. /Credit No. / Grant No.: **7289-KE and 7290-KE**

RFB No: **KE-ICTA-458650-NC-RFB**

Issued on: **1st July 2025**

Specific Procurement Notice – Request for Bids without Prequalification

Request for Bid
Information Systems
(Design, Supply and Installation)
(Without Prequalification)

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

Project**: Kenya Digital Economy Acceleration Project**

Contract title**: Provision of Automation Services for Selected Ministries, Departments & Agencies**

LOT 1: Data Management Information System for Office of the Data Protection Commissioner

LOT 2: Case Management System, Legislative Drafting Information Management System, & Legal Opinion System for Office of the Attorney General

LOT 3: Correctional Services Management Information System for State Department for Correctional Services

Country**: Kenya**

Loan No. /Credit No. / Grant No.: **7289-KE and 7290-KE**

RFB No: **KE-ICTA-458650-NC-RFB**

Issued on: **1ˢᵗ July 2025**

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 Provision of Automation Services for Selected Ministries, Departments & Agencies in Three (3) LOTS:
LOT 1: Data Management Information System for Office of the Data Protection Commissioner.

LOT 2: Case Management System, Legislative Drafting Information Management System, & Legal Opinion System for Office of the Attorney General.

LOT 3: Correctional Services Management Information System for State Department for Correctional Services.

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 now invites sealed Bids from eligible Bidders for Provision of Automation Services for Selected Ministries, Departments & Agencies in Three (3) Lots

Lot Number	Description	Quantity	Delivery Period from contract commencement date	Location
LOT 1	Data Management Information System	1	12 calendar months	Office of Data Protection Commissioner
LOT 2	Case Management Systems	1	12 calendar months	Office of Attorney General
	Legislative Drafting Information Management System	1	12 calendar months	
	Legal Opinion System	1	12 calendar months	
LOT 3	Correctional Services Management Information Systems	1	12 calendar months	State Department for Correctional Services

3.   Bidders may Bid for one or several lots, as further defined in the bidding document. Bidders wishing to offer discounts in case they are awarded more than one contract will be allowed to do so, provided those discounts are included in the Letter of Bid.

4.   Bidding will be conducted through national competitive procurement using Request for Bids (RFB) as specified in the World Bank's "Procurement Regulations for IPF Borrowers" First Published July 2016, Revised Fifth Edition September 2023 ("Procurement Regulations"), and is open to all eligible Bidders as defined in the Procurement Regulations.

5. Interested eligible Bidders may obtain further information from The Information and Communications Technology Authority*,* Deputy Director, Supply Chain Management, procurement@ict.go.ke and inspect the bidding document during office hours 0900 to 1600 hours at the address given below.

6. The bidding document in English may be downloaded free of charge 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 procuring entity by email with full contact details if they intend to participate, as this will facilitate issuance of notifications by the procuring entity, to all bidders where necessary.

7. Bids must be delivered to the address below on or before **1000 hours EAT 14th August 2025**. Electronic Bidding **will not** be permitted. Late Bids will be rejected. Bids will be publicly opened in the presence of the Bidders' designated representatives and anyone who chooses to attend at the address below on **1000 hours EAT 14th August 2025**

8. All Bids must be accompanied by a **Bid Security** of **Kes. 1 Million (Kenya Shillings One Million) for LOT 1** or equivalent in a freely convertible currency, **Kes. 2.5 Million (Kenya Shillings Two Million, five hundred thousands) for LOT** 2 or equivalent in a freely convertible currency & **Kes. 1 Million (Kenya Shillings One Million) for LOT 3** or equivalent in a freely convertible currency

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

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

Stanley Kamanguya, OGW
Chief Executive Officer
The Information and Communications Technology Authority
12th Floor, Telposta Towers, Kenyatta Avenue
Nairobi, Kenya.
(+254) 20 667 6999
info@ict.go.ke / procurement@ict.go.ke
www.icta.go.ke

Table of Contents

PART 1 – BIDDING PROCEDURES

SECTION I - INSTRUCTIONS TO BIDDERS (ITB)
Contents

Section I - Instructions to Bidders

A.   GENERAL

1. Scope of Bid

1.1. The Purchaser, as indicated in the BDS, or its duly authorized Purchasing Agent if so specified in the BDS (interchangeably referred to as "the Purchaser" issues this bidding document for the supply and installation of the Information System as specified in Section VII, Purchaser's Requirements. The name, identification and number of lots (contracts) of this RFB are specified in the BDS.

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

Throughout this bidding document:

(a) the term "in writing" means communicated in written form (e.g. by mail, e-mail, fax, including if specified in the BDS, 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 Sub-Clause 1.1; and

(h) "Purchaser's Personnel" is as defined in GCC Sub-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 BDS 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 BDS toward the project named in the BDS. The Borrower intends to apply a portion of the funds to eligible payments under the contract(s) for which this bidding 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, Bidders 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 Bidders

4.1.   A Bidder may be a firm that is a private entity, a state-owned enterprise or institution subject to ITB 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 Bidding process and, in the event the JV is awarded the Contract, during contract execution. Unless specified in the BDS, there is no limit on the number of members in a JV.

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

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

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

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

(d)   has a relationship with another Bidder, directly or through common third parties, that puts it in a position to influence the Bid of another Bidder, or influence the decisions of the Purchaser regarding this Bidding 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 Bid; 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 project specified in the BDS ITB 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 bidding document or specifications of the Contract, and/or the Bid 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 Bidding process and execution of the Contract.

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

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

4.5.   A Bidder 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 BDS.

4.6.   Bidders 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 Bidder shall not be under suspension from bidding 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 Bidding is open for all eligible Bidders, unless otherwise specified in ITB 15.2.

4.10.   A Bidder 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 bidding 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 Bidder and as specified in the Contract.

5.3. For purposes of ITB 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 BIDDING DOCUMENT

6. Sections of Bidding Document

6.1 The bidding 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 ITB 8:

PART 1 - Bidding Procedures

Section I - Instructions to Bidders (ITB)

Section II - Bid Data Sheet (BDS)

Section III - Evaluation and Qualification Criteria

Section IV - Bidding 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

6.1.   The Specific Procurement Notice – Request for Bids (RFB) issued by the Purchaser is not part of this bidding 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-Bid meeting (if any), or Addenda to the bidding document in accordance with ITB 8. In case of any contradiction, documents obtained directly from the Purchaser shall prevail.

6.4   The Bidder is expected to examine all instructions, forms, terms, and specifications in the bidding document and to furnish with its Bid all information or documentation as is required by the bidding document.

7. Clarification of Bidding Document, Site Visit, Pre-bid Meeting

7.1. A Bidder requiring any clarification of the bidding document shall contact the Purchaser in writing at the Purchaser's address specified in the BDS or raise its enquiries during the pre-Bid meeting if provided for in accordance with ITB 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 Bids within a period specified in the BDS. The Purchaser's shall forward copies of its response to all Bidders who have acquired the bidding document in accordance with ITB 6.3, including a description of the inquiry but without identifying its source. If so specified in the BDS, the Purchaser shall also promptly publish its response at the web page identified in the BDS. Should the Purchaser deem it necessary to amend the bidding document as a result of a request for clarification, it shall do so following the procedure under ITB 8 and ITB 23.2.

7.2. The Bidder 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 Bid and entering into a contract. The costs of visiting the site shall be at the Bidder's own expense.

7.3. The Bidder 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 Bidder, 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 Bidder's designated representative is invited to attend a pre-Bid meeting and/or a site visit, if provided for in the BDS. 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 Bidder is requested, as far as possible, to submit any questions in writing, to reach the Purchaser not later than one week before the meeting.

7.6. Minutes of the pre-Bid 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 Bidders who have acquired the bidding document in accordance with ITB 6.3. Any modification to the bidding document that may become necessary as a result of the pre-Bid meeting shall be made by the Purchaser exclusively through

the issue of an Addendum pursuant to ITB 8 and not through the minutes of the pre-Bid meeting.

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

8. Amendment of Bidding Document

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

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

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

C. PREPARATION OF BIDS

9. Cost of Bidding

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

10. Language of Bid

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

11. Documents Comprising the Bid

11.1. The Bid submitted by the Bidder shall comprise the following:

(a) **Letter of Bid** prepared in accordance with ITB 12;

(b) **Price Schedules** completed in accordance with ITB 12 and ITB 17;

(c) **Bid Security or Bid-Securing Declaration** in accordance with ITB 20;

(d) **Alternative Bid:** if permissible, in accordance with ITB 13;

(e) **Authorization:** written confirmation authorizing the signatory of the Bid to commit the Bidder, in accordance with ITB 21.3;

(f) **Eligibility of Information System:** documentary evidence established in accordance with ITB 14.1 that the Information System offered by the Bidder in its Bid or in any alternative Bid, if permitted, are eligible;

(g) **Bidder's Eligibility:** documentary evidence in accordance with ITB 15 establishing the Bidder's eligibility and qualifications to perform the contract if its Bid is accepted;

(h) **Conformity:** documentary evidence established in accordance with ITB 16 that the Information System offered by the Bidder conform to the bidding document;

(i) **Subcontractors:** list of subcontractors, in accordance with ITB 16.4;

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

   (i) all Software included in the Bid, 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 Bid;

   All Materials not identified as Custom Materials shall be deemed Standard Materials, as defined in GCC Clause 1.1 (c);

   Re-assignments among the Software and Materials categories, if necessary, will be made during the implementation of the Contract according to GCC Clause 39 (Changes to the Information System); and

(k) any other document required **in the BDS.**

11.2. In addition to the requirements under ITB 11.1, Bids submitted by a JV shall include a copy of the Joint Venture Agreement entered into by all members indicating at least the parts of the Information System to be executed by the respective members. Alternatively, a

letter of intent to execute a Joint Venture Agreement in the event of a successful Bid shall be signed by all members and submitted with the Bid, together with a copy of the proposed Agreement indicating at least the parts of the Information System to be executed by the respective members.

11.3.   The Bidder shall furnish in the Letter of Bid information on commissions and gratuities, if any, paid or to be paid to agents or any other party relating to this Bid.

12. Letter of Bid and Price Schedules

12.1.   The Bidder shall complete the Letter of Bid, including the appropriate Price Schedules, using the relevant forms furnished in Section IV, Bidding Forms. The forms must be completed without any alterations to the text, and no substitutes shall be accepted except as provided under ITB 21.3. All blank spaces shall be filled in with the information requested.

13. Alternative Bids

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

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

13.3.   Except as provided under ITB 13.4 below, Bidders wishing to offer technical alternatives to the Purchaser's requirements as described in the bidding 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 Bidder with the Most Advantageous Bid conforming to the basic technical requirements shall be considered by the Purchaser.

13.4.   When Bidders are invited in the BDS 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 ITB 35.

14. Documents Establishing the Eligibility of the Information System	14.1.	To establish the eligibility of the Information System in accordance with ITB 5, Bidders shall complete the country of origin declarations in the Price Schedule Forms, included in Section IV, Bidding Forms.
15. Documents Establishing the Eligibility and Qualifications of the Bidder	15.1.	To establish its eligibility and qualifications to perform the Contract in accordance with Section III, Evaluation and Qualification Criteria, the Bidder shall provide the information requested in the corresponding information sheets included in Section IV, Bidding Forms.
	15.2.	In the event that prequalification of potential Bidders has been undertaken as stated in the BDS, only Bids from prequalified Bidders shall be considered for award of Contract. These qualified Bidders should submit with their Bids any information updating their original prequalification applications or, alternatively, confirm in their Bids that the originally submitted prequalification information remains essentially correct as of the date of Bid submission.
16. Documents Establishing Conformity of the Information System	16.1.	Pursuant to ITB 11.1 (h), the Bidder shall furnish, as part of its Bid, documents establishing the conformity to the bidding documents of the Information System that the Bidder proposes to design, supply and install under the Contract.
	16.2.	The documentary evidence of conformity of the Information System to the bidding documents including:

    (a)   Preliminary Project Plan describing, among other things, the methods by which the Bidder will carry out its overall management and coordination responsibilities if awarded the Contract, and the human and other resources the Bidder proposes to use. The Preliminary Project Plan must also address any other topics specified in the BDS. In addition, the Preliminary Project Plan should state the Bidder'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 Bidder proposes to coordinate the activities of all involved parties;

    (b)   written confirmation that the Bidder accepts responsibility for the successful integration and inter-operability of all components of the Information System as required by the bidding 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 Bidder should use the Technical Responsiveness Checklist (or Checklist Format) in the Sample Bidding Forms (Section IV). The commentary shall include explicit cross-references to the relevant pages in the supporting materials included in the bid. Whenever a discrepancy arises between the item-by-item commentary and any catalogs, technical specifications, or other preprinted materials submitted with the bid, 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 BDS ITB 17.2 requires Bidders to bid.

16.3.   References to brand names or model numbers or national or proprietary standards designated by the Purchaser in the bidding documents are intended to be descriptive and not restrictive. Except as specified in the BDS for specific items or standards, the Bidder may substitute alternative brand/model names or standards in its bid, 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 Bidder intends to purchase or subcontract, the Bidder shall give details of the name and nationality of the proposed subcontractors, including manufacturers, for each of those items. In addition, the Bidder shall include in its Bid 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 Bidder shall be responsible for ensuring that any subcontractor proposed complies with the requirements of ITB 4, and that any goods or services to be provided by the subcontractor comply with the requirements of ITB 5 and ITB 16.1.

17. Bid 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 Bidder to fulfill the

requirements of the Information System, must be priced separately and summarized in the corresponding cost tables in the Sample Bidding 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 BDS, the Bidder must also bid 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 Bidding Forms (Section IV), in accordance with the instructions provided in the tables and in the manner specified below:

(a)   if specified **in the BDS,** the Bidder must also bid 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 Bidder'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. Bidders 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 Bidder has left blank in the cost tables provided in the Sample Bid 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 bid and, provided that the bid is substantially responsive, an adjustment to the bid price will be made during bid evaluation in accordance with ITB 31.3.

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 BDS, as follows:

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

Unless otherwise specified **in the BDS**, 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 Bidder shall be free to use transportation through carriers registered in any eligible countries.   Similarly, the Bidder 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 BDS, 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 ITB 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 ITB 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.

17.8.   Unless otherwise specified in the BDS, 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 bidding documents (as, e.g., a requirement for the Bidder to include the travel and subsistence costs of trainees).

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

18. Currencies of Bid and Payment

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

18.2. The Bidder may express the Bid price in any currency. If the Bidder 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 Bids

19.1. Bids shall remain valid until the date specified in the BDS or any extended date if amended by the Purchaser in accordance with ITB 8. A Bid that is not valid until the date specified in the BDS, or any extended date if amended by the Purchaser in accordance with ITB 8, shall be rejected by the Purchaser as nonresponsive.

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

19.3. If the award is delayed by a period exceeding fifty-six (56) days beyond the expiry of the initial Bid validity specified in accordance with ITB 19.1, the Contract price shall be determined as follows:

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

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

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

20. Bid Security   20.1.   The Bidder shall furnish as part of its Bid, either a Bid-Securing Declaration or a Bid Security as specified in the BDS, in original form and, in the case of a Bid Security, in the amount and currency specified in the BDS.

20.2.   A Bid-Securing Declaration shall use the form included in Section IV, Bidding Forms.

20.3.   If a Bid Security is specified pursuant to ITB 20.1, the bid security shall be a demand guarantee in any of the following forms at the Bidder'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 BDS,**

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 Bid submission, that a correspondent financial institution is not required. In the case of a bank guarantee, the Bid Security shall be submitted either using the Bid Security Form included in Section IV, Bidding Forms or in another substantially similar format approved by the Purchaser prior to Bid submission. In either case, the form must include the complete name of the Bidder. The Bid Security shall be valid for twenty-eight (28) days beyond the original date of expiry of the Bid validity, or beyond any extended date if requested under ITB 19.2.

20.4.   If a Bid Security or a Bid-Securing Declaration is specified pursuant to ITB 20.1, any Bid not accompanied by a substantially responsive Bid Security or Bid-Securing Declaration shall be rejected by the Purchaser as non-responsive.

20.5. If a Bid Security is specified pursuant to ITB 20.1, the Bid Security of unsuccessful Bidders shall be returned as promptly as possible upon the successful Bidder's furnishing of the Performance Security pursuant to ITB 48.

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

20.7. The Bid Security may be forfeited:

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

(b)   if the successful Bidder fails to:

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

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

20.8. The Bid Security or the Bid-Securing Declaration of a JV shall be in the name of the JV that submits the bid. If the JV has not been legally constituted into a legally enforceable JV at the time of Bidding, the Bid Security or the Bid-Securing Declaration shall be in the names of all future members as named in the letter of intent referred to in ITB 4.1 and ITB 11.2.

20.9. If a Bid Security is not required in the BDS, and;

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

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

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

21. Format and Signing of Bid

21.1. The Bidder shall prepare one original of the documents comprising the Bid as described in ITB 11 and clearly mark it "Original." Alternative Bids, if permitted in accordance with ITB 13, shall be clearly marked "Alternative". In addition, the Bidder shall submit copies of the Bid, in the number specified in the BDS and clearly mark them "Copy." In the event of any discrepancy between the original and the copies, the original shall prevail.

21.2. Bidders shall mark as "CONFIDENTIAL" information in their Bids 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 Bid shall be typed or written in indelible ink and shall be signed by a person duly authorized to sign on behalf of the Bidder. This authorization shall consist of a written confirmation as specified in the BDS and shall be attached to the Bid. The name and position held by each person signing the authorization must be typed or printed below the signature. All pages of the Bid where entries or amendments have been made shall be signed or initialed by the person signing the Bid.

21.4. In case the Bidder is a JV, the Bid 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 Bid.

D. SUBMISSION AND OPENING OF BIDS

22. Submission, Sealing and Marking of Bids

22.1. The Bidder shall deliver the Bid in a single, sealed envelope (one (1) envelope process). Within the single envelope the Bidder shall place the following separate, sealed envelopes:

(a) in an envelope marked "ORIGINAL", all documents comprising the Bid, as described in ITB 11; and

(b) in an envelope marked "COPIES", all required copies of the Bid; and,

(c) if alternative Bids are permitted in accordance with ITB 13, and if relevant:

(i) in an envelope marked "ORIGINAL – ALTERNATIVE BID", the alternative Bid; and

(ii) in the envelope marked "COPIES – ALTERNATIVE BID" all required copies of the alternative Bid.

22.2. The inner and outer envelopes shall:

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

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

(c) bear the specific identification of this Bidding process indicated in accordance with ITB 1.1; and

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

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

23. Deadline for Submission of Bids

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

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

24. Late Bids

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

25. Withdrawal, Substitution, and Modification of Bids

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

(a)   prepared and submitted in accordance with ITB 21 and ITB 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 Bids, in accordance with ITB 23.

25.2.   Bids requested to be withdrawn in accordance with ITB 25.1 shall be returned unopened to the Bidders.

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

26. Bid Opening

26.1.   Except as in the cases specified in ITB 24 and ITB 25.2, the Purchaser shall conduct the Bid opening in public, in the presence of Bidders` designated representatives and anyone who chooses to attend, and at the address, date and time specified in the BDS. Any specific electronic Bid opening procedures required if electronic bidding is permitted in accordance with ITB 23.1, shall be as specified in the BDS.

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

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

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

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

26.6. Only Bids, alternative Bids and discounts that are opened and read out at Bid opening shall be considered further in the evaluation. The Letter of Bid and the Price Schedules are to be initialed by representatives of the Purchaser attending Bid opening in the manner specified in the BDS.

26.7. The Purchaser shall neither discuss the merits of any Bid nor reject any Bid (except for late Bids, in accordance with ITB 24.1).

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

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

(b) the Bid Price, per lot if applicable, including any discounts;

(c) any alternative Bids; and

(d) the presence or absence of a Bid Security or a Bid-Securing Declaration.

26.9. The Bidders' representatives who are present shall be requested to sign the record. The omission of a Bidder'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 Bidders.

E. EVALUATION AND COMPARISON OF BIDS

27. Confidentiality   27.1. Information relating to the evaluation of Bids and recommendation of contract award, shall not be disclosed to Bidders or any other persons not officially concerned with the Bidding process until the Notification of Intention to Award the Contract is transmitted to all Bidders in accordance with ITB 42.

27.2.   Any effort by a Bidder to influence the Purchaser in the evaluation of the Bids or Contract award decisions may result in the rejection of its Bid.

27.3.   Notwithstanding ITB 27.2, from the time of Bid opening to the time of Contract award, if any Bidder wishes to contact the Purchaser on any matter related to the Bidding process, it should do so in writing.

28. Clarification of Bids

28.1.   To assist in the examination, evaluation, and comparison of the Bids, and qualification of the Bidders, the Purchaser may, at its discretion, ask any Bidder for a clarification of its Bid. Any clarification submitted by a Bidder 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 Bid shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the Purchaser in the evaluation of the Bids, in accordance with ITB 32.

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

29. Deviations, Reservations, and Omissions

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

(a)   "Deviation" is a departure from the requirements specified in the bidding document;

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

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

30. Determination of Responsiveness

30.1.   The Purchaser's determination of a Bid's responsiveness is to be based on the contents of the Bid itself, as defined in ITB 11.

30.2.   A substantially responsive Bid is one that meets the requirements of the bidding 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 Information System specified in the Contract; or

(ii)   limit in any substantial way, inconsistent with the bidding document, the Purchaser's rights or the Bidder's obligations under the proposed Contract; or

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

30.3.   The Purchaser shall examine the technical aspects of the Bid in particular, to confirm that all requirements of Section VII, Purchaser's Requirements have been met without any material deviation, reservation, or omission.

30.4.   To be considered for Contract award, Bidders must have submitted Bids:

(a)   for which detailed Bid evaluation using the same standards for compliance determination as listed in ITB 29 and ITB 30.3 confirms that the Bids are commercially and technically responsive, and include the hardware, Software, related equipment, products, Materials, and other Goods and Services components of the Information System in substantially the full required quantities for the entire Information System or, if allowed in the BDS ITB 35.8, the individual Subsystem, lot or slice Bid on; and are deemed by the Purchaser as commercially and technically responsive; and

(b)   that offer Information Technologies that are proven to perform up to the standards promised in the bid by having successfully passed the performance, benchmark, and/or functionality tests the Purchaser may require, pursuant to ITB 39.3.

31. Nonmaterial Nonconformities

31.1.   Provided that a Bid is substantially responsive, the Purchaser may waive any nonconformity in the Bid that does not constitute a material deviation, reservation or omission.

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

31.3.   Provided that a Bid is substantially responsive, the Purchaser shall rectify quantifiable nonmaterial nonconformities related to the Bid Price. To this effect, the Bid 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 Bidders. If the price of the item or component cannot be derived from the price of other substantially responsive Bids, the Purchaser shall use its best estimate.

32. Correction of Arithmetical Errors

32.1.   Provided that the Bid is substantially responsive, 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.

32.2.   A Bidder shall be requested to accept the correction of arithmetical errors. Failure to accept the correction in accordance with ITB 32.1 shall result in the rejection of the Bid.

33. Conversion to Single Currency

33.1.   For evaluation and comparison purposes, the currency(ies) of the Bid shall be converted into a single currency as specified in the BDS.

34. Margin of Preference	34.1. No margin of domestic preference shall apply.

35. Evaluation of Bids

35.1. The Purchaser shall use the criteria and methodologies listed in this ITB and Section III, Evaluation and Qualification criteria. No other evaluation criteria or methodologies shall be permitted. By applying the criteria and methodologies the Purchaser shall determine the Most Advantageous Bid.

Preliminary Examination

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

Technical Evaluation

35.3. The Purchaser will examine the information supplied by the Bidders Pursuant to ITB 11 and ITB 16, and in response to other requirements in the Bidding document, taking into account the following factors:

    (a) overall completeness and compliance with the Technical Requirements; and deviations from the Technical Requirements;

    (b) suitability of the Information System offered in relation to the conditions prevailing at the site; and the suitability of the implementation and other services proposed, as described in the Preliminary Project Plan included in the bid;

    (c) achievement of specified performance criteria by the Information System;

    (d) compliance with the time schedule called for by the Implementation Schedule and any alternative time schedules offered by Bidders, as evidenced by a milestone schedule provided in the Preliminary Project Plan included in the bid;

(e)   type, quantity, quality, and long-term availability of maintenance services and of any critical consumable items necessary for the operation of the Information System;

(f)   any other relevant technical factors that the Purchaser deems necessary or prudent to take into consideration;

(g)   any proposed deviations in the bid to the contractual and technical provisions stipulated in the bidding documents.

35.4.   If specified in the BDS, the Purchaser's evaluation of responsive Bids will take into account technical factors, in addition to cost factors. The scores to be given to technical factors and sub factors, and the weights to be assigned for the technical factors and cost are specified in the BDS. An Evaluated Bid Score (B) will be calculated for each responsive Bid using the formula, specified in Section III, Evaluation and Qualification Criteria, which permits a comprehensive assessment of the Bid cost and the technical merits of each Bid.

35.5.   Where alternative technical solutions have been allowed in accordance with ITB 13, and offered by the Bidder, the Purchaser will make a similar evaluation of the alternatives. Where alternatives have not been allowed but have been offered, they shall be ignored.

Economic Evaluation

35.6.   To evaluate a Bid, the Purchaser shall consider the following:

(a)   the Bid 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 ITB 32.1;

(c)   price adjustment due to discounts offered in accordance with ITB 26.8;

(d)   converting the amount resulting from applying (a) to (c) above, if relevant, to a single currency in accordance with ITB 33; and

(e)   price adjustment due to quantifiable nonmaterial nonconformities in accordance with ITB 31.3;

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

35.7.   If price adjustment is allowed in accordance with ITB 17.9, the estimated effect of the price adjustment provisions of the

Conditions of Contract, applied over the period of execution of the Contract, shall not be taken into account in Bid evaluation.

35.8.   The Purchaser will evaluate and compare the Bids that have been determined to be substantially responsive, pursuant to ITB 30. The evaluation will be performed assuming either that:

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

(b)   if specified **in the BDS**, Contracts will be awarded to the Bidders for each individual Subsystem, lot, or slice defined in the Technical Requirements whose Bids result in the Most Advantageous Bid/Bids for the entire System.

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

36. Comparison of Bids

36.1.   The Purchaser shall compare all substantially responsive Bids in accordance with ITB 35.6 to determine the lowest evaluated cost.

37. Abnormally Low Bids

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

37.2.   In the event of identification of a potentially Abnormally Low Bid, the Purchaser shall seek written clarifications from the Bidder, including detailed price analyses of its Bid 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 bidding document.

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

38. Unbalanced or Front Loaded Bids

38.1.   If the Bid that is evaluated as the lowest evaluated cost is, in the Purchaser's opinion, seriously unbalanced or front loaded the Purchaser may require the Bidder to provide written clarifications. Clarifications may include detailed price analyses to demonstrate the consistency of the Bid prices with the scope of information systems, installations, proposed

methodology, schedule and any other requirements of the bidding document.

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

(a) accept the Bid; or

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

(c) reject the Bid.

39. Eligibility and Qualification of the Bidder

39.1. The Purchaser shall determine to its satisfaction whether the Bidder that is selected as having submitted the lowest evaluated and substantially responsive Bid is eligible and meets the qualifying criteria specified in Section III, Evaluation and Qualification Criteria.

39.2. The determination shall be based upon an examination of the documentary evidence of the Bidder's qualifications submitted by the Bidder, pursuant to ITB 15, as well as other information the Purchaser deems necessary and appropriate. This determination may include visits or interviews with the Bidder's clients referenced in its bid and site inspections.

39.3. Prior to Contract award, the Purchaser will verify that the successful Bidder (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 Bidder. If any proposed subcontractor does not meet the requirement, the Purchaser will require the Bidder to propose a replacement subcontractor.

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

39.5. An affirmative determination shall be a prerequisite for award of the Contract to the Bidder. A negative determination shall result in disqualification of the Bid, in which event the Purchaser shall proceed to the next lowest evaluated cost or best evaluated Bid, as the case may be, to make a similar

determination of that Bidder's qualifications to perform satisfactorily.

39.6. The capabilities of the manufacturers and subcontractors proposed by the Bidder that is determined to have offered the Most Advantageous Bid 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 Bid will not be rejected, but the Bidder will be required to substitute an acceptable manufacturer or subcontractor without any change to the Bid 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 Bid, and to Reject Any or All Bids

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

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 ITB 46. The Standstill Period commences the day after the date the Purchaser has transmitted to each Bidder the Notification of Intention to Award the Contract. Where only one Bid 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 Bidder the Notification of Intention to Award the Contract to the successful Bidder. The Notification of Intention to Award shall contain, at a minimum, the following information:

(a) the name and address of the Bidder submitting the successful Bid;

(b) the Contract price of the successful Bid;

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

(d)   the names of all Bidders who submitted Bids, and their Bid prices as readout and as evaluated prices and technical scores (if applicable);

(e)   a statement of the reason(s) the Bid (of the unsuccessful Bidder 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;

F. AWARD OF CONTRACT

43. Award Criteria   43.1.   Subject to ITB 40, the Purchaser shall award the Contract to the successful Bidder. This is the Bidder whose Bid has been determined to be the Most Advantageous Bid. The determination of the Most Advantageous Bid will be made in accordance to one of the two options as defined in the BDS. The methodology options are:

(a) when **rated criteria are used**: The Bidder that meets the qualification criteria and whose Bid:

(i) is substantially responsive; and

(ii) is the best evaluated Bid (i.e. the Bid with the highest combined technical/quality/price score); or

(b) when **rated criteria are not used**: The Bidder that meets the qualification criteria and whose Bid has been determined to be:

(i) substantially responsive to the bidding document; and

(ii) the lowest evaluated cost.

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 BDS.

45. Notification of Award

45.1.   Prior to the date of expiry of the Bid validity and upon expiry of the Standstill Period, specified in ITB 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 Bidder, in writing, that its Bid 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 Bidders that submitted Bids, and their Bid prices as read out at Bid opening, and as evaluated;

(d)   name of Bidders whose Bids were rejected and the reasons for their rejection;

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

(f)   successful Bidder's Beneficial Ownership Disclosure Form, if specified in BDS ITB 47.1.

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 ITB 42, an unsuccessful Bidder 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 Bidders 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 Bidders 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 Bidders may be done in writing or verbally. The Bidder shall bear their own costs of attending such a debriefing meeting.

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

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

47.3.   Notwithstanding ITB 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 Bidder shall not be bound by its Bid, always provided, however, that the Bidder 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 Bidder in completing any formalities, including applying for

permits, authorizations and licenses necessary for the export of the Information System under the terms of the Contract.

48. Performance Security

48.1. Within twenty-eight (28) days of the receipt of the Letter of Acceptance from the Purchaser, the successful Bidder shall furnish the performance security in accordance with the General Conditions, subject to ITB 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 Bidder is in the form of a bond, it shall be issued by a bonding or insurance company that has been determined by the successful Bidder 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 Bidder 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 Bid Security. In that event the Purchaser may award the Contract to the Bidder offering the next Most Advantageous Bid.

49. Adjudicator

49.1. Unless the BDS states otherwise, the Purchaser proposes that the person named in the BDS 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 BDS. The proposed hourly fee for the Adjudicator is specified in the BDS.   The expenses that would be considered reimbursable to the Adjudicator are also specified in the BDS. If a Bidder does not accept the Adjudicator proposed by the Purchaser, it should state its non-acceptance in its Bid Form and make a counterproposal of an Adjudicator and an hourly fee, attaching a résumé of the alternative. If the successful Bidder and the Adjudicator nominated in the BDS 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 BDS and propose a new one. If by the day the Contract is signed, the Purchaser and the successful Bidder have not agreed on the appointment of the Adjudicator, the Adjudicator shall be appointed, at the request of either party, by the Appointing Authority specified in the SCC clause relating to GCC Clause 43.1.4, or if no

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

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

SECTION II - BID DATA SHEET (BDS)

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

ITB Reference	A. General
ITB 1.1	The reference number of the Request for Bids is: **KE-ICTA-458650-NC-RFB**
	The Purchaser is: **The Information and Communications Technology Authority**
	The name of the RFB is: **Provision of Automation Services for Selected Ministries, Departments & Agencies**
	LOT 1: Data Management Information System for Office of the Data Protection Commissioner
	LOT 2: Case Management System, Legislative Drafting Information Management System, & Legal Opinion System for Office of the Attorney General
	LOT 3: Correctional Services Management Information System for State Department for Correctional Services
	The Purchaser **shall** accept bids for multiple lots under this bidding document.
	The lots are:
	LOT 1: Data Management Information System for Office of the Data Protection Commissioner
	LOT 2: Case Management System, Legislative Drafting Information Management System, & Legal Opinion System for Office of the Attorney General
	LOT 3: Correctional Services Management Information System for State Department for Correctional Services
ITB 1.3 (a)	Electronic Procurement **shall not** be applicable to this procurement.
	The Purchaser shall use the following electronic-procurement system to manage this procurement process: **Not Applicable**
	The electronic-procurement system shall be used to manage the following aspects of the Procurement process: **Not Applicable**

ITB 2.1	The Borrower is: **The Government of Kenya, through the ICT Authority, which is the implementing agency**. Loan or Financing Agreement amount: **USD 390 Million** The name of the Project is: **Kenya Digital Economy Acceleration Project**
ITB 4.1	Maximum number of members in the JV shall be: **2**
ITB 4.5	A list of debarred firms and individuals is available on the Bank's external website: http://www.worldbank.org/debarr.

B. Bidding Document

ITB 7.1	For **Clarification of Bid purposes** only, the Employer's address is: Attention: **Deputy Director, Supply Chain Management** Address: **P.O. Box 27150-00100** Floor/ Room number*:* **12th Floor, Telposta Towers** City: **Nairobi** ZIP Code: **Not Applicable** 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** Web page: **www.icta.go.ke/tenders OR www.tenders.go.ke**
ITB 7.1	Web page: Web page: **www.icta.go.ke/tenders** OR www.**tenders.go.ke**
ITB 7.4	A Pre-Bid meeting **SHALL** take place on the following date, time, and place: Virtually Via Teams, or Jitsu, or Google Meet Date: 22nd July 2025 Time: 10.30 EAT. Place: Virtually. Bidders interested to participate in the pre-bid meeting may please send their requests to the email mentioned in ITB 7.1 for sending them the link for the meeting.

C. Preparation of Bids

ITB 10.1	The language of the Bid is: **English**
	All correspondence exchange shall be in **English** language.
	Language for translation of supporting documents and printed literature is **English**
ITB 11.1 (k)	The Bidder shall submit with its Bid the following additional documents:
	The additional documents shall include the following:
	Code of Conduct for Supplier's Personnel (ES)
	The Bidder shall submit its Code of Conduct that will apply to the Supplier's Personnel (as defined in GCC sub-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 Bidder 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 Bidder may introduce additional requirements, including as necessary to take into account specific Contract issues/risks.
	Management Strategies and Implementation Plans (MSIP) to manage the (ESHS) risks
	The Bidder shall submit Management Strategies and Implementation Plans (MSIPs) to manage the following key Environmental Social, Health and Safety (ESHS) risks:
	- Environmental concerns including increased e-waste generation and energy consumption concerns
	- Social, Occupational, Health and Safety risks including potential for GBV/ SEA/ SH, gender discrimination at work and exposure to poor working conditions.
	Key Management Strategies and Implementation Plans (MSIP)
	Occupational Health and Safety Management Plan
	Establish safe working conditions and procedures for all personnel.
	Regular training on health and safety practices and emergency response.
	Monitoring and enforcement of compliance with health and safety regulations.
	Establish systems of prevention of cyberbullying
	Accident Management Protocol
	Procedures for incident reporting, investigation, and corrective actions.
	First-aid training for staff and provision of necessary medical supplies.

Clear communication channels for emergency situations.

Waste Management Plan

Strategies for the collection, storage, recycling, and disposal of e-waste.

Identification and management of hazardous materials and electronic components.

Compliance with local and international e-waste regulations.

Energy Management Plan

Strategies to minimize energy consumption during operation and installation.

Consideration of renewable energy sources where feasible.

Regular audits of energy use and efficiency measures.

Anti-discrimination and Diversity Policy

Initiatives to promote diversity and inclusion in the workplace.

Training on discrimination prevention for all employees.

Reporting mechanisms for discrimination or harassment incidents.

Gender-Based Violence (GBV) Prevention Framework

Education and training programs focused on preventing GBV, SEA, and sexual harassment.

Creation of confidential reporting systems for victims.

Collaboration with local organizations for outreach and support services.

HIV and AIDS Prevention and Control Plan

Workplace education programs about HIV/AIDS and other STIs.

Access to testing and counseling services for employees.

Confidential support networks for affected individuals.

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.

	Emergency Response Preparedness Plan Develop emergency response protocols for natural disasters and accidents. Regular drills and training for all staff on emergency procedures. Establishment of communication plans to inform stakeholders during emergencies. **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. **Monitoring and Evaluation Plan** 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.
ITB 13.1	**Alternative Bids are not permitted**
ITB 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.
ITB 13.4	Alternative technical solutions shall be permitted for the following parts of the Information System: **None.**
ITB 15.2	Prequalification **has not** been undertaken.
ITB 16.2 (a)	In addition to the topics described in ITB Clause 16.2 (a), the Preliminary Project Plan must address the following topics: (i) *Project Organization and Management Sub-Plan, including management authorities, responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format);* (ii) *Implementation Sub-Plan;* (iii) *Training Sub-Plan;* (iv) *Testing and Quality Assurance Sub-Plan;*

	(v) *Warranty Defect Repair and Technical Support Service Sub-Plan*
ITB 16.3	In the interest of effective integration, cost-effective technical support, and reduced re-training and staffing costs, Bidders shall offer the following items: **None**
ITB 17.2	The Bidder **must** bid for Recurrent Cost Items
ITB 17.2	The Bidder **must not** bid for contracts for Recurrent Cost Items not included in the main Contract.
ITB 17.5	The Incoterms edition is: **Incoterms 2020**.
ITB 17.5 (a)	Named place of destination is: **Lot 1 – Office of Data Protection Commissioner** **Lot 2 – Office of Attorney General and Department of Justice** **Lot 3 – State Department for Correctional Services**
ITB 17.6	Named place of final destination (or Project site) is: **Lot 1 – Office of Data Protection Commissioner** **Lot 2 – Office of Attorney General and Department of Justice** **Lot 3 – State Department for Correctional Services**
ITB 17.8	ITB 17.8 is modified as follows: **There are no modifications to ITB 17.8**
ITB 17.9	The prices quoted by the Bidder **shall not** be subject to adjustment during the performance of the Contract.
ITB 18.1	The Bidder **is** required to quote in the currency of the Purchaser's Country the portion of the Bid price that corresponds to expenditures incurred in that currency.
ITB 19.1	The Bid shall be valid until: **15th December 2025**
ITB 19.3 (a)	The Bid price shall be adjusted by the following factor(s): **Not Applicable**
ITB 20.1	A Bid Security **shall be** required. A Bid-Securing Declaration **shall not be** required. The amount and currency of the Bid Security shall be:

	(i) **Kes. 1 Million (Kenya Shillings One Million) for LOT 1** or equivalent in a freely convertible currency,
	(ii) Kes. 2.5 Million (Kenya Shillings Two Million, Five Hundred Thousand) for LOT 2 or equivalent in a freely convertible currency &
	*(iii)***Kes. 1 Million (Kenya Shillings One Million) for LOT 3** or equivalent in a freely convertible currency
ITB 20.3 (d)	Other types of acceptable securities: **None**
ITB 21.1	In addition to the original of the Bid, the number of copies is: **One (1) hard copy and One (1) Digital Copy in USB Drive.**
ITB 21.3	The written confirmation of authorization to sign on behalf of the Bidder shall consist of: **Power of Attorney**
D. Submission and Opening of Bids	
ITB 23.1	For **Bid submission purposes** only, the Purchaser's address is: Attention: **Chief Executive Officer** Street Address: **Telposta Towers, Kenyatta Avenue** Floor/ Room number: **12th Floor, Boardroom** City: **Nairobi** ZIP/Postal Code: **Not Applicable** Country: **Kenya** The deadline for Bid submission is: Date: **14th August 2025** Time: **1000 Hours EAT**
ITB 23.1	Bidders **shall not** have the option of submitting their Bids electronically. The electronic Bidding submission procedures shall be: **Not Applicable**
ITB 26.1	The Bid opening shall take place at: Street Address: **Telposta Towers, Kenyatta Avenue** Floor/ Room number: **12th Floor, Boardroom** City: **Nairobi** Country: **Kenya** Date: **14th August 2025**

	Time: **1000 Hrs. EAT**
ITB 26.1	The electronic Bid opening procedures shall be: **Not Applicable**
ITB 26.6	The Letter of Bid and the Price Schedules shall be initialed by representatives of the Purchaser attending Bid opening

E. Evaluation, and Comparison of Bids

ITB 33.1	The currency(ies) of the Bid shall be converted into a single currency as follows: **Kenya Shillings**
	The currency that shall be used for Bid evaluation and comparison purposes to convert all Bid 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: **Bid Submission Deadline**
ITB 35.4	The Purchaser's evaluation of responsive Bids **will take** into account scored technical factors, in addition to cost factors.
	The technical factors (sub-factors) and the corresponding weight out of 100% are:

Technical Factor	Weight in percentage

1.   Experience of the Firm
 	
 The firm should provide at least three (3) references **(whether in the private or Public Sector Agencies)** where they have undertaken assignments of similar nature and complexity in the last 7 years. Details of these assignments, including client names and addresses, scope, value, and duration, must be provided.
 	
 For each project, Enclose the relevant **Documentary proof that includes the following:**
 	
 Copies of Purchase Order / Work Order/contract
 	
     a.   Completion Certificate
     b.   Recommendation Letters
	40

2. Work Plan a) The bidder should provide a logical, well-structured work plan	10

	consistent with the time frames and terms of reference of this RFB to demonstrate understanding of the specifications b) The bidder should provide Technical approach, support and Methodology including proposed concept design of carrying out the Assignment. Provide a detailed implementation methodology indicating the following, as a minimum: 1 Tentative project plan 2 Project organization 3 Project Management Methodology 4 System architecture 5 Training and knowledge transfer plan 6 Test plan 7 Integration strategy 8 post GO-LIVE support strategy clearly indicating what is in scope and what shall be out of scope and how out of scope items shall be handled 9 Proposed support and maintenance plan 10 Sample Service Level Agreement document 11 Warranty The bidder should provide a warranty that the solution provided will perform satisfactorily as per requirements mentioned in the specification during implementation, operation and maintenance period c) The workplan should have a training plan to demonstrate ability to carry out the services under this assignment as per (training module 8.2 and 12.0 for lot 1, lot 2 and 3 respectively)	
	3. <u>Service Level Agreement</u> Bidder to provide a dully filled SLA document with clear escalation matrix and procedures.	5

	4. <u>Key Technical Experts</u>
	  A. Project Manager
	
	  I. A minimum of Masters in Computer Science, Engineering, IT or related degree
	 II. He should have a minimum of 5 years of experience in the Management of IT Projects
	III. Professional experience in developing, implementing and
		10

	managing scalable systems with competencies in systems and information management and IT in general. Give a minimum of 2 projects. IV. ICT-related certification, PRINCE2/PMI /PMP or other equivalent project management certifications	
	B. System designer and developer/System Engineer I. B.SC/ in Computer Science, Engineering or related degree II. Have relevant certifications in systems development e.g. expert system engineering professional (ESEP), certified system engineering professional (CSEP), etc. or have relevant certification in the area of web-based systems and certification in various Programming software and databases e.g. C, C++, ORACLE, MYSQL etc. III. 4+ years of experience in ICT system design, development and implementation with a bias on database management. Give a minimum of 2 projects.	7
	C. Security expert I. B.SC/ in Computer Science, Engineering or related degree II. Have relevant certifications in the area of system security III. 4+ years of experience in the ICT security field and should have experience in ICT systems security and design, development, and Implementation of security solutions. Give reference a minimum of four projects	5
	D. Database Administrator I. B.SC/ in Computer Science, Engineering or related degree II. Have relevant certifications in Database administration e.g. Oracle, SAP, Microsoft SQL Database administrator, etc. and have relevant certification in the area of web-based systems and certification in various Programming software e.g. C, C++, ORACLE, MYSQL, the area	6

	III. 4+ years of experience in ICT database administration, development and implementation. Give a minimum of four projects	
	E. System Integrator I. B.Sc. in computer science/IT or relevant field and have relevant certifications in the area of ICT infrastructure (e.g. networks. Hardware etc.) II. (4+ Years) experience in integrating and deploying systems of diverse technologies. Experience in installing, maintaining and upgrading integrated systems, Give reference of 3 projects III. Have relevant certifications in systems Integration, Records Management and Certified Workflow designer	6
	F. Webmaster (designer and developer) and Mobile Application I. B.Sc. in computer science/IT or relevant field II. Certifications in website development/graphic design/mobile applications tools III. Experience: Give reference of 3 projects where the person has designed	6
	G. Quality Assurance Expert I. At least 8 years of experience in designing, developing and maintaining test cases and strategies for testing and quality assurance. II. A Bachelor's Degree in IT or related. (Information System, Computer Science, Computer Engineering, Software Engineering e.tc) III. Give reference of a minimum of 3 projects undertaken in the last 8 years IV. Professional Certifications in system quality assurance. (Certified quality engineer, certified quality auditor, Certified Test Engineer (CSTE) Certified	5

Software Quality Analyst (CSQA), Certified Associate in Software Testing (CAST), CMSQ (Certified Manager of Software Quality (attach certificate)		
Note: The bidder must attach Curriculum Vitae and copies of Certificates for all the Key Technical Team		
TOTAL	**100**	

The technical proposal scoring methodology is specified in Section III-Evaluation and Qualification Criteria. Bidders must meet the mandatory technical evaluation criteria for the offered system before being assessed for the technical factors.

Technical evaluation criteria for assessing conformance of the offered system to the Purchaser's technical requirements/specifications

LOT 1: Data Management Information System for Office of the Data Protection Commissioner

S/N	Requirement	Description	Bidder's Response (YES/NO)
1.	**Registration Module**	A client facing web-based system to enable data controllers and processors register in line with the data protection act ,2019 and the attendant regulations.	
		Platform for generating and publishing a list of registered data controllers and processors on the website in conformity with the regulations (14. (1) and subject to section 21 of the Act.	
		Dashboard for tracking applications and their statuses in line with the act and the ODPC service charter.	
		Provision for revocation of an entity's certificate of registration and automatic cancellation from the record and the register upon revocation.	
		Provision for change or variation of registrations.	

			Integration with BRS system for validation and due diligence of both local and foreign companies operating in Kenya during registration	
			Backend for review of applications, approvals as per the defined workflows and policies.	
			Provision for renewal of certificates prior or upon expiry.	
			Emails and SMSs integrations for push of notifications and reminders on action items relating to registrations.	
			Auto generation of certificate for printing upon approval.	
			Withdrawal of an application	
			Categorization of application based on the counties, regions and the defined approval matrix.	
			Inclusion of a ticketing module linked to ODPC call center to ensure tracking and timely resolution of registration requests.	
			Integration with the existing systems and the approved payment platforms & gateways which include but not limited to paybills and bank to ensure efficiency in payment of registration fees.	
			Provision for querying and validation of a certificate.	
	2.	**Data breach Module**	Creation of a data breach reporting module on the system.	
			Mapping of reported data breaches for actions as per the defined user roles and matrices.	
			Tracking of data breaches and their respective statuses.	
	3.	**Compliance Module**	Creation of a Data Privacy Impact Assessment (DPIA) module in line with the requirements.	
			A sub module for submission and approval of a data transfer request.	
			Provision for making requests for data protection advisories and tracking of advisories issued by the office.	

			Submission of Data Protection Impact Assessments.	
			Emails and SMSs integrations for acknowledge receipt of Data Breach Notifications, advisory request, cross border transfer requests and DPIAs.	
	4.	**Data Audits Module**	Provision for data audit planning and reporting on the number of audits performed.	
			Randomized selection of entities to audit based on registration details (including sector, size, safeguards, etc.)	
			Provision for sending notifications/reports of data audits to controllers/processors	
	5.	**Quality Assurance Certification Module**	Provision for a module for offer/issuance of certification of data protection seals and marks to encourage data protection compliance by controllers and processors.	
	6.	**Complaints, Investigation and Enforcement Module**	End to end complaints module to enable data subjects lodge complaints and allow internal staff to review the complaints as per the complaints handling procedure.	
			Provision for acknowledgement of a complaint by the office.	
			Provision for preliminary review of a complaint.	
			Notification of a complaint to a respondent.	
			Provision for investigation of a complaint as per the defined procedures.	
			Provision for investigation of a complaint as per the defined procedures.	
			Assignment of tasks to officers and tracking of their statuses.	
			Generation of automated register of complaints and their statuses.	
			Provision for withdrawal of a complaint by a data subject.	
			Discontinuation and notification of the same to the data subject and/or a respondent.	

				Transcription/ Hansard module to take complaints made over the phone through ODPC call center.	
				Automatic assignment of tracking numbers once a complaint has been lodged and if the complaint is against a DP or DC, the complaint can be linked to that that particular entry.	
				Inclusion of the Alternative Dispute Resolution (ADR) mechanisms on to the enforcement sub -modules.	
				Provision for reinstitution of a complaint after a decline/discontinuation.	
				Ability for joint handling of a complaint.	
				Provision for submission of determinations before the enforcement processes.	
				Provision for referral to ODPP for prosecution.	
				Provision for automated summons.	
				Generation of automatic Enforcement registers.	
				Provision for submission of an investigation report for approval.	
				Provision for prompts/alerts/notifications with time-based escalations incorporated in the workflow.	
				Integration with the existing systems and the approved payment platforms & gateways which include but not limited to paybills and bank to ensure efficiency in payments for administrative fines and penalty fees.	
				Application for review of enforcement notice(s) by a data subject.	
				Provision for appeals of determination, enforcement notices and penalty notices.	
				Facilitate issuance of enforcement, penalty notices and administrative fines to data processors and / or controllers.	

	7.	**General Key Features**	Intuitive graphical interface for a short learning curve.	
			Network ready with multi-user password control.	
			Web Based	
			Employee Self Service portal.	
			Email and SMS Integration.	
			Integration with Bank payments- Card, bank Deposits and SWIFT	
			Process Workflow, Alerts and Embedded Document attachment.	
			Reporting	
			Other characteristics of IDMIS	
	8.	**Workflow and Alerts**	Document, content management and intranet	
			Document Access Control	
			Workflow Configuration and Management	
			Alerts and notification on email.	
	9.	**Reporting /Analytics**	Advanced analytics and reporting on the number of breaches received, DPIAs submitted, complaints lodged and timelines for responding and level of compliance with the act and the service charter.	
			Business intelligence capabilities and analytics based on registrations, data breaches, transactions and complaints reports. (Weekly, Monthly, Quarterly, Annual)	
			Ability to generate performance reports based on service delivery.	
			Annual Report to Parliament.	
			Ad-hoc Reports (management reports).	
			Custom Reports and Reporting Services	
			Business Intelligence and Analytics - Integration with other corporate applications generating data	
			Dashboard with Top level Graphical Analytics including forecasting	
	10.		User Setup and Administration	

		System administration module	Provision for automated backups and restore.	
			Security Administration including application of security filters and privileges	
			Help desk	
			Incident reporting, ticketing and support	
			System Administration, Database Management, User Setup and Administration, Roles and access privileges administration, Workflow Configuration and Management	
			Audit Trails, Archiving, Automated backups and Restore, Reporting	
	11.	**Help desk, ticketing and incidents reporting**	Automatically assign tasks to officers and monitor tickets based on the service charter and generate tickets for each task.	
			Tracking of workflows and escalation matrix of tasks to ensure compliance and adherence to legal time lines.	
			Integration with call center services for timely resolution of enquiries as per the act and the service charter.	
			A platform for reporting of incidences and tracking of their resolution status.	
			A platform for customer feedback on ODPC services.	
	12.	**Carry out necessary maintenance of as per request**	This include but not limited to: analysis of access logs, error logs and implementation of solutions to found exceptions	
	13.	**Code maintenance and upgrade on security management**	This include but not limited to: fine tuning of system errors, closure of any existing bugs and security loopholes. The bidder shall carry out proactive security updates and batching.	
	14.	**Security management and audit trail**	System security and application administration, Audit Trails & archival of logs and	
	15.	**System restoration**	The bidder shall in collaboration with OPDC will ensure the IDMIS's backups are up to date and are able to restore the	

			IDMIS System in case of failure/hacking.	
	16	**Availability**	The system has to be accessible 24 hours a day, 7 days a week from any part of the world with minimum if not zero downtime (99.9% availability).	
	17.	**Search Functionality**	The vendor should implement a seamless search functionality to enable users to easily filter and search contents. The contracted vendor will ensure the Search Engine Optimization (SEO).	
	18.	**Privacy**	The system should ensure seamless user experience while ensuring security and privacy of information collected in line with the Data Protection Act, 2019 & Data protection Regulations, 2022	
	19.	**Vulnerability Assessment**	The Vendor should perform a vulnerability assessment and submit a report for independent verifications by ODPC.	
	20.	**Licenses and software's**	The Vendor should build and implement the IDMIS System on the latest platforms, technologies and software's	
	21.	**General**	Review testing results for compliance with policies, procedures, plans,and metrics (e.g. defect rates, progress against schedule, etc.). Correct defects identified during the testing efforts. Prepare application(s)/module(s) for migration into INPRS production environment.	
	22.	**Unit Testing:**	The vendor will carry out the unit testing in house to make sure each component and module of the system functions as designed.	
	23.	**Integration Testing:**	After all modules of the system are developed, integration testing is carried out to make sure that all modules function and perform as expected when working in combination.	
	24.	**Load testing:**	Since the application will be used by a large number of users in future, load testing will be performed to see how the	

		system performs under heavy loads. This may require fine tuning the web server, application, application server, and/or the database server or network configuration and load balancing.	
25.	**Recovery Testing:**	One of the important aspects of an application is how well it can recover in case of a system failure, server shutdown, or service failure. Tests will be carried out to see how well the system recovers from crashes and hardware failures.	
26.	**Security Testing**	it is necessary to perform detailed security testing of the system. This involves a complete penetration test to make sure the application and the server is not vulnerable to any type of attacks such as SQL injection attack, XSS attacks etc. This will be done by using threat detection and vulnerability scanner software	
27.	**Usability Testing**	The client will test the navigation between screens, user-friendliness and workflows of each of the screens. Against this, if deficiencies are identified the interface maybe redesigned during this testing Stage based on feedback from the Client.	
28.	**Functional Testing:**	A complete end to end functional testing cycle will run. During the functional test, actual processes, and all key services provided by system will be tested against the business requirement, (end to end) to see if the system meets the requirements as described in the in the RFP document and stores data and generate reports properly.	
29.	**Acceptance Testing**	An end to end functional and quality of service testing (including security, performance and robustness) will be performed by the Ministry before any system sign off.	

	30.	**UAT Test Script**	An end to end user functional and quality of service testing will be performed by the Ministry prior to any system sign off.	
	31.	**Rollout**	It is anticipated that this project may be carried out in phases across in an initial period of one-year period with additional support of at least two years. ODPC shall plan with the successful bidder on the roll-out of the proposed solution based on priority and professional opinion.	
	32.	**Data migration**	Bidders are required to create and submit a detailed technical proposal and duration for Data migration and conversion requirements from the existing IDMIS to the new system that contain all the necessary deliverables that the bidder will follow to ensure smooth phased migration.	
	33.	**Detailed Implementation Schedule**	Provide a detailed implementation schedule detailing.	
			the number of ODPC staff required to facilitate timely project delivery services and material critical for the successful project implementation. Highlight the critical milestones that are expected during project implementation with the approach to be taken for a successful and timely project implementation.	
			the number of your staff required for timely project delivery	
	34.	**Post implementation stabilization**	Bidder shall provide Product support after going live, as a part of this project by deputing technical and functional consultants at site for not less than six months after implementation.	
			During the stabilization period the bidder would help the ODPC to correct any troubleshooting while doing transactions or generating reports. The bidder will correct the user manuals and configuration manuals if required.	

| | 35. | **Hardware Specifications** | Bidders should provide advice to the ODPC in the scoping of hardware requirements to be provisioned for implementation of IDMIS solution | |
| | 36. | **Copyright and Intellectual Property** | copyright of the entire system and its components developed by the vendor under this tender will belong to ODPC and should form part of deliverables to be handed over and this shall be covered under an escrow agreement. | |

LOT 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for Office of the Attorney General

Module 1: Legal Case Management System (LCMS)

The bidder must meet or exceed the following technical and functional requirements for the **Legal Case Management System.**

Category	Details	Conformity (Yes/No)
Case Management	Track case files, organize evidence, manage case timelines, and provide real-time case updates.	
Client and Contact Management	Manage client interactions, external counsel details, and communication records.	
Document Management	Secure storage, advanced search functionalities, version control, document automation, and e-signature support.	
Task and Workflow Management	Assign tasks, monitor workflow progression, set reminders, and ensure seamless collaboration.	
Reporting and Analytics	Generate insights on case durations, outcomes, productivity, and task completion rates.	
Dashboard Overview	The system must provide a comprehensive dashboard that displays an overview of all cases, clients, lawyers/firms, trials, evidence, invoiced amounts, and other relevant case metrics.	

		Filtering & Search	The dashboard must allow filters based on case types, regions, case statuses, and other relevant parameters to enable efficient data retrieval.	
		Remote & Desktop Access	The system should allow users to organize and manage cases remotely through a web-based interface and on desktop applications.	
		Matter & Contact Linkage	The solution should link all contacts, tasks, and other case-related elements to their respective matters, e.g., linking witness contacts and parties' contacts to the case file.	
		Cause of Action Tracking	The system must support a Cause of Action feature, allowing the clear categorization of cases such as land disputes, labor cases, contracts, criminal matters, etc. This will help in tracking trends, preparing reports, and conducting legal research.	
		Notes & Reminders	The system must support sticky notes, reminders, and personal notes that can be sent to self or staff members as needed for efficient case tracking and follow-ups.	
		Virtual Tags & Trial Stickers	The bidder must ensure the system provides virtual tags, stickers, and notes for trial preparation, making it easy for staff to find relevant information quickly.	
		Research & Authorities Integration	The system should have a Legal Research Element, allowing users to attach lists of authorities and relevant research to specific matters. It should also integrate with electronic legal research databases (e.g., LexisNexis, Thomas Legal, etc.) for effective legal reference.	
		Legal Research Library	A centralized Legal Research Library must be provided, allowing users to create, store, and attach legal research materials to case matters.	
		Precedent Setting Cases	The system must flag precedent-setting cases and key case authorities to help in legal decision-making and argument preparation.	
		Judgment, Liabilities & Award Logs	The system must maintain records of judgments, liabilities, and financial awards, logging the date, amount, and responsible parties. If employees are found liable, the	

		system should track surcharges and recovery of funds.	
	Case Timeline & Audit Trail	The solution should track all case developments with a detailed timeline, showing who made what changes and when. Users must be able to see new time entries, document uploads, and other case updates in real time.	
	User Accessibility & Mobility	The system must allow secure access to case files, tasks, and relevant information from anywhere, at any time, ensuring seamless remote and on-premises work.	
	Security & Compliance	The bidder must ensure that the system complies with relevant data protection laws and includes security features such as role-based access control, audit logs, and encrypted communications.	
	Calendar		
		Track ongoing matters in individual and departmental wide dashboards.	
		Case alerts to enable users to be updated with court deadlines and other statutory deadlines.	
		Set reminders	
		Multiple notifications on different issues including case progress, case milestones, meetings, court dates etc.	
	Client Management		
		Easily organize contact details, documents, and communication logs from file opening to closure.	
		Track office interactions with—clients, companies, outside counsel, witnesses, etc.	
		Communication – track and manage client and office letters, emails and other forms of communication	
	Client portal	Enable clients and witnesses to communicate and collaborate with the State Counsel, provide witness statements, replying affidavits, responses and documents once mapped for a particular matter.	

	Status Update	Clients should have access to real-time case status updates as mapped.	
	Security	Files should be able to be stored and backed-up both on premise and offsite.	
		Compliance with local and international data protection laws (e.g., Data Protection Act of Kenya, EU GDPR) to ensure privacy for clients and case data.	
	Document management	Access to documents from anywhere.	
		Securely access, edit, and store your case files from anywhere with legal document software (case management system).	
	Permissions Control	The bidder shall demonstrate the implementation of user access management, including controls to regulate who can view, edit, and modify documents. The solution should support configurable permission settings to enforce access restrictions as required.	
	Advanced Search	Documents should be easily searchable either using keywords, clients, file reference, word, pdf and any other word processing document.	
		Conflict search enabled using broad search terms such as subject matter, title, text content, or parties.	
		Metadata search enabled (e.g. The size of the document, time it was created, author etc.)	
		Ability to sort files by different categories e.g. department, parties, authors, dates, subject matter expandable.	
	Version Control	· The system must allow tracking of previous and updated versions of documents. · Must support "Track Changes" functionality similar to MS Word for document edits and updates.	
	Document automation tools	a) Automatically create letters and other key documents from predesigned templates (the Users will detail the design).	b)
		b) Automate routine legal documents e.g. memorandum of appearance.	

		c) Auto-fill and generate court returns and documents with pre-populated and synced data thus reducing risks of errors when completing forms.	
		d) Convert existing Word files into reusable online templates.	
	Electronic Signatures	The system must support electronic signing of legal documents.	
		a) Ensure that electronically signed documents are legally binding and admissible in court, meeting all jurisdictional requirements.	
		b) Implement security measures to safeguard electronically signed documents from unauthorized access or tampering.	
		c) Support access to electronically signed documents from anywhere, enhancing collaboration and efficiency in legal proceedings.	
		d) Ensure compliance with established legal standards and robust security measures for electronic signatures.	
	Task management/ Workflow		
		a) Task allocation	
		b) Review, prepare, and send documents for signature. No need to download, print or scan documents.	
		c) Workflow enabling users to send tasks to the next user as required.	
		d) Allow tracking of task progression	
		e) Calendar editing and setting deadlines on tasks.	
		f) Prioritize and sort tasks depending on urgency and importance.	
		g) Schedule tasks and set reminders for deadlines to ensure that critical tasks are not overlooked and deadlines are met.	
		h) Collaborate on legal documents and easily manage documents as a team.	
		i) Create standardized task lists	
		j) Build a series of tasks based on standard operating procedures for the office.	

		k) Pre-define and order timing of pre-trial preparation.	
		l) Set task deadlines, duplicate lists and assign task lists related to particular cases.	
	Integrations	Ability to integrate with other applications used in the office and internationally accepted ones.	
		a) Integrations: Ability to integrate with other applications used in the office and internationally accepted ones.	
		b) Integrations: Ability to integrate with other applications used in the office and internationally accepted ones.	
		c) Integrate with the Kenya Judiciary Case Management System (appropriate name and requirements shall be provided by the Users).	
	Billing and invoice	a) Requests for travel approval and payment of expenses.	
		b) Payment for Court Travel payment etc link accounts with IFMIS and finance department.	
		c) Payment vouchers for clients and cases with decretal awards against the government.	
		d) Track the status of unpaid matters, or add automated interest to late payments as required.	

Module 2: Legal Advisory Database

The bidder must demonstrate the proposed approach for implementing the Legal Advisory Database System.

Clean and Intuitive Interface		Conformity (Yes/No)
Minimalist Design	· Keep the interface clean with minimal clutter. Use neutral colors (e.g., white, gray, and blue) to create a professional look.	
Clear Navigation	· Implement a straightforward navigation system with main categories like "Search Opinions," "Saved Searches," "Recent Opinions," "Submit New Opinion," and "Profile Settings."	

	Breadcrumbs	· Display breadcrumbs to help users easily track their location within the database and navigate back to prior pages.	
	User Dashboard	· A personalized dashboard with quick access to recent searches, most-referenced opinions, and saved opinions should be displayed upon login.	
	c) Advanced Search and Filtering		
	Keyword Search	· Implement a search bar that supports keyword search across metadata (e.g., case name, date, topic, jurisdiction) and full-text search within opinions.	
	Advanced Filters	· Users should be able to filter opinions based on various criteria, such as: ➢ **Date:** (e.g., year of issuance) ➢ **Type of Legal Matter:** (e.g., civil, criminal, administrative) ➢ **Department/Agency:** (e.g., Ministry of Health, Ministry of Finance) ➢ **Attorney General Signature:** (e.g., opinions authored by a specific AG)	
	Boolean Search Operators	· Allow the use of Boolean operators (AND, OR, NOT) for complex search queries.	
	Search Results Sorting	· Results should be sortable by relevance, date, agency, or case type.	
	d) Metadata and Categorization		
	Opinion Metadata:	· Each opinion entry should include metadata such as: ➢ Title of Opinion ➢ Opinion Date ➢ Attorney General (author) ➢ Government Department or Agency involved ➢ Summary of the legal matter ➢ Status (e.g., active, withdrawn, amended)	
	Tagging System	● Allow tagging of opinions with multiple keywords or tags (e.g., "Constitutional Law," "Labor Dispute") to improve categorization and searchability.	

		e) Opinion View and Details Page	
	Structured Format	· Display opinions in a readable, structured format with clear headings (e.g., "Facts," "Legal Questions," "Opinion Conclusion").	
	Downloadable Formats	· Allow users to download opinions in PDF or Word format for offline review or sharing.	
	Cross-Referencing	· Display related opinions or previous precedents within the same page (e.g., "This opinion cites Opinion #123").	
	Version Control	· If opinions have been revised, ensure version history is available, with a clear comparison tool highlighting the changes.	
		f) Collaboration and Notes	
	Comments and Notes	❖ Enable users to add private notes to opinions for future reference, with an option to mark important sections of the document.	
	Collaboration Tools	· Implement collaborative tools (if required) for government attorneys to discuss opinions, share insights, or flag important cases internally.	
		g) Security and Compliance	
	Secure Access	· Implement multi-factor authentication (MFA) to ensure that only authorized personnel can access the system.	
	Data Encryption	· Ensure all legal opinions and associated data are encrypted, both at rest and in transit.	
	Audit Trail	· Keep an audit trail of who accesses and edits opinions to maintain accountability and transparency.	
		h) Mobile-First and Responsive Design	
	Mobile-First Approach	· Ensure that the database is fully responsive and can be accessed on various devices, including mobile phones and tablets, as attorneys may need access on the go.	
	Simplified Mobile UI	· For mobile devices, focus on simplifying the search and opinion retrieval process with fewer on-screen elements and larger buttons for touch input.	

	i) Error Handling and Feedback		
	Clear Error Messages	● Display meaningful error messages if users input incorrect search parameters or if there are system issues.	
	Loading States	● Show a loading indicator when search queries are processing, especially if large datasets are being queried	
	Autosave and Drafts	● For those submitting or editing opinions, auto-save should be enabled to prevent loss of work	
	j) Performance and Speed		
	Fast Search	● The system must be optimized for fast retrieval of documents, even when querying large datasets	
	Pagination or Infinite Scroll	● To handle large search results efficiently, consider using pagination or infinite scroll for result pages.	
	k) Training and Support		
	Help Section	● Provide an easily accessible help section or FAQs with common questions and user guides.	
	Tutorials:	● Onboarding tutorials or tooltips for first-time users explaining key features (e.g., how to filter opinions or save searches).	
	l) Integration with Other Legal Systems		
	● **APIs for Integration**	● The system must be capable of integrating with other government or legal databases, as needed, to ensure seamless data exchange. This includes, but is not limited to, linking with court databases, legal precedent databases, and other relevant legal information sources. The integration should be smooth, secure, and allow for real-time data synchronization and retrieval to enhance the system's functionality and user experience.	
	m) User Feedback and Reporting		
	● **Feedback Mechanism**	● Include a feedback tool for users to report issues, suggest features, or request changes.	

● **Usage Analytics**	● Admins should be able to access usage analytics to understand how the system is being used and optimize it further.	
9. Summary of Salient Features		
The proposed legal advisory database or portal should possess the following salient features:		
Comprehensive indexing	● Implement a robust indexing system to categorize legal advisories by topic, legal issue, date, and other relevant criteria.	
Full-text search	● Allow users to search the full text of legal advisories for efficient retrieval of specific information.	
Advanced search capabilities	● Offer options for filtering search results by date range, issuing department, and other criteria.	
Headnote and summary	● Include clear and concise headnotes and summaries for each legal advisory to provide a quick overview of the key points.	
Internal citations	● Enable easy navigation between interconnected legal advisories through internal citations and links.	
Annotation capabilities	● Allow authorized users to annotate legal advisories for internal reference and knowledge sharing.	
Version control	● Track changes made to legal advisories and maintain a history of all versions for audit purposes.	
Security measures	● Implement robust security measures to restrict unauthorized access and ensure data confidentiality. This may include role-based access control, encryption, and audit logging.	
User roles and permissions	● Establish a user role management system to grant different access levels (e.g., read-only, edit) based on user needs.	
User interface	● Provide a user-friendly and intuitive interface that is easy to navigate and search.	
Accessibility	● Ensure the system complies with accessibility standards to accommodate users with disabilities.	
Reporting tools	● Generate reports on usage statistics, search trends, and other relevant data	

		to inform decision-making and system optimization.	
	Integration capabilities	● Consider potential for future integration with existing OAG&DOJ systems for centralized information management.	
	Mobile	● Compatibility to access the system from mobile devices.	
	Category	**Specifications/Requirements to be Met by the Bidder**	
	Document Upload & Storage	● System should accept uploads of legal advisories in multiple formats (PDF, Word, etc.).	
		● Ability to upload new legal advisories and categorize them based on criteria such as date, subject matter, issuing department, and clients.	
	Metadata & Categorization	● Allow for easy addition of metadata to each legal advisory, including date, subject matter, issuing department, keywords, and case citations.	
	Version Control	● Facilitate version control to track changes made to legal advisories.	
	Access Control & Security	● Implement a secure access control system with user roles and permissions.	
	System Integration	● Capability to integrate with existing Electronic Documents and Records Management Systems (EDRMS) for seamless data transfer.	
	-	● Integrate with existing Office of the Attorney General & Department of Justice (OAG&DOJ) knowledge management systems and Case Management System.	
		● Ability to integrate with other e-repositories locally and internationally recognized (e.g., Lexis Nexis, Kenya Law).	
	Legal Opinion Submission	● An interface for State Counsel in the MDAs to upload their preliminary legal opinions.	
	Collaboration & Annotations	● Ability to add sticky notes and send notes to self or staff as necessary.	

Tagging & Quick Reference	● Implement Virtual Tags and Stickers to enable staff to find relevant information quickly and make User Briefs responsive.	
Research & Legal References	● Research Element: System should allow attachment of List of Authorities and other relevant research to matters.	
	● Legal Research Library: Maintain a user's legal research in one place with other integrated legal research libraries	
	● System must integrate with paid electronic legal research databases (e.g., LexisNexis, Thomas Legal).	
	● Allow users to create legal research globally and attach it to matters to create effective precedents.	

Module 3: **Legislative Drafting Information Management System (LDIMS)**

Functional Requirements/Business Requirements	
1. Bill and Subsidiary Legislation Management:	**Conformity (Yes/No)**
● Register and track requests for legislative drafting from MCDAs.	
● Assign and track tasks to Parliamentary Counsel based on expertise, workload, and type of legislation (Bill or subsidiary legislation).	
● Manage the progress of drafts through various stages (instructions received, research, drafting, review, approval).	
● Track and display information on existing legal acts to be altered or implemented by the draft law or regulation.	

		● Generate detailed feedback loops (e.g., surveys, performance dashboards, and user satisfaction metrics) ● The system should generate a unique reference number for each file recorded, specific to the Offices, Ministries, Agencies, and other Institutions from which the instructions are received.	
		● Compliance Validation: Validate drafts against statutory requirements and legal standards.	
		● Comparisons: See how drafts will change the law in clear details	
		● Links and reference to laws appear as the user is drafting	
		● Access the law in effect as the user is drafting	
		● Identify and alert users to potential conflicts or duplications with the current draft - (by use of Business Intelligence)	
		● Record and manage requests for legal opinions.	
		● Collaboration between Parliamentary Counsels working on the same draft.	
		● Incorporate workflow automation tools (e.g., task assignment, review cycles with built-in approval mechanisms, and automated task progression) to further enhance the legislative drafting process.	
		● Integrate with version control systems to track changes made to drafts.	
		● Integrate robust proofreading tools (e.g., grammar and legal structure checks) to further enhance the quality of legislative drafts	
		● Automated legal proofreading to check for formatting, citation, and statutory compliance to reduce human error.	

		● Maintain a record of revisions and changes made to drafts.	
		● Maintain an archive of finalized Bills and subsidiary legislation.	
		● The system must allow the categorization of files into Bills, Proclamations, Regulations, Government Notices, General Notices, and other future inputs. This can be achieved using dropdown menus or tabs for different types of instructions, with each instruction having its own template.	
	2. Document Management:		
		● Automate core processes of the legislative drafting workflow as defined in the LDD SOP (e.g., routing drafts for review, amendments, and managing approvals).	
		● Automated Comparison: The system should compare sections in a legislative proposal with the master statute databases.	
		● Change Detection: Detect any changes that have not been correctly formatted and highlight discrepancies.	
		● Generate reports on changes and amendments efficiently.	
		● Secure storage of legislative documents, including draft Bills, subsidiary legislation, memoranda, instructions, revision notes, and communication records.	
		● Maintain version histories for all drafts and amendments and automatically generate amendment instructions from a marked-up version of a bill.	
		● The system should have the capability of uploading/scanning of related document to form part of the file.	

		● Maintain version histories for all drafts and amendments and automatically generate amendment instructions from a marked-up version of a bill.	
		● The system should have the capability of uploading/scanning of related document to form part of the file.	
		●The system should have provision for additional fields to be added by user if needed.	
		● The System must provide a method for automatically linking events, file status changes, documents, and correspondence. Summery reports (History of the tile from initial state lo date)	
		● Enable easy retrieval of documents based on various criteria (Ministry, date, subject matter).	
		● Integrate with existing document management systems or EDRMS within the OAG&DOJ	
		● The system should provide customizable templates for bill drafting based on predefined legislative formats.	
		● Automated Proof-reading: Check drafts for grammatical, typographical, and formatting errors. ● Automated notifications for pending tasks, approvals, and deadlines.	
		● Document approval workflow with digital signatures.	
	3. Legislative Research:		
		● Provide access to a comprehensive legal research library containing Kenyan legislation, case law, parliamentary materials, and relevant international legal instruments.	
		● The system should include advanced search functionalities to retrieve specific legal information efficiently.	

	● Integrate with external legal databases e.g Kenya Law	
	● The system should include analytical tools to generate reports on legislative trends and highlight key focus areas based on historical data.	
	4. Communication	
	● The system should enable seamless communication between Parliamentary Counsel, Ministries, and other stakeholders through integrated messaging and notification features.	
	● Enable communication with requesting entities for clarifications, feedback, or updates.	
	● The system should enable real-time collaborative document editing and annotations for authorized users	
	● Track correspondences by individual and by individual involvement to a particular instruction	
	● The system should allow one to set reminders/notifications/alerts escalated notification to immediate supervisor)	
	5. Reporting:	
	● Generate reports on the volume and types of legislative drafting requests received.	
	● Generate reports on the status of requests, drafts, and approvals.	
	● Record metadata on the legal basis for the adoption of laws or regulations. Store dates of adoption, entry into force, and application dates. ● Track performance metrics like turnaround time for completing drafts.	
	● Dashboard for monitoring overall progress and key performance indicators (KPIs).	

		● It should be capable of producing data and collective summaries, including a quarterly report of the completed work of legislative drafters based on agreed metrics. Additionally, the system should be able to monitor and manage workflow and produce summaries accordingly.	
		● Historical Data Analysis: Support for historical data reporting and trend analysis to track legislative drafting performance over time and identify areas for improvement.	
		● Options to export reports in various formats (e.g., PDF, Excel) for sharing with stakeholders, as well as secure sharing mechanisms within the system.	
		● Ensuring that reporting features are aligned with role-based access controls, allowing appropriate access to reports based on user permissions.	
	6. Legislative Tracking:		
		● Track the progress of Bills through Parliament, including committee stages, second reading, and third reading.	
		● Monitor further proposals to the Bills from MDAs for onward transmission to the parliament.	
		● The system should track progress, have a section for comments of actions taken and Status of file.	

	Technical Requirements	
	7. Security:	
		● Implement user authentication and role-based access control to restrict access to sensitive information.	

		● Ensure data encryption for storage and transmission of legislative documents.	
		● Adhere to relevant legal and regulatory requirements regarding data privacy (e.g., Kenya's Data Protection Act, GDPR, HIPAA) and security standards (e.g., ISO 27001).	
		Secure login with multi-factor authentication.	
		● Implement logging mechanisms to track user activities and access attempts. Monitor login attempts for anomalies and potential security breaches.	
		● Real-time monitoring of system performance, availability, and security metrics.	
		● Automated alerting mechanisms to notify ICT personnel of potential issues or anomalies that may indicate a disaster or compromise.	
	8. Scalability**:**		
		● The system should be able to accommodate an increasing volume of legislative drafting requests and documents.	
	9. User Interface:		
		● Develop an intuitive user interface (UI) that is user-friendly and supports efficient navigation and task completion. Consider customizable views and dashboards tailored to different user roles and tasks.	

		● Implement session timeout controls and mechanisms to prevent unauthorized access due to idle sessions. Provide options for users to securely log out and manage their active sessions.	
		● Offer support for Kiswahili (in addition to English) to enhance accessibility.	
		● The system should have a language tool (Grammar and spell check)	
	10. Integration:		
		● Compliance and Standards Integration: Ensure integration with regulatory compliance standards such as the Statutory Instruments Act, 2013, and other legal frameworks relevant to legislative drafting and publication processes.	
		● Workflow Integration: Implement integration of workflow processes to facilitate smooth transitions between drafting stages, review cycles, and approval procedures. This ensures that all stakeholders are informed and involved at each step of the legislative drafting process.	
		● Reporting and Analytics Integration: Integrate reporting and analytics capabilities to generate insights into legislative drafting timelines, efficiency metrics, and compliance with legal requirements. This supports decision-making	

		and process improvement initiatives.	
		● Incorporate advanced data analytics (e.g., predictive trends, drafting efficiency patterns, and real-time legislative impacts) to enhance decision-making.	
		● Implement AI-driven insights to help identify drafting bottlenecks and opportunities for process improvement.	
		● Integrate with existing government ICT systems like email, calendar, and document management systems.	
		● Integrate with e-Parliament platform (if applicable) for tracking Bill progress	
	11. Accessibility:		
	a) Accessibility Standards:	● Ensure compliance with accessibility standards (e.g., WCAG 2.1) to accommodate users with disabilities. This includes support for assistive technologies such as screen readers and keyboard navigation.	
	b) Secure Remote Access:	● Enable secure remote access to the system, possibly through VPN or secure web portal, ensuring encrypted communication channels to protect data in transit.	
		● Optimize the system for mobile devices to facilitate access from smartphones or tablets, ensuring responsiveness and usability across different screen sizes. It should also have offline capabilities (Given the nature	

		of legislative work, drafters might need access to documents or drafting features in areas with limited connectivity).	
	12. Audit Trail:		
		● Maintain a comprehensive audit trail to track all actions performed within the system, including user activity and changes made to documents.	
		● Log the identity of the user performing the action, including their username or unique identifier, to attribute actions accurately.	
		● Implement measures to ensure that logged events cannot be altered or deleted by users, maintaining data integrity and accountability.	
		● Provide authorized personnel with the ability to review and search through audit logs efficiently for investigation and compliance purposes.	
		● Define a retention policy for audit logs that complies with regulatory requirements and organizational policies, ensuring logs are available for audits and investigations.	
		● Integrate audit trail data with system monitoring tools to detect anomalies or suspicious activities in real-time.	
		● Set up alerts or notifications for critical events or deviations from normal user	

		behavior, prompting immediate review and response.	
	13. **UI/UX Guidelines:**		
	a)	**User Roles & Permissions**	
		• Implement a clear role-based access control (RBAC) system. Different users (attorneys, researchers, administrators, clerks) should have access only to relevant data and features.	
		• Display only the necessary tools/features for each user's role to reduce clutter.	
		• Provide visual cues or restrictions on actions for users with limited permissions (e.g., grayed-out options for restricted actions).	
	b)	**Dashboard for Quick Access**	
		• Develop a customizable dashboard with an overview of pending, recent, and historical opinions. Users should quickly access recent opinions, popular requests, and active matters.	
		• Use widgets or panels that show recent activities, deadlines, and popular topics.	
		• Allow customization based on user preferences (drag-and-drop widgets or filtering options).	
		• Provide search summaries for frequently referenced legal matters.	
	c)	**Advanced Search & Filtering**	

		● Create an intuitive, robust search engine with advanced filters (e.g., by date, issue area, opinion number, attorney, department). Users need to retrieve legal opinions and documents quickly and accurately.	
		● Include autosuggestions as user's type keywords, making searches faster and more intuitive.	
		● Allow complex query building (e.g., Boolean search) for power users.	
		● Enable filtering by metadata such as date range, type of opinion, relevance to specific laws, or department requested by.	
	d) Document Management System (DMS)	
		● Implement a document management interface where users can view, download, or annotate opinions. Users will need quick access to both digital and historical records.	
		● Provide document previews or snippets for fast scanning.	
		● Include version control for opinions and track amendments or supplements to legal opinions.	
		● Add features for attaching related documents or linking opinions to specific cases or laws.	
	e) Opinion Creation Workflow	
		● The system should include customizable templates to standardize the drafting of legal opinions and legislative documents.	

	● Streamline the drafting process to ensure uniformity and ease of use across the system.	
	● Use guided steps or a wizard for the drafting process, with drop-down options for categorizing opinions (legal area, government entity, etc.).	
	● Autosave functionality to prevent data loss.	
	● Option for users to input citations and related case laws through an integrated library or reference system.	
f)	**User-Friendly Interface with Legal Jargon**	
	● Simplify complex legal terminologies without sacrificing accuracy. Users of varying legal expertise will use the system.	
	● Tooltips or info popups to explain specific legal terms or jargon.	
	● Allow tagging of documents with user-generated keywords to assist non-legal personnel in searching documents.	
	● Simplify labels and form field instructions, using plain language where possible.	
g)	**Access to Historical Opinions**	
	● Ensure historical opinions are well organized and easily searchable by year, topic, or issuing attorney. State Counsels often reference older legal opinions when drafting new ones.	
	● Archive views with pagination or infinite scrolling for large datasets.	

		● Filter by administration (presidential terms) or key events (e.g., constitutional amendments).	
		h) Audit Trails & Document History	
		● Track and display edits, reviews, and approvals of legal opinions. Legal documents need a detailed audit trail for accountability and transparency.	
		● Provide a "Document History" tab showing who edited what and when.	
		● Allow comments, approvals, or rejections within the opinion draft workflow, making collaboration easier.	
		● Notifications for changes in critical legal documents.	
		i) Collaboration Features	
		● The system should provide features to enable collaborative drafting and reviewing of legal opinions among authorized users.	
		● Integrate real-time document editing or comment sections for peer review and discussion.	
		● Allow "mentions" or task assignments within the document for team collaboration.	
		● Enable tracking of who has viewed and signed off on an opinion.	
		j) Responsiveness and Mobile Access	

	● Ensure that the system is mobile-friendly for access on tablets and smartphones. Legal professionals often work remotely or need quick access to documents outside of their offices.	
	● Design for touch interaction with large buttons and dropdowns that are easy to navigate on small screens.	
	● Ensure seamless transition from desktop to mobile for continued document access.	
	● Provide offline access for essential documents or opinion drafts.	
k) Data Security & Privacy		
	● Prioritize security features like encryption, two-factor authentication (2FA), and access logs. Legal opinions contain sensitive governmental information.	
	● Make sure access logs and warnings about unauthorized access are easily visible.	
	● Use visual alerts for data sensitivity classifications (e.g., confidential, public).	
	● Ensure that secure login screens and document encryption protocols are visible but not intrusive to the user experience.	
l) Legal Reference Integration		
	● Integrate external legal references, case law databases, and relevant statutes. Legal opinions often	

		cite laws, statutes, and previous cases.	
		● Offer cross-referencing capabilities to pull in relevant legal precedents or statutory laws within the drafting interface.	
		● Provide a side-by-side view or pop-up when referencing laws or statutes in an opinion.	
	m) Notifications and Alerts		
		● Include notifications for updates, pending approvals, or deadlines related to opinions. Time-sensitive legal matters need proactive alerts.	
		● Implement email and system notifications for users on important updates (opinion finalizations, due dates, etc.).	
		Ensure critical alerts are prominent on the dashboard, such as opinions due for review or response deadlines.	
	n) Visual Consistency & Branding		
		● Use consistent branding and styling throughout the application to reflect the Attorney General's Office. Maintain a professional and cohesive look that reflects authority and trust.	
		● Utilize the office's official color scheme and typography.	
		● Keep layout clean, with sufficient white space and standardized button styles, fonts, and icons for easy navigation.	
	o) Accessibility Standards (WCAG)		

	• **Guideline:** Follow WCAG (Web Content Accessibility Guidelines) to make the system accessible to all users. Legal systems must be accessible to people with disabilities.	
	• Ensure compatibility with screen readers.	
	• Use high-contrast designs and larger fonts for readability.	
	• Enable keyboard navigation for users with mobility impairments.	
14. Training:		
	• The system should incorporate user training modules and self-learning resources to facilitate capacity building for Parliamentary Counsel and other users.	
	• The system should be accompanied by structured technical documentation and user manuals to enable ICT personnel to conduct first-line support.	
15. Technical **Support:**		
	• New systems should be able to operate in a virtual environment.	
	• The system should be able to run on multiple operating systems e.g. Windows, Linux.	
	• The system should have lifetime licensing, including free updates for the first five years from the time the entire system goes live.	
	• ICT staff should be granted full privileges.	

		● The system should include a structured support mechanism for a period of 24 months, with detailed service-level requirements to be fulfilled by the implementing entity.	
		● Client support should be available through technical support, email, and telephone.	
		● Clear and detailed maintenance activities and duties should be performed on the system (quarterly, bi-annually, annually).	
	16. Disaster Recovery:	
		● The system must include a disaster recovery mechanism to ensure business continuity in case of system outages or data loss.	
		● The system should have inbuilt capacity for regular and automated backups of all system data, configurations, and documents.	
		● The system should have built in mechanism that restores data quickly to minimize downtime in case of data loss.	
	17. Data Migration:	
		● The system should include tools and functionalities to facilitate the migration of existing legislative drafting data while ensuring data integrity.	
		● The system should support data extraction, integrity validation, and lineage tracking to ensure seamless transition from legacy systems.	
		● The system must include automated validation processes to ensure data migration meets predefined quality standards and business rules set by the OAG&DOJ.	

		● The system should support automated testing functionalities to verify the accuracy, completeness, and consistency of migrated data, including the use of sample data sets and edge cases.	
		● The system should include built-in rollback mechanisms, backup functionalities, and data recovery tools to address potential migration failures or data corruption.	
		● The system should provide logging and troubleshooting tools to address data integrity issues post-migration.	
	18. Key deliverables		
		a) The supplier must deliver a system that meets the predefined functional and non-functional requirements.	
		b) The system must be designed to integrate all components seamlessly as per the approved specifications.	
		c) **Source Code and Compiled Software**: The supplier should deliver the system together with its source code to enable future maintenance and upgrades.	
		d) **User and Technical Documentation**: The system should include built-in manuals, guides, and help files that assist end-users in operating the system effectively.	
		e) **Training Materials and Sessions**: The system provider should deliver structured training materials and facilitate initial user training to ensure proficiency in system use.	

LOT 3: Correctional Services Management Information System for State Department for Correctional Services.

1.0	**RECEIVING A PRISONER**	**CONFORMITY (YES/NO)**

	1.1	a.The system should be able to capture prisoner's name, prisoner number, case number, source (transfer, court or hospital), and status i.e. remand, convicted, Borstal, Youth Correctional Training Centre (YCTC) and capture all the information in the warrant. b. Ability to knockout/ knock in movement of prisoners. c. Ability to capture CAM10 (children under the age of 4yrs accompanying their mothers). d. Ability to auto generate and alert on the number of times the prisoner has been detained.	
	1.2	a. The system should be able to identify and verify the prisoner details captured during the search process. b. The system should be able to Capture biometric data.	
	1.3	c. Ability to assign admission number	
	1.4	d. Ability to view and clear the prisoner to be admitted into prison (by the duty officer during the day and sleeping-in officer during the night). e. Ability to timeout the duty officer after final lockup, and sleep-in officer after unlock. f. Ability to show status of a prisoner who has been denied entry into prison, reasons and the clearance (authorization) by the officer in charge.	
	2.0	**ADMISSION**	
	2.1	a. The system should have ability to categorize prisoner into: male, female, Intersex; Convicted, remand; Borstal boys, Borstal Girls; Youth Correctional Training Centre (YCTC); Terrorism and terrorism related; serious organized crime.	
	2.2	b. Ability to capture result of medical screening using PF10 register and notify the medical officer for medical attention.	
	2.3	c. Ability to capture additional information upon profiling using PF1 form, Property, valuable, cash, weight, photo, transfer information, initial assessment results, details of accommodation assigned and personal items issued, appeal status if convicted, pending cases, previous convictions, and multiple cases for convicted. d. Ability to have prisoner cash management module	

		e. Ability to verify the captured details with prisoner's biometrics.	
	2.4	e. Ability to capture and categorize prisoner's disposable items, action taken and who authorized the action. f. Biometric approval by the prisoner of his/her items on actions taken above.	
	2.5	g. Ability to capture next of kin details and notify them.	
	3.0	**RISK ASSESSMENT**	
	3.1	a. Ability to categorize risk assessment, and ability to share risk assessment report upon transfer b. Ability to capture risk factors based on risk assessment tools c. Ability to capture results of each assessment i.e. high/medium/low based on risk assessment reporting template. d. Ability to add and identify security interventions based on risk assessment input, age, health, sentence etc. e. Ability to identify the appropriate security infrastructure based on the risk level. f. Ability to generate risk assessment report	
	4.0	**NEED ASSESSMENT**	
	4.1	a. Ability to capture criminogenic factors b. Ability to capture results of need assessment based on needs assessment reporting template. c. Ability to identify interventions based on "b" above. d. Ability to generate needs assessment report	

		5.0		
		CLASSIFICATION OF PRISONERS		
		5.1		

5.0
CLASSIFICATION OF PRISONERS
5.1

a. Ability to retrieve prisoner's details including risk assessment report and intervention plan in-order to classify them based on risk level.

b. Ability to assign and categorize security regime i.e. restricted/normal regime.

c. Ability to select proposed security interventions and management plans.

d. Ability to allocate accommodation.

e. Ability to alert in event there is change in accommodation.

f. Ability to use access control and CCTV to regulate and monitor movement within the facility.

g. Ability to notify any irregular movement within the facility.

h. Ability to send alerts in case of any emergency to the relevant authorities.

i. In case of serious incidents like riots it should deactivate all control rooms and activate the main command center to take control.

j. The system should allocate the next station to a prisoner and time limit upon clearance and give alerts in the event of exceeding the time limit or change in the allocated station.

k. Ability to capture the details of a prison officer escorting the prisoner in and out of an accommodation unit.

l. Ability to discharge prisoners from the accommodation unit.

	6.0	**DISENGAGEMENT, DE-RADICALIZATION, REHABILITATION, EMPOWERMENT**	
	6.1	a. Ability to categorize Disengagement, De-radicalization, Rehabilitation and Empowerment. b. Ability to retrieve prisoner's details including needs assessment reports and sentence plans. c. Ability to assign the intervention, measures, programs and deployments to be undertaken then match with the intervention provider. d. Ability to capture intervention progress reports provided by the provider. e. Ability to show intervention status. f. Ability to generate a report	
	7.0	**COMPUTATION AND REMISSION OF SENTENCE**	
	7.1	a. Ability to sort those who are eligible or not eligible for remission. b. Ability to categorize types of sentence computation i. Normal sentence ii. Concurrent sentences iii. Consecutive sentence iv. Overlapping sentences v. After Recapture where a prisoner has been apprehended within 30 days vi. Recapture where a prisoner has been at large for more than a month vii. Computation for substantive sentence viii. After loss of remission ix. Upon appeal x. Commutation xi. Revision xii. Petition xiii. Upon grant of further remission xiv. After deprivation of remission. (standing order No.92, there are other formulas dictated by court) c. Ability to allow customized computations based on orders and directives (Above customized computation should have a workflow with different levels of approvals).	
	8.0	**RECEPTION BOARD**	
	8.1	a. Ability to review prisoner's details and reports. e.g. dashboard b. Ability to capture board's resolutions and assign them to respective officers for action. c. Ability to notify reception board members to conduct a reception board	

		d. Generate reception reports	
	9.0	**DISCHARGE BOARD**	
	9.1	a. Ability to review prisoner's details and reports. e.g. dashboard b. Ability to capture board's resolutions and assign them to respective officers for action. c. Ability to assign a proposed person/institution that will support the prisoner upon release. d. Ability to automatically notify and refer to external agencies and generate a report for notification e. Ability to automatically notify and refer to external agencies and generate a report for notification. f. Generate discharge reports	
	10.0	**PRISONERS DISCIPLINE**	
	10.1	a. Ability to retrieve prisoner's information b. Ability to add, update and retrieve offences and sanctions. c. Ability to capture sanctions and automatically compute new release dates.	
	11.0	**COURT PRODUCTION**	
	11.1	a. Ability to categorize different productions b. Ability to retrieve/add/update court related information for both physical and virtual court sessions. c. Ability to send notifications on due court production. d. Ability to track prisoner movement out of prison. e. Generate production reports	
	12.0	**TRANSFER OF PRISONER**	
	12.1	a. Ability to categorize transfer type into on-court order or upon request by OIC through form PF17 attaching form PF43, assessment reports, PF10, PF1 and relevant documents b. Ability to retrieve /capture and update prisoner's transfer details. c. Ability to notify OIC of the receiving station. d. Ability to generate transfer requests e. Ability to track prisoner's transfer history. f. Ability for the system to integrate with the Fleet Management System. g. Ability to generate reports.	
	13.0	**REMOVAL OF A PRISONER FROM PRISON**	

	13.1	a. Ability to categorize removals e.g. hospital, mental facility, leper settlement. b. Ability to retrieve/ add and update medical information. c. Ability to track prisoner movement and location. d. Ability to show prisoners treatment status. e. Ability to generate reports with relevant institutions f. Ability to generate removal reports.	
	14.0	**BORSTAL**	
	14.1	a. Ability to select and confirm availability of a vacancy b. Ability to receive and process requests c. Ability to categorize Borstal facility. d. Ability to track availability of vacancy. e. Ability to allocate a Borstal facility. f. Ability to alert in event there is change in accommodation. g. Ability to use access control and CCTV to regulate and monitor movement within the facility. h. Ability to notify any irregular movement within the facility. i. Ability to send alerts in case of any emergency to the relevant authorities. j. In case of serious incidents like riots it should deactivate all control rooms and activate the main command center to take control. k. The system should allocate the next station and time limit upon clearance and give alerts in the event of exceeding the time limit or change in the allocated station. l. Ability to capture the details of an officer escorting the Borstal girl/ Borstal boy out of the accommodation unit. m. Ability to discharge Borstal girl/ Borstal boy from the accommodation unit.	
	15.0	**PRESIDENTIAL PARDONS**	
	15.1	a. Ability to retrieve prisoners' details. b. Ability to review prisoners' petitions to confirm eligibility. c. Ability to capture petition requests. d. Biometrics approval by the prisoner. e. Ability to forward the request to Power of Mercy f. Ability to capture and track status. g. Ability to track the petition status. h. Ability to generate pardon reports	
	16.0	**OTHER PARDONS**	

	16.1	a. Ability to retrieve prisoners' details. b. Ability to review prisoners previous pardon status for eligibility. c. Ability to capture the pardon request. d. Biometrics approval by the prisoner. e. Ability to submit the pardon request. f. Ability to capture and track status. g. Ability to capture the decision about the requested pardon. h. Ability to generate reports.	
	17.0	**ESCAPE**	
	17.1	a. Ability to categories escapes b. Ability to retrieve prisoner's details c. Ability to capture reports d. Ability to generate reports on escape. e. Ability to track the status of escape and if recaptured the system should compute new dates of release.	
	18.0	**DEATH OF A PRISONER**	
	18.1	a. Ability to retrieve details b. Ability to capture death reports c. Ability to discharge the body d. Ability to generate reports	
	19.0	**DISCHARGE OF A PRISONER**	
	19.1	a. Ability to categorize types of discharge b. Ability to retrieve details c. Ability to capture discharge report d. Ability to notify OIC and CGP. e. Ability to notify other agencies upon discharge f. Ability to generate reports g. Ability to generate certificate of completion for the prisoners	
	20.0	**VISITATION**	
	20.1	a. Ability to categorize types of visits. b. Ability to capture visitors' details. c. Ability of a visitor to make visitation request d. Ability to process requests and notify the visitor on progress e. Ability to track the visitor movement and notify them of the time allocated. f. Ability to map prisoners' details to the visitor. g. Ability to notify the OIC and the duty officer of any visitors who have exceeded time allocated. h. Ability to generate reports	
	21.0	**LOCKUPS AND UNLOCKS**	

	21.1	a. Ability to categorize different types of counts (morning unlock, midday lockup, Midday unlock). b. Ability to confirm the number of prisoners' tally with biometrics counts. c. Ability to use biometrics for lockups and unlocks.	
	22.0	**YCTC (Youth Corrective Training Center)**	
	22.1	a. Ability to capture details of youthful offenders b. Ability to allocate activities. c. Ability to capture time management scheduleAbility to capture report d. Ability to generate report	
	23.0	**INTEGRATED COMMAND AND CONTROL CENTER (C&CC)**	
	23.1	a. The Integrated command and control center at the prison headquarters should be linked to other command centers within the stations. b. Ability to provide a unified view of the prisons. c. Ability to communicate with other intelligent components of ICMIS. d. Ability to disable all other sub command and control centers (within the stations). e. Ability to notify the C&CC controller and Commissioner General of Prisons (CGP) in the event of a security breach. f. Ability to detect and notify the C&CC controller and CGP in the event of attempted penetration to the system. g. Ability to integrate a 3D view of every prison. h. Ability to generate customized alerts to other security agencies. i. Ability to integrate with access control systems.	
	24.0	**MEDICAL TREATMENT OF PRISONERS INSIDE THE PRISON**	
	24.1	a. Ability to retrieve/ add and update medical information. b. Ability to track prisoner movement and location. c. Ability to show prisoners treatment status. d. Ability to generate referral reports.	
	25.0	**RATION STORE MANAGEMENT**	
	25.1	a. Ability to retrieve prisoners' details. b. Ability to capture the amount and type of food received in a ration store. c. Ability to compute amount and type of food allocated to each prisoner on daily basis d. Ability to compute the cumulative amount of food to be released per day based on the number of prisoners In a prison	

		e. Ability to ascertain food balance in the store	
	26.0	**USER MANAGEMENT AND PRIVILEGES**	
	26.1	a. The system must utilize username and password to authenticate users and support two-factor authentication to strengthen access control when necessary. b. Role-based access control shall be used to define content and functionality applicable to users. This must be in line with the user's job function or role. c. Reports must only be accessed by authenticated and authorized users in line with their job function or role. Only authorized users must be able to edit or make changes to data.	
	27.0	**REPORTS**	
	27.1	a. Ability to generate reports for all the modules above b. Ability to show report in different graphical representation c. Ability to export the reports to different formats e.g. excel etc. d. Ability to have a dashboard with Analytics presentations.	
	28	**Kenyan Offenders Incarcerated Abroad**	
	28.1	Ability to capture all person details including and not limited to Name, Age, Passport number, ID number, Photo, Language Spoken, and Biometrics Ability to capture the Next of kin details Ability to capture the crime committed and the sentencing	

PROBATION AND AFTERCARE SERVICE (CASE MANAGEMENT SYSTEM)

		Requirements	Conformity (YES/NO)
	1.0	**Social Inquiries and Offender Assessment**	
	1.1	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts (bail reports, Victim Impact Statement, Presentence, Diversion, Plea bargaining, Resentencing and any other report)	
	1.2	Ability to allocate and reallocate the case to a Probation Officer to undertake.	
	1.3	Ability to retrieve and view historical records of the Offender including criminal records	

	1.4	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office and link up with Kenya Police and Kenya Prisons in future.	
	1.5	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources) Ability to track and monitor progress of case to conform to timelines Ability to input changes, edit arising from new information obtained	
	1.6	Ability to flag accused child, accused violent extremist/ suspected accused violent extremist Ability to flag child suspected of Sexual offences	
	1.7	Ability to assess the accused risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	1.8	Ability to request and schedule case conference	
	1.9	Ability to allow supervisor to approve and select officers to participate in case conference Ability for supervisors to monitor progress of report online	
	1.10	Ability to input the recommendations of the case conference	
	1.11	Ability to input Report	
	1.12	Ability to approve Reports at various levels (Station, County, Region, Headquarters) Ability to input feedbacks from the various levels quality control	
	1.13	Ability to digitally sign and generate Bail Information Report (Ability to print, sign, upload) Ability to digitally generate and sign Bail/Bond Information Report, Pre-sentence reports, Victim Impact Statement, Diversion, Plea – Bargaining, Resentencing report, Home Final Report,ity to digitally sentences, Victim Impact	

		Statement, Diversion, Plea –Bargaining, Resentencing report, Home Final Report,	
	1.14	Ability to submit report to Court	
	1.15	Ability to record court outcome (bail granted, denied, reviewed or sustained)	
2.0		**PROBATION SERVICE**	
		Probation Orders	
	2.1	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts	
	2.2	Ability to allocate and reallocate the case to a Probation Service Officer the case to	
	2.3	Ability to generate and view historical records of the Offender	
	2.4	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office)	
	2.5	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources)	
	2.6	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	2.7	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	2.8	Ability to request and schedule case conference	
	2.9	Ability to allow supervisor to approve and select officers to participate in case conference	
	2.10	Ability to input the recommendations of the case conference	
	2.11	Ability to input pre-sentence Report	

	2.12	Ability to approve Pre-sentence Report at various levels (Station, County, Region, Headquarters)
	2.13	Ability to digitally sign and generate pre-sentence Report (Ability to print, sign, upload)
	2.14	Ability to submit pre-sentence Report to Court
	2.15	Ability to record court outcome
	2.16	Supervision in the Community (triggered by a Court Order)
	2.17	Ability to upload Court Order into the system
	2.18	Ability to register the case and generate serial number
	2.19	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender
	2.20	Ability to update offender details (PR2 from)
	2.21	Ability to capture supervision notes (Recording of offender's reporting, day, time, discussions, progress in PR2A Form)
	2.22	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)
	2.23	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Offenders with special needs(SNO) ,Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)
	2.24	Ability to develop individual treatment, supervision and rehabilitation plans
	2.25	Ability to capture reintegration, resettlement and rehabilitation interventions used
	2.26	Ability to allow Community Probation Volunteer comments Ability to allow CPVs should be looked into such that some limits on the accessibility rights to the system are addressed.
	2.27	Ability to generate summary reports of the progress made during supervision (after every 6 months)
	2.28	Ability to compute sentence period (start date/ time and end date/ time)

2.29	Ability to capture Form PR 9	
2.30	Ability to generate Form PR 9 Report	
2.31	Ability to upload and submit Case Committee Minutes	
2.32	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)	
2.33	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office	
2.34	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case) Ability to generate exit summary report of the offender under community supervision	
2.35	Ability to choose mode of completion (successful, unsuccessful, absconded)	
2.36	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence	
2.37	Ability to monitor offenders electronically (GPS)	
2.38	Ability to capture Probation Officer's supervisor's comments/ evaluation/ inspection of case work	
2.39	Ability to request for empowerment (tools, education, start-up capital, etc)	
2.40	Ability to record empowerment granted to offender	
2.41	Probation Hostel	
2.42	Social inquiry and report preparation	
2.43	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Court	
2.44	Ability to allocate the case to a Probation Officer to undertake the case, and ability to re-allocate to an alternative Probation Officer	
2.45	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
2.46	Ability to generate and view historical records of the Offender	
2.47	Ability to request for records from other jurisdictions	

	2.48	Ability to capture interview/ social inquiry data (e.g. Interview of accused person, accused family, victim and victims' family, community, other independent sources)	
	2.49	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	2.50	Ability to request and schedule case conference	
	2.51	Ability to allow supervisor to approve and select officers to participate in case conference	
	2.52	Ability to input the recommendations of the Case Conference	
	2.53	Ability to input Pre-sentence Report	
	2.54	Ability to approve Pre-sentence Report at various levels (Station, County, Region, Headquarters)	
	2.55	Ability to request approval for application for vacancy to Probation Hostel (Station, County, Region, Headquarters)	
	2.56	Ability to apply and receive confirmation for vacancy to Probation Hostel (Station, County, Region, Headquarters)	
	2.57	Ability to sign and generate Pre-sentence Report (Ability to print, sign, upload)	
	2.58	Ability to submit Pre-sentence Report to Court	
	2.59	Ability to record Court outcome	
		Application for vacancy	
	2.60	Ability to apply for a vacancy to Probation Hostel	
	2.61	Ability to receive availability and non-availability from Probation Hostel	
		Admission to Probation Hostel	
	2.62	Ability to upload escort documents to the system (Presentence Report, Court Order, Variation Order, Notice to Offender, Medical Report, School documents, Birth Certificate/ National Identity Card Number, and other documents not listed herein)	

	2.63	Ability to compute sentence period (start date/ time and end date/ time), and to compute sentence period added (occasioned by a Court Order)	
	2.64	Ability to perform full body screening of probationer	
	2.65	Ability to confirm date and time of arrival of probationer to the Probation Hostel (this information to be relayed to the Probation Station/ County Probation Office)	
	2.66	Ability to update probationer details in (PR2 Form – Home directions, nearest school/ market, landmark)	
	2.67	Ability to fill Hostel Admission Form	
	2.68	Ability to allocate probationer to a Probation Officer for supervision	
	2.69	Ability to input items issued to a probationer	
		Supervision at a Probation Hostel	
	2.70	Ability to confirm orientation	
	2.71	Ability to capture work/ tasks assigned to probationer	
	2.72	Ability to capture offender's biometric data	
	2.73	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	2.74	Ability to capture supervision notes in (PR2A Form - Recording of probationer's reporting, day, time, discussions, progress)	
	2.75	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)	
	2.76	Ability to assess the probationer's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	2.77	Ability to develop individual treatment,	
	2.78	Ability to capture rehabilitation interventions used	
	2.79	Ability to capture Form PR 9	
	2.80	Ability to generate Form PR 9 report	

	2.81	Ability to upload and submit Case Committee Minutes	
	2.82	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)	
	2.83	Ability to input and transmit reports from the Probation Hostel to Probation Stations/ County Probation Offices, and back (Summary Assessment Report, Initial Environmental Adjustment Report, First Progress Report, First Progress Report, Final Environmental Adjustment Report, Final Report)	
		Exit process from a Probation Hostel	
	2.84	Ability to input returned items issued to probationer	
	2.85	Ability to transfer case to Probation Station/ County Probation Station for supervision	
		Supervision in the community	
	2.86	Ability to upload Court Order into the system	
	2.87	Ability to register the case and generate a serial number	
	2.88	Ability to capture offender's biometric data	
	2.89	Ability to compute Supervision period (start date/ time and end date/ time) Ability to capture extension of supervision order	
	2.90	Ability to update probationer details in PR2 Form	
	2.91	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	2.92	Ability to capture supervision notes in PR2A Form (Recording of offender's reporting, day, time, discussions, progress)	
	2.93	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)	
	2.94	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	

	2.95	Ability to develop individual treatment, supervision and rehabilitation plans	
	2.96	Ability to capture reintegration, resettlement and rehabilitation interventions used	
	2.97	Ability to allow Community Probation Volunteer comments	
	2.98	Ability to generate summary reports of the progress made during supervision (after every 6 months)	
	2.99	Ability to capture Form PR 9 report	
	2.100	Ability to consolidate Form PR 9 (collect all PR 9s for each individual case and Probation Officer, and consolidate into one form)	
	2.101	Ability to upload and submit Case Committee Minutes	
	2.102	Ability to monitor, select and report breach of Court Order/ (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)	
	2.103	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office	
	2.104	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)	
	2.105	Ability to choose mode of completion (successful, unsuccessful, absconded)	
	2.106	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence	
	2.107	Ability to monitor offenders electronically (GPS)	
	2.108	Ability to capture Probation Officer's supervisor's comments/ evaluation/ inspection of case work	
	2.109	Ability to request for empowerment (tools, education, startup capital, etc)	
	2.110	Ability to record empowerment granted to offender	
	2.111	Community Resource and Training Centre	
		Ability for course application and admission	
		Ability to capture trainer details	
	2.112	Ability to capture course details	

2.113	Ability to capture course calendar	
2.114	Ability to assess/ monitor learning (assessment forms)	
2.115	Ability to issue and return reading materials, case studies, journals, etc	
2.116	Ability to store and retrieve audio and video lectures	
2.117	Ability to generate certificates	
	Probation half way houses	
	Application for admission	
2.118	Ability to apply for admission (Ability to upload Application Form)	
2.119	Ability to notify applicant of acceptance or decline of application	
2.120	Admission to Probation and Aftercare HalfWay House	
2.121	Ability to upload documents to the system (e.g. National Identity Card, Court Order, etc)	
2.122	Ability to compute period of stay (start date/ time and end date/ time), and to compute extended period	
2.123	Ability to perform full body screening	
2.124	Ability to update housemate details in (PR2 Form – Home directions, nearest school/ market, landmark)	
2.125	Ability to fill Admission Form	
2.126	Ability to allocate house mate to a Probation Officer for monitoring	
2.127	Ability to input items issued to a house mate and returned by house mate	
2.128	Ability to confirm orientation	
	Stay at Probation and Aftercare Half Way House	
2.129	Ability to capture work/ tasks assigned to a house mate	
2.130	Ability to capture house mate's biometric data	
2.131	Ability to flag recovering violent extremist offender/ suspected violent extremist	
2.132	Ability to capture notes in (reintegration progress, incidences, occupation)	
2.133	Ability to develop reintegration and resettlement plan	
2.134	Ability to capture reintegration and resettlement interventions used	

	2.135	Ability to report breach of House Rules (this should trigger disciplinary measures or termination of residency)	
		Exit process from a Probation and Aftercare Half Way House	
	2.136	Ability to input returned items issued to house mate	
	2.137	Ability to transfer housemate to another half-way house	
	3.0	**COMMUNITY SERVICE ORDER**	
		Social Inquiry and Report Preparation	
	3.1	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts(CSO presentence, sentence review)	
	3.2	Ability to allocate the case to a Community Service Officer to undertake, and to re-allocate to an alternative Community Service Officer	
	3.3	Ability to generate and view historical records of the Offender	
	3.4	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office)	
	3.5	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources)	
	3.6	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	3.7	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	3.8	Ability to capture work agencies and availability of work suitable for offender Ability to capture skills transferred to clients Ability to capture work profile -work agencies at station level Ability to capture tangible projects at station level	

		3.9	Ability to request and schedule case conference	
		3.10	Ability to allow supervisor to approve and select officers to participate in case conference	
		3.11	Ability to input the recommendations of the case conference	
		3.12	Ability to input CSO Pre-sentence Report	
		3.13	Ability to approve CSO Pre-sentence Report at various levels (Station, County, Region, Headquarters)	
		3.14	Ability to digitally sign and generate CSO Pre-sentence Report (Ability to print, sign, upload)	
		3.15	Ability to submit CSO Pre-sentence Report to Court	
		3.16	Ability to record court outcome (Probation Order, Community Service Order, Fine, Imprisonment, Conditional Discharge, Unconditional Discharge, Other-specify)	
		3.17	Supervision in the community (triggered by a court order)	
		3.18	Ability to upload court order into the system	
		3.19	Ability to register the case and generate a serial number	
		3.20	Ability to capture offender's biometric data	
		3.21	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
		3.22	Ability to update offender details	
		3.23	Ability to capture supervision notes (Recording of offender's reporting, day, time, discussions, progress)	
		3.24	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)	
		3.25	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, offenders with special needs(SNO),Child Sexual Offenders RNR, Violent Extremist Offenders – PKRAVET)	
		3.26	Ability to develop individual treatment, supervision and rehabilitation plans	

	3.27	Ability to capture reintegration, resettlement and rehabilitation interventions used Ability to capture crime prevention activities done at the Regional, County and Station level Ability to upload evidence for crime prevention activities Ability to capture Community Service Order partners	
	3.28	Ability to allow Community Probation Volunteer comments	
	3.29	Ability to assign to an offender in a work agency and notify agency	
	3.30	Ability to confirm arrival of an offender to a work agency	
	3.31	Ability to capture Form CS 6	
	3.32	Ability to generate summary reports of the progress made during supervision (after every 6 months) Ability to upload CSO supervision forms (capture CS 2 Work placement confirmation form, capture CS3 Reporting instructions form, capture CS 4 Work attachment report form)	
	3.33	Ability to compute sentence period (start date and/or time and end date and/or time)	
	3.34	Ability to compute work quantification (number of hours worked x wage rate as per area)	
	3.35	Ability to capture Form CS 7 summary report	
	3.36	Ability to generate Form CS 7 report	
	3.37	Ability to upload and submit Case Committee Minutes	
	3.38	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders) Ability to upload CSO breach of order forms CS B & C	
	3.39	Ability to transfer offender to another Community Service Officer/ Probation Station/ County Probation Office 4Ability to upload CSO supervision forms(CS D Notice to offender of substitution of CS Officer, CS E –application for review and variation)	

3.40	Ability to delegate case (where a Community Service Officer is temporarily unable to undertake the case)	
3.41	Ability to choose mode of completion satisfactorily, absconded, unsatisfactorily	
3.42	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence	
3.43	Ability to monitor offenders electronically (GPS) Ability to capture location of tree nurseries and number of trees planted at station level (GPS)	
3.44	Ability to capture Community Service Officer supervisor's comments/ evaluation/ inspection of case work	
3.46	Ability to request for empowerment (tools, education, start-up capital, etc)	
3.47	Ability to record empowerment granted to offender	
4.0	**AFTERCARE**	
	Borstal Report Preparation And Supervision In The Community	
4.1	Social inquiry and report preparation	
4.2	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Court	
4.3	Ability to allocate the case to a Probation Officer to undertake the case, and ability to re-allocate to an alternative Probation Officer	
4.4	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
4.5	Ability to generate and view historical records of the Offender	
4.6	Ability to request for records from other jurisdictions	
4.7	Ability to capture interview/ social inquiry data (e.g. Interview of accused person, accused family, victim and victims' family, community, health records, other independent sources)	
4.8	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders -	

		RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET) Ability to refer for specialized assessments	
	4.9	Ability to request and schedule case conference	
	4.10	Ability to allow supervisor to approve and select officers to participate in case conference	
	4.11	Ability to input the recommendations of the Case Conference	
	4.12	Ability to input Pre-sentence Report	
	4.13	Ability to approve Pre-sentence Report at various levels (Station, County, Region, Headquarters)	
	4.14	Ability to request approval for application for vacancy to Borstal Institution (Station, County, Region, Headquarters)	
	4.15	Ability to apply and receive confirmation for vacancy to Borstal Institution (Station, County, Region, Headquarters)	
	4.16	Ability to sign and generate Pre-sentence Report (Ability to print, sign, upload)	
	4.17	Ability to submit Pre-sentence Report to Court	
	4.18	Ability to record Court outcome	
	4.19	Application for vacancy	
	4.20	Ability to apply for a vacancy to Borstal Institution	
	4.21	Ability to receive feedback on availability and non-availability	
	4.22	Supervision in the community	
	4.23	Ability to upload Borstal Release License into the system	
	4.24	Ability to register the case and generate a serial number	
	4.25	Ability to capture offender's biometric data	
	4.26	Ability to compute sentence period (start date/ time and end date/ time)	
	4.27	Ability to update probationer or ex-Borstal inmate details	
	4.28	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender Ability to flag specialized needs offenders	

	4.29	Ability to capture supervision notes (Recording of offender's reporting, day, time, discussions, progress)
	4.30	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity) Ability to apply for supervision extension
	4.31	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)
	4.32	Ability to develop individual treatment plan
	4.33	Ability to capture reintegration, resettlement and rehabilitation interventions used
	4.34	Ability to allow Community Probation Volunteer comments
	4.35	Ability to generate summary reports of the progress made during supervision (after every 6 months)
	4.36	Ability to capture Progress report
	4.37	Ability to consolidate Progress reports (collect all Progress reports for each individual case and Probation Officer, and consolidate into one report)
	4.38	Ability to upload and submit Case Committee Minutes
	4.39	Ability to monitor, select and report breach of Release License (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)
	4.40	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office
	4.41	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)
	4.42	Ability to choose mode of completion (successful, unsuccessful, absconded)

	4.43	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence	
	4.44	Ability to monitor offenders electronically (GPS)	
	4.45	Ability to capture Probation Officer's supervisor's comments/ evaluation/ inspection of case work	
	4.46	Ability to request for empowerment (tools, education, startup capital, etc)	
	4.47	Ability to record empowerment granted to offender	
	4.48	Power of Mercy Advisory social inquiry, report preparation and supervision in the community	
	4.49	Social Inquiry and Report Preparation	
	4.50	Ability to capture notification and registration of referral of case from Power of Mercy Advisory Committee at the Headquarters	
	4.51	Ability to allocate the case to a Probation Officer to undertake (Headquarters), and to re-allocate to an alternative Probation Officer (County Probation Office)	
	4.52	Ability to retrieve and view historical records of the petitioner	
	4.53	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	4.54	Ability to request for records from other jurisdictions (that is, other County Probation Offices)	
	4.55	Ability to capture interview/ social inquiry data (e.g. Interview of petitioner, petitioner's family, victim and victims' family, community, other independent sources)	
	4.56	Ability to assess the petitioner's risks and needs and classify the risks/ needs into high, medium, low. (Types of assessment tools: (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET) Ability to refer for specialized assessment	
	4.57	Ability to request and schedule Case Conference	

	4.58	Ability to allow supervisor to approve and select Probation Officers to participate in Case Conference	
	4.59	Ability to input the recommendations of the Case Conference	
	4.60	Ability to input Power of Mercy Advisory Report	
	4.61	Ability to approve Power of Mercy Advisory Report at various levels (Region, Headquarters)	
	4.62	Ability to sign and generate Power of Mercy Advisory Report Category Report (Ability to print, sign, upload)	
	4.63	Ability to submit Power of Mercy Advisory Report/ Power of Mercy Advisory Special Category Report to headquarters Ability to access and update Pomac PMR 1 and 2a reports.	
	4.64	Ability to record outcome (Presidential Order, Pardoned, Not pardoned, Other-specify) Ability to record pending outcome	
	4.65	Supervision in the Community (triggered by a Presidential Order)	
	4.66	Ability to upload Presidential Order into the system	
	4.67	Ability to register the case and generate serial number	
	4.68	Ability to capture pardonee's biometric data	
	4.69	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	4.70	Ability to Compute supervision period (start date/ time and end date/ time)	
	4.71	Ability to update Pardonee details	
	4.72	Ability to capture supervision notes Recording of pardonee's reporting, day, time, discussions, progress)	
	4.73	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)	
	4.74	Ability to assess the pardonee's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child	

		Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	4.75	Ability to develop individual treatment, supervision and rehabilitation plans	
	4.76	Ability to capture reintegration, resettlement and rehabilitation interventions used	
	4.77	Ability to allow Community Probation Volunteer comments	
	4.78	Ability to generate summary reports of the progress made during supervision (after every 6 months)	
	4.79	Ability to capture Progress Report	
	4.80	Ability to generate Progress Report	
	4.81	Ability to upload and submit Case Committee Minutes	
	4.82	Ability to transfer pardonee to another Probation Officer/ County Probation Office	
	4.83	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)	
	4.84	Ability to choose mode of completion (successful, unsuccessful, absconded)	
	4.85	Ability to generate Certificate of Completion for pardonee that have successfully completed their sentence	
	4.86	Ability to monitor pardonee electronically (GPS)	
	4.87	Ability to capture supervisor's comments/ evaluation/ inspection of case work	
	4.88	Ability to request for empowerment (tools, education, start-up capital, etc)	
	4.89	Ability to record empowerment granted to offender	
	4.90	Special category psychiatric, leniency, capability social inquiry, and special needs offenders, report preparation and supervision in the community	
	4.91	Social Inquiry and Report Preparation	
	4.92	Ability to capture notification and registration of referral of case from the Psychiatrist (Mathari Hospital)	

4.93	Ability to allocate the case to a Probation Officer to undertake the case, and ability to re-allocate to an alternative Probation Officer	
4.94	Ability to retrieve and view historical records of the Offender	
4.95	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
4.96	Ability to request for records from other jurisdictions (that is, other Probation Stations, County Probation Offices)	
4.97	Ability to capture interview/ social inquiry data (e.g., Interview of accused person, accused family, victim and victims' family, community, health records, other independent sources)	
4.98	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Types of assessment tools: Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET) Ability to refer for specialized assessment	
4.99	Ability to request and schedule Case Conference	
4.100	Ability to allow supervisor to approve and select Probation Officers to participate in case conference	
4.101	Ability to input the recommendations of the case conference	
4.102	Ability to input Capability Report/ Leniency Report	
4.103	Ability to approve Capability Report/ Leniency Report at various levels (Probation Station, County Probation Office, Region, Headquarters)	
4.104	Ability to sign and generate Capability Report/ Leniency Report (Ability to print, sign, upload)	
4.105	Ability to submit Capability Report/ Leniency Report to Psychiatrist	
4.106	Ability to record outcome (Probation Order, Community Service Order, Fine, Imprisonment, Conditional Discharge, Unconditional Discharge, Other-specify)	
4.107	Supervision in the Community (triggered by a Court Order)	
4.108	Ability to upload Court Order into the system	
4.109	Ability to register the case and generate serial number	
4.110	Ability to capture offender's biometric data	
4.111	Ability to compute sentence period (start date/ time and end date/ time)	

	4.112	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	4.113	Ability to update offender details	
	4.114	Ability to capture supervision notes (recording of probationer's reporting, day, time, discussions, progress)	
	4.115	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)	
	4.116	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Types of assessment tools: Substance abuse disorders, female offenders, offenders with mental disorders, child offenders, adult sexual offenders, child sexual offenders, violent extremist offenders)	
	4.117	Ability to develop individual treatment	
	4.118	Ability to capture reintegration, resettlement and rehabilitation interventions used	
	4.119	Ability to allow Community Probation Volunteer comments	
	4.120	Ability to generate summary reports of the progress made during supervision (after every 6 months)	
	4.121	Ability to capture Progress Report	
	4.122	Ability to consolidate Progress (collect all Progress Reports for each individual case and officer, and consolidate into one form)	
	4.123	Ability to upload and submit Case Committee Minutes	
	4.124	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)	
	4.125	Ability to transfer probation to another Probation Officer/ Probation Station/ County Probation Office	
	4.126	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)	
	4.127	Ability to choose mode of completion (successful, unsuccessful, absconded)	
	4.128	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence	
	4.129	Ability to monitor probationer electronically (GPS)	
	4.130	Ability to capture supervisor's comments/ evaluation/ inspection of case work	
	4.131	Ability to request for empowerment (tools, education, startup capital, etc)	
	4.132	Ability to record empowerment granted to offender	
	4.133	ALTERNATIVE DISPUTE RESOLUTION / RESTORATIVE JUSTICE AND VICTIM-OFFENDER MEDIATION SOCIAL INQUIRY,	

		REPORT PREPARATION AND SUPERVISION IN THE COMMUNITY	
	4.134	Social Inquiry and Report Preparation	
	4.135	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts	
	4.136	Ability to allocate and reallocate the case to a Probation Officer	
	4.137	Ability to retrieve and view historical records of the Offender	
	4.138	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office)	
	4.139	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources)	
	4.140	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender	
	4.141	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	4.142	Ability to request and schedule case conference	
	4.143	Ability to allow supervisor to approve and select officers to participate in case conference	
	4.144	Ability to input the recommendations of the case conference	
	4.145	Ability to input Alternative Dispute Resolution Report/ Restorative Justice and Victim-Offender Mediation Report	
	4.146	Ability to approve Alternative Dispute Resolution Report/ Restorative Justice and Victim-Offender Mediation Report at various levels (Station, County, Region, Headquarters)	
	4.147	Ability to digitally sign and generate Report (Ability to print, sign, upload)	
	4.148	Ability to submit report to Court	
	4.149	Ability to record court outcome (Agreement, specify other)	
	4.150	Supervision in the Community (triggered by a Court Order)	
	4.151	Ability to upload Court Order into the system	
	4.152	Ability to register the case and generate a serial number	

	4.153	Ability to compute supervision period (start date/ time and end date/ time) Ability to capture extension of supervision order	
	4.154	Ability to capture offender biometric data	
	4.155	Ability to flag child offender, offender violent extremist / suspected accused violent extremist offender	
	4.156	Ability to update offender details	
	4.157	Ability to capture supervision notes (recording of probationer's reporting, day, time, discussions, progress)	
	4.158	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)	
	4.159	Ability to assess the accused risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	4.160	Ability to develop supervision plan	
	4.161	Ability to capture reintegration and resettlement Ability to capture interventions engaged	
	4.162	Ability to allow Community Probation Volunteer comments	
	4.163	Ability to generate summary reports of the progress made during supervision (after every 6 months)	
	4.164	Ability to capture Progress Report	
	4.165	Ability to generate Progress Report	
	4.166	Ability to upload and submit Case Committee Minutes	
	4.167	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)	
	4.168	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office	
	4.169	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)	
	4.170	Ability to choose mode of completion (successful, unsuccessful, absconded)	
	4.171	Ability to generate Certificate of Completion for offenders that have successfully completed their supervision	
	4.172	Ability to monitor offender electronically (GPS)	
	4.173	Ability to capture Probation Officer's supervisor comments/ evaluation/ inspection of case work	
	5.0	**PROBATION STAFF TRAINING**	
	5.1	Ability for course application and admission	

	5.2	Ability to capture trainer details	
	5.3	Ability to capture training details	
	5.4	Ability to capture training calendar	
	5.5	Ability to assess/ monitor learning (assessment forms)	
	5.6	Ability to issue and return reading materials, case studies, journals, etc	
	5.7	Ability to store and retrieve audio and video lectures	
	5.8	Ability to generate certificates	
	6.0	**REPORTS**	
	6.1	Ability to generate Offender Assessment Report and categorize it as High Risk, Medium Risk, Low Risk, Unfavorable or committal to institutions. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)	
	6.2	Ability to generate the Case Conference recommendation	
	6.3	Ability to generate CSO Pre-sentence Report/ Resentencing Report/ Sentence Review Report/ Power of Mercy Advisory Report/ Power of Mercy Advisory Special Category Report/ Capability Report/ Leniency Report/ Bail Information Report/Plea Bargaining Report/ Victim Impact Assessment Report/ Alternative Dispute Resolution Report/ Restorative Justice and Victim-Offender Mediation Report /Probation Presentence Report/Diversion Report	
	6.4	Ability to generate data in different formats (No. of cases per officer/ station/ county/ region/ national, most prevalent offences per station/ county/ region/ national, No. of cases per male/ female/ boy/ girl/ adult vs children, etc)	
	6.5	Ability to analyze data and give reports (per Probation Station/ County Probation Office/ Region/ National)	
	6.6	Ability to generate CS 7 and CS 9 Reports	
	6.7	Ability to generate a supervisor inspection report at various levels (Station, County, Region, Headquarters)	
	6.8	Ability to input and transmit reports from the Probation Hostel to Probation Stations and County Probation Offices, and back (Summary Assessment Report, Initial Environmental Adjustment Report, First Progress Report, First Progress Report, Final Environmental Adjustment Report, Final Report)	

ITB 35.4	Discount Rate (I) for net present value calculations of recurrent costs (if any) is 2% percent per annum. If rated criterion is used: The weight to be given for cost, X is: 40%
ITB 35.8	Bids for Subsystems or slices of the overall Information System **will *not*** be accepted.
ITB 39.3	As additional qualification measures, the Information System (or components/parts of it) offered by the Bidder with the Most Advantageous Bid may be subjected to the following tests and performance benchmarks prior to Contract award*:* measures ***that will be used in the evaluation of Bids**,* ● *demonstration tests* ● *performance benchmarks* ● *documentation review* ● *reference site visits* *and will be carried out by the respective Project Implementation Units*
F. AWARD OF CONTRACT	
ITB 43	The award will be made on the basis of ***rated criteria*** pursuant to ITB 35.7, if applicable, in accordance with Section III, Evaluation and Qualification Criteria.
ITB 44	The maximum percentage by which quantities may be increased is: **20 percent** The maximum percentage by which quantities may be decreased is: **20 percent** The items for which the Purchaser may increase or decrease the quantities are the following. ● Integration of modules with existing systems ● Any additional modules
ITB 47.1	The successful Bidder **shall** be required to submit the Beneficial Ownership Disclosure Form.
ITB 49	There will be an Adjudicator under this Contract. The hourly fee for this proposed Adjudicator is estimated to be KES 15,000 with a maximum of eight (8) hours a day. The hourly fee is proposed on the

	understanding that the appointed adjudicator will only work on a call basis by the Parties on events of disagreements or disputes. Biographical data of the proposed Adjudicator is as follows: **To be provided.**
ITB 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: The terms of the Bidding Documents; and The Purchaser's decision to award the contract. If a Bidder wishes to make a Procurement-related Complaint, the Bidder 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: **Stanley Kamanguya, OGW** Title/position: **Chief Executive Officer** Purchaser: **The Information and Communications Technology Authority** Email address*:* ceo@ict.go.ke / info@ict.go.ke / procurement@ict.go.ke Fax number: **Not Applicable**

Résumé of the proposed Adjudicator.

[insert résumé]

SECTION III - EVALUATION AND QUALIFICATION CRITERIA
(WITHOUT PREQUALIFICATION)

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

In addition to the criteria listed in ITB 35.3 (a) to (e), the following factors shall apply:

1. Technical Evaluation (ITB 35.3 and ITB 35.4)

If, in addition to the cost factors, the Purchaser has chosen to give weight to important technical factors (i.e., the price weight, X, is less than 1 in the evaluation), the total technical points assigned to each Bid in the Evaluated Bid Formula will be determined by adding and weighting the scores assigned by an evaluation committee to technical features of the Bid **in accordance with the BDS** and the scoring methodology below:

Technical proposal scoring methodology

(a) During the evaluation process, the evaluation committee will assign each desirable/preferred feature a whole number score from 0 to 4, where 0 means that the feature is absent, and 1 to 4 either represent predefined values for desirable features amenable to an objective way of rating (as is the case for, e.g., extra memory, or extra mass storage capacity, etc., if these extras would be conducive for the utility of the system), or if the feature represents a desirable functionality (e.g., of a software package) or a quality improving the prospects for a successful implementation (such as the strengths of the proposed project staff, the methodology, the elaboration of the project plan, etc., in the bid), the scoring will be 1 for the feature being present but showing deficiencies; 2 for meeting the requirements; 3 for marginally exceeding the requirements; and 4 for significantly exceeding the requirements.

(b) The score for each feature (i) within a category (j) will be combined with the scores of features in the same category as a weighted sum to form the Category Technical Score using the following formula:

$$S_j \equiv \sum_{i=1}^{k} t_{ji} * w_{ji}$$

where:

t_{ji} = the technical score for feature "i" in category "j"

w_{ji} = the weight of feature "i" in category "j"

k = the number of scored features in category "j"

and $$\sum_{i=1}^{k} w_{ji} = 1$$

(c)   The Category Technical Scores will be combined in a weighted sum to form the total Technical Bid Score using the following formula:

$$T \equiv \sum_{j=1}^{n} S_j * W_j$$

where:

S_j = the Category Technical Score of category "j"

W_j = the weight of category "j" as specified in the BDS

n = the number of categories

and $$\sum_{j=1}^{n} W_j = 1$$

2. Economic 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: Four Weeks .

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

If an adjustment for a proposed accelerated time schedule is specified above it shall be made accordingly: For evaluation purposes a *[specify: **number**]* percent reduction in the *[specify: **overall** / **pro rata**]* Bid Price shall be made for each week the proposed achievement of the Operational Acceptance is advanced relative to the Implementation Schedule in the Purchaser's Requirements up to a limit of *[specify: **number**]* weeks of acceleration.

If awarded the Contract, the Bidder's accelerated Implementation Schedule would be formally incorporated into the Contract and this schedule shall govern the application of the contract clauses pertaining to Performance Security, liquidated damages as well as other relevant contract clauses.

(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 Bidder 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 Bid price for evaluation.

Option 1: 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:

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

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 BDS for ITB 35.4.**

(c)   Specific additional criteria: Not Applicable.

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

*[specify **evaluation method**, otherwise state "**Not Applicable**"]*

3. Technical alternatives: Not Applicable.

If invited in accordance with ITB 13.4, will be evaluated as follows: *[specify additional criteria or state "none"]*

4. Combined Evaluation

The Purchaser will evaluate and compare the Bids that have been determined to be substantially responsive, pursuant to ITB 30.

If indicated by the BDS, the Purchaser's evaluation of responsive Bids will take into account technical factors, in addition to cost factors.

In such a case, an Evaluated Bid Score (B) will be calculated for each responsive Bid using the following formula, which permits a comprehensive assessment of the Bid price and the technical merits of each Bid:

$$B \equiv \frac{C_{low}}{C} X + \frac{T}{T_{high}} (1 - X)$$

where

C = Evaluated Bid Price

C_{low} = the lowest of all Evaluated Bid Prices among responsive Bids

T = the total Technical Score awarded to the Bid

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

X = weight for the Price as specified in the BDS

The Bid with the best evaluated Bid Score (B) among responsive Bids shall be the Most Advantageous Bid provided the Bidder was prequalified and/or it was found to be qualified to perform the Contract in accordance with ITB 39.

5. Qualification

Factor	5.1 ELIGIBILITY					
Sub-Factor	Criteria					**Documentation Required**
	Requirement	**Single Entity**	Bidder			
			Joint Venture (existing or intended)			
			All members combined	**Each member**	**At least one member**	
5.1.1 Nationality	Nationality in accordance with ITB 4.4.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Form ELI –5.1.1 and 5.1.2, with attachments
5.1.2 Conflict of Interest	No- conflicts of interests as described in ITB 4.2.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Bid
5.1.3 Bank Ineligibility	Not having been declared ineligible by the Bank as described in ITB 4.5.	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Bid
5.1.4 State owned Entity of the Borrower country	Compliance with conditions of ITB 4.6	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Form ELI –5.1.1 and 5.1.2, with attachments

Factor	5.1 ELIGIBILITY					
Sub-Factor	Criteria					**Documentation Required**
	Requirement	**Single Entity**	**Bidder**			
			Joint Venture (existing or intended)			
			All members combined	**Each member**	**At least one member**	
5.1.5 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 Bidder's country, or by an act of compliance with UN Security Council resolution, both in accordance with ITB 4.8	Must meet requirement	Must meet requirement	Must meet requirement	N / A	Letter of Bid

Factor	5.2 HISTORICAL CONTRACT NON-PERFORMANCE				
Sub-Factor	Criteria				**Documentation Required**
	Requirement	**Bidder**			
		Single Entity	**Joint Venture (existing or intended)**		
			All members combined	**Each member**	**At least one member**	

5.2.1	History of non-performing contracts	Non-performance of a contract[1] did not occur as a result of Bidder's default since 1st January *[insert year]*.	Must meet requirement by itself or as member to past or existing JV	N / A	Must meet requirement[2]	N / A	Form CON - 2
5.2.2	Suspension	Not under suspension based on execution of a Bid Securing Declaration or Proposal Securing Declaration pursuant to ITB 4.7 and ITB 20.10	Must meet requirement	N / A	Must meet requirement	N / A	Letter of Bid

---

[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.

5.2.3 Pending Litigation	Bidder'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 Bidder.	Must meet requirement by itself or as member to past or existing JV	N / A	Must meet requirement	N / A	Form CON – 2
5.2.4 Litigation History	No consistent history of court/arbitral award decisions against the Bidder[3] since 1st January *[insert year]*	Must meet requirement	Must meet requirement	Must meet requirement	N/A	Form CON – 2
5.2.5 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 Bidder)	N/A	Must meet requirement (including each subcontractor proposed by the Bidder)	N/A	Letter of Bid, Form CON-3

---

[3]   The Bidder shall provide accurate information on the related Letter of Bid 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 Bidder or any member of a joint venture may result in failure of the Bid.

[4]

Factor	5.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
5.3.1 Historical Financial Performance	Submission of audited balance sheets 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 to demonstrate the current soundness of the Bidders financial position and its prospective long term profitability.	Must meet requirement	N / A	Must meet requirement	N / A	Form FIN – 5.3.1 with attachments
5.3.2 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 for all the Lots	Must meet requirement	Must meet requirement	N/A	N/A	Form FIN –5.3.2

Factor	5.3 FINANCIAL SITUATION					
Sub-Factor	Criteria					**Documentation Required**
	Requirement	**Bidder**				
		Single Entity	**Joint Venture (existing or intended)**			
			All members combined	**Each member**	**At least one member**	
5.3.3 Financial Resources	The Bidder 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:	Must meet requirement	Must meet requirement	N/A	N/A	Form FIN –5.3.3

Factor	5.4 EXPERIENCE					
Sub-Factor	**Requirement**	Criteria				**Documentation Required**
		Bidder				
		Single Entity	**Joint Venture (existing or intended)**			
			All members combined	**Each member**	**At least one member**	
5.4.1 General Experience	Experience under Information System contracts in the role of prime supplier, management contractor, JV member, or subcontractor for at least the last **seven years** [**7**] years prior to the applications submission deadline.	Must meet requirement	N / A	Must meet requirement	N / A	Form EXP-5.4.1
5.4.2 Specific Experience	Participation as a prime supplier, management contractor, JV[5] member, sub-contractor, in at least **Three (3)** contracts within the last **Seven years** (7) years, each with a value of at least **Kes. 50 Million for Lot 1, Kes 100 Million for Lot 2 and Kes 50 Million for Lot 3** that have been successfully and substantially completed and that are similar to the proposed Information System. *[Specify minimum key requirements in terms of physical size, complexity,*	Must meet requirement	Must meet requirements	N / A	Must meet the following requirement *[specify any key requirement to be met by one member]*	Form EXP 5.4.2

---

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

Factor	5.4 EXPERIENCE					
Sub-Factor	Criteria					Documentation Required
	Requirement	Bidder				
		Single Entity	Joint Venture (existing or intended)			
			All members combined	Each member	At least one member	
	methods, technology and/or other characteristics from those described in Section VII, Purchaser's Requirements 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).					

5.5   Key Personnel – Applicable

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

5.6   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:

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.

5.7   Manufacturer's authorization

For all powered (active) hardware and/or software components of the Information System which the Bidder does not itself produce, by submission of documentary evidence in its Bid, the Bidder 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.

(i)   In the case of powered (active) hardware and other powered equipment, this must be documented by including Manufacturer's Authorizations in the Bid (based on the form in Section IV);

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

(iii)   In the case of proprietary commercial software (i.e., excluding open source or "freeware" software) that the Bidder does not manufacture itself and for which the Bidder does not or will not establish an OEM relationship with the manufacture, the Bidder must document to the Purchaser's satisfaction that

the Bidder is not excluded from sourcing these items from the manufacturer's distribution channels and offering these items for supply in the Borrower's Country.

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

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

5.8 Local Representation

In the case of a Bidder not doing business within the Purchaser's country, the Bidder shall submit documentary evidence in its Bid 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 Bidder's maintenance, technical support, training, 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).

SECTION IV - BIDDING FORMS

Table of Forms

Letter of Bid

<table>
<tr><td>

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

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

<u>*Note*</u>*: All italicized text is to help Bidders in preparing this form.*

</td></tr>
</table>

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

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

Alternative No.: *[insert **identification No if this is a Bid 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 bidding document, including Addenda issued in accordance with Instructions to Bidders (ITB 8);

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

(c) **Bid-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 ITB 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.]

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

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

[Option 1, in case of one lot:] Total price is: *[insert **the total price of the Bid in words and figures, indicating the various amounts and the respective currencies***]*;

Or

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

(g) **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***];

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

(i) **Performance Security:** If our Bid is accepted, we commit to obtain a Performance Security in accordance with the bidding document;

(j) **One Bid Per Bidder:** We are not submitting any other Bid(s) as an individual Bidder, and we are not participating in any other Bid(s) as a Joint Venture member, and meet the requirements of ITB 4.3, other than alternative Bids submitted in accordance with ITB 13;

(k) **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;

(l) **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 ITB 4.6***];

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

(n) **Binding Contract**: We understand that this Bid, 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;

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

(p) **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 Bidder: *[*insert **complete name of the Bidder**]

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

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

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 Bid submitted by joint venture specify the name of the Joint Venture as Bidder

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

PRICE SCHEDULE FORMS

Notes to Bidders 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 Bidders shall have read the Technical Requirements and other sections of these bidding 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 Bidders are unclear or uncertain as to the scope of any item, they shall seek clarification in accordance with the Instructions to Bidders in the bidding documents prior to submitting their bid.

Pricing

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

5.   Bid prices shall be quoted in the manner indicated and in the currencies specified in ITB 18.1 and ITB 18.2. Prices must correspond to items of the scope and quality defined in the Technical Requirements or elsewhere in these bidding documents.

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

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

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 Bid Submission Form)				

Name of Bidder:	
Authorized Signature of Bidder:	

3.2   Supply and Installation Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITB 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 Bidder:		
Authorized Signature of Bidder:		

3.3   Recurrent Cost Summary Table

Costs MUST reflect prices and rates quoted in accordance with ITB 17 and ITB 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 Bidder:		
Authorized Signature of Bidder:		

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 ITB 17 and ITB 18.

				Unit Prices / Rates					Total Prices				
				Supplied Locally	Supplied from outside the Purchaser's Country				Supplied Locally	Supplied from outside the Purchaser's Country			
Component No.	Component Description	Country of Origin Code	Quantity	*[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 Bidder:		
Authorized Signature of Bidder:		

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

Lot number: *[if a multi-lot procurement, insert: **lot number,** otherwise state **"single lot procurement"]**

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 ITB 17 and ITB 18.

Compone nt No.	Component	Maximum all-inclusive costs (for costs in *[insert: **currency]**)*						Sub-total for *[insert: **currency]**
		Y1	Y2	Y3	Y4	...	Yn	
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							

Compone nt No.	Component	Maximum all-inclusive costs (for costs in *[insert: **currency**]*)						Sub-total for *[insert: **currency**]*
		Y1	Y2	Y3	Y4	...	Yn	
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 Bidder:		
Authorized Signature of Bidder:		

3.6   Country of Origin Code Table

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

FORM ELI 5.1.1- BIDDER INFORMATION FORM

[Note: The Bidder 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 Bid submission**]*

RFB No.: *[insert **number of Bidding process]***

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

Page _____ of_ _____ pages

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

- Operation under commercial law
- Establishing that the Bidder is not under the supervision of the Purchaser

8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership. *[If required under BDS ITB 47.1, the successful Bidder shall provide additional information on beneficial ownership, using the Beneficial Ownership Disclosure Form.]*

FORM ELI 5.1.2- BIDDER'S JV MEMBERS INFORMATION FORM

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

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

RFB No.: *[insert **number of Bidding process**]*

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

Page _____ of_ _____ pages

1. Bidder's Name: *[insert **Bidder's legal name**]*
2. Bidder's JV Member's name: *[insert **JV's Member legal name**]*
3. Bidder's JV Member's country of registration: *[insert **JV's Member country of registration**]*
4. Bidder's JV Member's year of registration: *[insert **JV's Member year of registration**]*
5. Bidder's JV Member's legal address in country of registration: *[insert **JV's Member legal address in country of registration**]*
6. Bidder's JV Member's authorized representative information Name: *[insert **name of JV's Member authorized representative**]* Address: *[insert **address of JV's Member authorized representative**]* Telephone/Fax numbers: *[insert **telephone/fax numbers of JV's Member authorized representative**]* Email Address: *[insert **email address of JV's Member authorized representative**]*

> 7. Attached are copies of original documents of *[check the box(es) of the attached original documents]*
>
> ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or registration documents of the legal entity named above, in accordance with ITB 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 ITB 4.6.
>
> 8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership. *[If required under BDS ITB 47.1, the successful Bidder 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

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

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

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

RFB No.: *[insert **RFB 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 5.2.1.			
☐ Contract(s) not performed since 1st January *[insert year]* specified in Section III, Evaluation and Qualification Criteria, requirement 5.2.1			
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 5.2.3.			
☐ Pending litigation in accordance with Sub-Factor 5.2.3 as indicated below.			

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 5.2.4.		
☐	Litigation History in accordance with Sub-Factor 5.2.4 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 Bidder, each member of a Joint Venture and each subcontractor proposed by the Bidder]

Bidder's Name: *[insert full name]*
Date: *[insert day, month, year]*
Joint Venture Member's or Subcontractor's Name: *[insert full name]*
RFB No. and title: *[insert RFB 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 5.4.1- GENERAL EXPERIENCE

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

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

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

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

Page _____ of _____ pages

Starting Month / Year	Ending Month / Year	Years *	Contract Identification	Role of Bidder
[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 Bidder: *[describe **Information System]*** Name of Purchaser: *[insert **Name of Purchaser]*** Address: *[insert **Address of Purchaser]***	*[describe **role of Bidder 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 Bidder: *[describe **Information System]*** Name of Purchaser: *[insert **Name of Purchaser]*** Address: *[insert **Address of Purchaser]***	*[describe **role of Bidder 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 Bidder: *[describe **Information System]*** Name of Purchaser: *[insert **Name of Purchaser]*** Address: *[insert **Address of Purchaser]***	*[describe **role of Bidder 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 Bidder: *[describe **Information System]*** Name of Purchaser: *[insert **Name of Purchaser]*** Address: *[insert **Address of Purchaser]***	*[describe **role of Bidder 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 – 5.4.2- SPECIFIC EXPERIENCE

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

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

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

RFB No.: *[insert **RFB 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 – 5.4.2 (CONT.)- SPECIFIC EXPERIENCE (CONT.)

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

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

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

RFB No.: *[insert **RFB 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 5.4.2 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 Bidder under the contract**]*

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

[Bidders and each partner to an Joint Venture bid 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.]

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

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

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

RFB No.: *[insert **RFB 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 of 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 of 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 of 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 – 5.3.1- FINANCIAL SITUATION: HISTORICAL FINANCIAL PERFORMANCE

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

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

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

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

RFB No.: *[insert **RFB 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 Bidder 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 – 5.3.2- AVERAGE ANNUAL TURNOVER

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

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

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

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

RFB No.: *[insert **RFB 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 5.3.2.

FORM FIN 5.3.3- FINANCIAL RESOURCES

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

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

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

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

RFB No.: *[insert **RFB 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**]*

PERSONNEL CAPABILITIES- KEY PERSONNEL

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

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

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

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

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

Page _____ of _____ pages

Bidders 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: *[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**]*

Candidate Summary

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

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

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

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

RFB No.: *[insert **RFB 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 experience
[insert year]	*[insert year]*	*[describe **experience relevant to the proposed Contract under the RFB**]*
[insert year]	*[insert year]*	*[describe **experience relevant to the proposed Contract under the RFB**]*
[insert year]	*[insert year]*	*[describe **experience relevant to the proposed Contract under the RFB**]*
[insert year]	*[insert year]*	*[describe **experience relevant to the proposed Contract under the RFB**]*

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 bidding documents.

Note to the Bidder:

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

The Bidder shall initial and submit the Code of Conduct form as part of its bid.

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 Bidder and, if JV, by each member]*

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

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

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

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

Page _____ of _____ pages

The Bidder shall provide adequate information to demonstrate clearly that it has the technical capability to meet the requirements for the Information System. The Bidder should summarize important certifications, proprietary methodologies, and/or specialized technologies that the Bidder 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 Bids Title and No.: *[Purchaser insert: **RFB 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 Bidder or Joint Venture**]* located at *[insert: **address of Bidder or Joint Venture**]* (hereinafter, the "Bidder") to submit a bid 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 bidding results in a Contract between you and the Bidder, 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 Bids Title and No.: *[Purchaser insert: **RFB 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 Bidder or Joint Venture**]* located at *[insert: **address of Bidder or Joint Venture**]* (hereinafter, the "Bidder") that it will submit a bid 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 Bidder 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 Bidders on working with the Intellectual Property Forms

In accordance with ITB 11.1(j), Bidders must submit, as part of their bids, lists of all the Software included in the bid assigned to one of the following categories: (a) System, General-Purpose, or Application Software; (b) Standard or Custom Software; (c) Proprietary or Open Source. Bidders must also submit a list of all Custom Materials. These categorizations are needed to support the Intellectual Property in the GCC and SCC. The Bidder 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 Bid

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

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

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

Note: The Technical Requirements are voiced as requirements of the *Supplier* and/or the *System*. The Bidder'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 Bidder should indicate *that* – and to the greatest extent practical – *how* the Bidder would comply with the requirements if awarded the contract. Whenever the technical requirements relate to feature(s) of existing products (e.g., hardware or software), the features should be described and the relevant product literature referenced. When the technical requirements relate to professional services (e.g., analysis, configuration, integration, training, etc.) some effort should be expended to describe how they would be rendered – not just a commitment to perform the [cut-and-paste] requirement. Whenever a technical requirement is for the Supplier to provide certifications (e.g., ISO 9001), copies of these certifications must be included in the Technical Bid.

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

Note: As a matter of practice, the contract cannot be awarded to a Bidder whose Technical Bid 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 bid evaluation and contract award, Bidders 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 BDS ITB 17.2 required Bidders to bid.

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

Technical Responsiveness Checklist (Format)

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

*[**Note to the Purchaser**: The Technical Responsiveness tables submitted by each Bidder can help structure the Purchaser's technical evaluation. In particular, the Purchaser can append rows to each of the Bidder's submitted responsiveness tables to record the Purchaser's assessment of the compliance, partial compliance, and non-compliance of the Bidder's response to the specific Technical Requirement – including the Purchaser's rationale for its conclusion (including, as appropriate, clear indications of the gaps in the Bidder's response/supporting documentation). These assessments can provide a standardized presentation of the detailed underlying logic of the Purchaser's final assessment of the responsiveness / non-responsiveness of the Bidder's technical proposal. Typically, the detailed response/assessment tables would appear as an attachment to the Bid Evaluation Report].*

FORM OF BID 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**]*

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

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

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

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

We have been informed that *[insert **name of the Bidder**, 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 bid (hereinafter called "the Bid") for the execution of *[insert **Name of Contract**]* under Request for Bids No. [insert **number**] ("the RFB").

Furthermore, we understand that, according to the Beneficiary's, Bids must be supported by a Bid 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 Bid prior to the Bid validity expiry date set forth in the Applicant's Letter of Bid, or any extended date provided by the Applicant; or

(b)   having been notified of the acceptance of its Bid by the Beneficiary prior to the expiry date of the Bid 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 Bidders ("ITB") of the Beneficiary's bidding document.

This guarantee will expire: (a) if the Applicant is the successful Bidder, 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 Bidder, upon the earlier of (i) our receipt of a copy of the Beneficiary's notification to the Applicant of the results of the Bidding process; or (ii) twenty-eight days after the expiry date of the Bid validity.

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)]

FORM OF BID SECURITY (BID BOND)

BOND NO. *[insert **number**]*

BY THIS BOND *[insert **Name**]* as Principal (hereinafter called "the Principal"), and *[insert **Name**]*, **authorized to transact business in** *[insert **Jurisdiction**]*, as Surety (hereinafter called "the Surety"), are held and firmly bound unto *[insert **Purchaser Name**]* as Obligee (hereinafter called "the Purchaser") in the sum of *[insert **amount in figures**]* [6] (*[insert **amount in words**]*), for the payment of which sum, well and truly to be made, we, the said Principal and Surety, bind ourselves, our successors and assigns, jointly and severally, firmly by these presents.

WHEREAS the Principal has submitted or will submit a written Bid to the Purchaser dated the *[insert **ordinal number** day of [insert **month**] [insert **year**]*, for *[insert **name of Contract**]* (hereinafter called the "Bid").

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION is such that if the Principal:

(a)   withdraws its Bid prior to the Bid validity expiry date set forth in the Principal's Letter of Bid, or any extended date provided by the Principal; or

(b)   having been notified of the acceptance of its Bid by the Purchaser prior to the expiry date of the Bid validity or any extension thereto provided by the Applicant has failed to; (i) execute the Contract Agreement, or (ii) furnish the Performance Security in accordance with the Instructions to Bidders ("ITB") of the Purchaser's bidding document.

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

The Surety hereby agrees that its obligation will remain in full force and effect up to and including the date 28 days after the date of expiry of the Bid validity set forth in the Principal's Letter of Bid or extended thereto provided by the Principal.

IN TESTIMONY WHEREOF, the Principal and the Surety have caused these presents to be executed in their respective names this *[insert **number** day of [insert **month**] [insert **year**]*.

---

[6]   The amount of the Bond shall be denominated in the currency of the *Purchaser*'s Country or the equivalent amount in a freely convertible currency.

Principal: _____ Surety: _____
                                     Corporate Seal (where appropriate)

_____ _____
(Signature)   *(Signature)*

(Printed name and title)   *(Printed name and title)*

FORM OF BID-SECURING DECLARATION

[The Bidder shall fill in this Form in accordance with the instructions indicated.]

Date: *[insert **date (as day, month and year)**]*
Bid No.: *[insert **number of bidding process**]*
Alternative No.: *[insert **identification No if this is a Bid for an alternative**]*

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

We, the undersigned, declare that:

We understand that, according to your conditions, Bids must be supported by a Bid-Securing Declaration.

We accept that we will automatically be suspended from being eligible for bidding or submitting proposals in any contract with the Purchaser for the period of time specified in Section II – Bid Data Sheet, if we are in breach of our obligation(s) under the bid conditions, because we:

(a)   have withdrawn our Bid prior to the expiry date of the Bid validity specified in the Letter of Bid or any extended date provided by us; or

(b)   having been notified of the acceptance of our Bid by the Purchaser prior to the expiry date of the Bid validity in the Letter of Bid or any extended date provided by us, (i) fail to sign the Contract agreement; or (ii) fail or refuse to furnish the Performance Security, if required, in accordance with the ITB.

We understand this Bid-Securing Declaration shall expire if we are not the successful Bidder, upon the earlier of (i) our receipt of your notification to us of the name of the successful Bidder; or (ii) twenty-eight days after the expiry date of the Bid validity.

Name of the Bidder***** *[insert **Name of Bidder**]*

Name of the person duly authorized to sign the Bid on behalf of the Bidder*******[insert **Name of authorized person**]*

Title of the person signing the Bid*[insert **Title of authorized person**]*

Signature of the person named above‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗ ‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗‗

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

*: In the case of the Bid submitted by joint venture specify the name of the Joint Venture as Bidder

**: Person signing the Bid shall have the power of attorney given by the Bidder attached to the Bid

 [Note: In case of a Joint Venture, the Bid-Securing Declaration must be in the name of all members to the Joint Venture that submits the bid.]

SECTION V - ELIGIBLE COUNTRIES

Eligibility for the Provision of Information System

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

Under ITB 4.8(a) and ITB 5.1: *[insert a list of the countries following approval by the Bank to apply the restriction or state "none"].*

Under ITB 4.8(b) and ITB 5.1:   *[insert a list of the countries following approval by the Bank to apply the restriction or state "none"]*

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:

1. 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.

2. 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;

3. 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;

4. 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;[7] (ii) to be a nominated[8] 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;

5. 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[9] 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.

---

[7] 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.

[8] 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.

[9] 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.

PART 2 – PURCHASER'S REQUIREMENTS

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

Technical Requirements

Notes on preparing the Technical Requirements

The Technical Requirements – in combination with the Implementation Schedule and the supporting System Inventory Tables – state the Supplier's obligations to design, supply and install the Information System and, as such, should be "voiced" to the Supplier (i.e., "The System MUST …" "The Supplier MUST …"). They form the contractual basis for the Purchaser-Supplier interactions on technical matters (in combination with refinements introduced through the Supplier's bid, the Project Plan, and any Change Orders).

The Technical Requirements also must include all the technical details that Bidders will need to prepare realistic, responsive, and competitive bids (i.e., covering all their obligations under the Contract if so awarded). However, matters addressed to the Bidder's (i.e., before contract award) generally belong in the Format of the Technical Bid Section 8 of Part 1.

Often Technical Requirements are based on either consultant's project proposals (voiced to the Purchaser's management) or bids from previous procurements (voiced to the Purchaser). In both instances, care needs to be taken in converting these materials into Technical Requirements (voiced to the Supplier). Otherwise, substantial ambiguity will be introduced into the Technical Requirements from, among other things, "aspirational" text suggesting the benefits (to the Purchaser) which are often not obligations that the Supplier can deliver on or be held to deliver upon. Bid based language will often include "sales pitches", such as "expandability up to sixteen processors", whereas the Technical Requirements need to be stated as threshold values to be cleared by the Supplier (e.g., "expandability to at least sixteen processors").

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 bidding, the requirements must still be vendor-neutral and admit the widest possible range of technical responses.

Accordingly, references to brand names, catalog numbers, or other details that limit the source of any item or component to a specific manufacturer should be avoided. Where such references are unavoidable, the words "or substantially equivalent" should be added to permit Bidders to bid equivalent or superior technologies. (The Purchaser will need to be ready to indicate how this equivalence will be assessed.) Only in the most exceptional circumstances may Bidders be required to offer brand-name items and the equivalency clause be omitted. The World Bank's consideration for exception requires that:

> *(a)   a brand-name component appears to have no equivalent or superior alternative, because: of its unique ability to reliably interoperate with a relatively large base of existing technologies; to conform with the Purchaser's adopted technological standards; and to offer overwhelming savings in terms of avoided costs for retraining, data conversion, macro / business template redevelopment, etc.;*

> *(b)   the World Bank has agreed in advance, during project preparation, that such brand-name restrictions are warranted; and*

   (c) such brand-name components are the absolute fewest possible and each component has been explicitly identified in the Bid Data Sheet for ITB 16.3 .

Similarly, 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.

To help ensure comparable bids and ease Contract execution, the Purchaser's requirements must be stated as clearly as possible, with minimum room for differing interpretations. Thus, wherever possible, technical requirements should include definitive characteristics and quantifiable measures. If technical characteristics in a specific range, or above or below specific thresholds, are required, then these should be clearly specified. For example, the expandability of a server should be stated as "no less than four processors." Technical specifications that state only "four processors" create unnecessary uncertainty for Bidders regarding whether or not, for example, a server that could be expanded up to six processor boards would be technically responsive.

Quantitative technical specifications must, however, be employed with care. They can dictate technical architectures and, thus, be unnecessarily restrictive. For example, a quantitative requirement for the minimum width of the data path in a processor may be unnecessarily restrictive. Instead, 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.

It is important that the Technical Requirements clearly identify which are mandatory features (for which a bid's nonconformance might require rejection for non-responsiveness) and which are preferable features that can be included or excluded from a bid at the Bidder's option. To enhance the clarity of the specifications, Purchasers are advised to use the word "MUST" (in bold capitals) in sentences describing mandatory requirements. A clear requirements numbering scheme is also essential.

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

Any applicable sustainable procurement/environmental and social sustainability requirements shall be added to the technical requirements.

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 Particular Conditions if any) and other parts of the specifications.

3.0.4 below indicates noise levels and emission standard. Additional 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 and pollution prevention and management measures.

Technical Requirements

Table of Contents: Technical Requirements

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
	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

	Term	Explanation
	ppm	pages per minute
	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

B. FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS

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

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

1.1.1.1

- Data Protection Act 2019
- Computer Misuse and Cyber Crimes Act 2018
- National ICT Policy Guidelines 2020

[as appropriate, summarize: **each relevant legal code and regulations that govern the business processes and procedures that will be automated with the Information System***;]*

1.2 Business Function Requirements to be met by the Information System

1.2.1   The Information System MUST support the following business functions

1.2.1.2 …

Note: *These business process descriptions may be textual as well as presented in a formal system analysis formats (e.g., process model and data model, use-case model, entity-relation diagrams, swim-lane diagrams, etc.)*

As appropriate, prepare a subsection for the Background and Informational Materials with samples of existing standardized reports, data entry forms, data formats, data coding schemes, etc. which the Information System will need to implement; reference these materials.

Lot 1: Data Management Information System for the Office of the Data Protection Commissioner.

A comprehensive IDMIS business management solution making allowance for government procedures, web based and supports workflow with enhanced graphical user interface for simplicity and ease of use. An integrated adaptable and scalable IDMIS solution that fully supports IDMIS Processes and Functionality.

Tenderers to provide detailed sentence responses to each requirement indicating the level of compliance. They should attach datasheets, brochures or commitments and submit them together with the Tender document. The system should have modules and features which include but not limited to:

No	Requirement	Description	Tenderer's Response

| a) | **Registration Module** | •A client facing web-based system to enable data controllers and processors to register in line with the data protection act ,2019 and the attendant regulations.

•Platform for generating and publishing a list of registered data controllers and processors on the website in conformity with the regulations (14. (1) and subject to section 21 of the Act.

• Dashboard for tracking applications and their statuses in line with the act and the ODPC service charter.

•Provision for revocation of an entity's certificate of registration and automatic cancellation from the record and the register upon revocation.

•Provision for change or variation of registrations.

• Integration with the BRS system for validation and due diligence of both local and foreign companies operating in Kenya during registration.

•Backend for review of applications, approvals as per the defined workflows and policies.

•Provision for renewal of certificates prior or upon expiry.

•Emails and SMSs integration for push of notifications and reminders on action items relating to registrations.

• Auto generation of certificate for printing upon approval.

•Withdrawal of an application | |

•Categorization of application based on the counties, regions and the defined approval matrix.

•Integration with the existing systems and the approved payment platforms & gateways which include but are not limited to mobile money paybills and banks to ensure efficiency in payment of registration fees.

•Inclusion of a ticketing module linked to ODPC call center to ensure tracking and timely resolution of registration requests.

•Provision for querying and validation of a certificate.

b)	**Data breach Module**	• Creation of a data breach reporting module on the system. • Mapping of reported data breaches for actions as per the defined user roles and matrices. • Tracking of data breaches and their respective statuses.	
c)	**Compliance Module**	• Creation of a Data Privacy Impact Assessment (DPIA) module in line with the requirements. • A sub module for submission and approval of a data transfer request. • Provision for making requests for data protection advisories and tracking of advisories issued by the office. • Submission of Data Protection Impact Assessments • Emails and SMSs integrations for acknowledge receipt of Data Breach Notifications, advisory request, cross border transfer requests and DPIAs.	
d)	**Data Audits Module**	• Provision for data audit planning and reporting on the number of audits performed. • Randomized selection of entities to audit based on registration details (including sector, size, safeguards, etc.) • Provision for sending notifications/reports of data audits to controllers/processors	
e)	**Quality Assurance**	• Provision for a module for offer/issuance of certification of data protection seals and	

	Certification Module	marks to encourage data protection compliance by controllers and processors.	

f)	**Complaints, Investigation and Enforcement Module**	• End to end complaints module to enable data subjects to lodge complaints and allow internal staff to review the complaints as per the complaints handling procedure. •Provision for acknowledgement of a complaint by the office. • Provision for preliminary review of a complaint. • Notification of a complaint to a respondent. • Provision for investigation of a complaint as per the defined procedures. • Assignment of tasks to officers and tracking of their statuses. • Generation of automated register of complaints and their statuses. • Provision for withdrawal of a complaint by a data subject. • Discontinuation and notification of the same to the data subject and/or a respondent. • Transcription/ Hansard module to take complaints made over the phone through ODPC call center. • Automatic assignment of tracking numbers once a complaint has been lodged and if the complaint is against a DP or DC, the complaint can be linked to that particular entry.	

- Inclusion of the Alternative Dispute Resolution (ADR) mechanisms on to the enforcement sub -modules.

- Provision for reinstitution of a complaint after a decline/discontinuation.

- Ability for joint handling of a complaint.

- Provision for submission of determinations before the enforcement processes.

- Facilitate issuance of enforcement, penalty notices and administrative fines to data processors and / or controllers.

- Provision for appeals of determination, enforcement notices and penalty notices

- Provision for referral to ODPP for prosecution.

- Generation of automatic Enforcement registers.

- Provision for automated summons

- Provision for submission of an investigation report for approval.

- Application for review of enforcement notice(s) by a data subject.

- Integration with the existing systems and the approved payment platforms & gateways which include but are not limited to paybills and bank to ensure efficiency in payments for

		administrative fines and penalty fees. • Provision for prompts/alerts/notifications with time-based escalations incorporated in the workflow.	

	General Key Features	• Intuitive graphical interface for a short learning curve • Network ready with multi-user password control • Web Based • Email and SMS Integration • Integration with Bank payments- Card, bank Deposits and SWIFT • Process Workflow, Alerts and Embedded Document attachment • Reporting • Other characteristics of IDMIS	
	Workflow and Alerts	• Document, content management and intranet • Document Access Control • Workflow Configuration and Management • Alerts and notification on email.	

g)	**Reporting / Analytics**	• Advanced analytics and reporting on the number of breaches received, DPIAs submitted, complaints lodged and timelines for responding and level of compliance with the act and the service charter.	
		• Business intelligence capabilities and analytics based on registrations, data breaches, transactions and complaints reports. (Weekly, Monthly, Quarterly, Annual)	
		• Ability to generate performance reports based on service delivery.	
		• Annual Report to Parliament.	
		• Ad-hoc Reports (management reports).	
		• Custom Reports and Reporting Services	
		• Business Intelligence and Analytics - Integration with other corporate applications generating data	
		• Dashboard with Top level Graphical Analytics including forecasting	

h)	**System administration module**	• User Setup and Administration • Provision for automated backups and restore • Security Administration including application of security filters and privileges • Help desk • Incident reporting, ticketing and support • System Administration • Database Management • User Setup and Administration • Roles and access privileges administration • Workflow Configuration and Management • Audit Trails, Archiving • Automated backups and Restore • Reporting	

i)	**Help desk, ticketing and incidents reporting**	• Automatically assign tasks to officers and monitor tickets based on the service charter and generate tickets for each task. • Tracking of workflows and escalation matrix of tasks to ensure compliance and adherence to legal timelines. • Integration with call center services for timely resolution of enquiries as per the act and the service charter. • A platform for reporting of incidents and tracking of their resolution status. • A platform for customer feedback on ODPC services.	
j)	**System Maintenance**		
i)	**Carry out necessary maintenance of as per request**	• This include but not limited to: analysis of access logs, error logs and implementation of solutions to found exceptions	
ii)	**Code maintenance and upgrade on security management.**	• This include but not limited to: fine tuning of system errors, closure of any existing bugs and security loopholes • The bidder shall carry out proactive security updates and batching.	

iii)	**Security management and audit trail**	• System security and application administration • Audit Trails & archival of logs and	
iv)	**System restoration**	• The bidder in collaboration with OPDC will ensure the IDMIS's backups are up to date and are able to restore the IDMIS System in case of failure/hacking.	
v)	**Availability**	• The system has to be accessible 24 hours a day, 7 days a week from any part of the world with minimum if not zero downtime (99.9% availability).	
vi)	**Search Functionality**	• The vendor should implement a seamless search functionality to enable users to easily filter and search contents. • The contracted vendor will ensure the Search Engine Optimization (SEO).	
vii)	**Privacy**	• The system should ensure seamless user experience while ensuring security and privacy of information collected in line with the Data Protection Act, 2019 & Data protection Regulations, 2022	

viii)	**Vulnerability Assessment**	•The Vendor should perform a vulnerability assessment and submit a report for independent verifications by ODPC.	
ix)	**Licenses and software's**	• The Vendor should build and implement the IDMIS System on the latest platforms, technologies and software's	

———

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for Office of the Attorney General

The Office of the Attorney General and Department of Justice (OAG&DOJ) seeks to implement an integrated **Attorney General Information System (AGis)**. This unified platform will initially incorporate three modules, namely:

> **Module 1:** Legal Case Management System (LCMS)
> **Module 2:** Legal Opinion Database, **and**
> **Module 3:** Legislative Drafting Information Management System (LDIMS).

AGis aims to streamline legal services, legislative drafting, and legal opinion management, thereby improving efficiency, accessibility, and security across these critical functionalities.

AGis will be developed with scalability in mind, supporting up to 12 modules to handle additional functionalities for future requirements within the OAG&DOJ. The system will be built on a preferably open-source technology, ensuring adaptability, cost-effectiveness, and security while providing a foundation for expanding functionalities in response to the department's evolving needs.

Module 1: Legal Case Management System (LCMS)

The bidder must meet or exceed the following technical and functional requirements for the **Legal Case Management System.**

Category	Details
Case Management	Track case files, organize evidence, manage case timelines, and provide real-time case updates.
Client and Contact Management	Manage client interactions, external counsel details, and communication records.

Document Management	Secure storage, advanced search functionalities, version control, document automation, and e-signature support.
Task and Workflow Management	Assign tasks, monitor workflow progression, set reminders, and ensure seamless collaboration.
Reporting and Analytics	Generate insights on case durations, outcomes, productivity, and task completion rates.
Dashboard Overview	The system must provide a comprehensive dashboard that displays an overview of all cases, clients, lawyers/firms, trials, evidence, invoiced amounts, and other relevant case metrics.
Filtering & Search	The dashboard must allow filters based on case types, regions, case statuses, and other relevant parameters to enable efficient data retrieval.
Remote & Desktop Access	The system should allow users to organize and manage cases remotely through a web-based interface and on desktop applications.
Matter & Contact Linkage	The solution should link all contacts, tasks, and other case-related elements to their respective matters, e.g., linking witness contacts and parties' contacts to the case file.
Cause of Action Tracking	The system must support a Cause of Action feature, allowing the clear categorization of cases such as land disputes, labor cases, contracts, criminal matters, etc. This will help in tracking trends, preparing reports, and conducting legal research.
Notes & Reminders	The system must support sticky notes, reminders, and personal notes that can be sent to self or staff members as needed for efficient case tracking and follow-ups.

Virtual Tags & Trial Stickers	The bidder must ensure the system provides virtual tags, stickers, and notes for trial preparation, making it easy for staff to find relevant information quickly.
Research & Authorities Integration	The system should have a Legal Research Element, allowing users to attach lists of authorities and relevant research to specific matters. It should also integrate with electronic legal research databases (e.g., LexisNexis, Thomas Legal, etc.) for effective legal reference.
Legal Research Library	A centralized Legal Research Library must be provided, allowing users to create, store, and attach legal research materials to case matters.
Precedent Setting Cases	The system must flag precedent-setting cases and key case authorities to help in legal decision-making and argument preparation.
Judgment, Liabilities & Award Logs	The system must maintain records of judgments, liabilities, and financial awards, logging the date, amount, and responsible parties. If employees are found liable, the system should track surcharges and recovery of funds.
Case Timeline & Audit Trail	The solution should track all case developments with a detailed timeline, showing who made what changes and when. Users must be able to see new time entries, document uploads, and other case updates in real time.
User Accessibility & Mobility	The system must allow secure access to case files, tasks, and relevant information from anywhere, at any time, ensuring seamless remote and on-premises work.
Security & Compliance	The bidder must ensure that the system complies with relevant data protection laws and includes security features such as role-based access control, audit logs, and encrypted communications.

Calendar	
	Track ongoing matters in individual and departmental wide dashboards.
	Case alerts to enable users to be updated with court deadlines and other statutory deadlines.
	Set reminders
	Multiple notifications on different issues including case progress, case milestones, meetings, court dates etc.
Client Management	
	Easily organize contact details, documents, and communication logs from file opening to closure.
	Track office interactions with—clients, companies, outside counsel, witnesses, etc.
	Communication – track and manage client and office letters, emails and other forms of communication
Client portal	Enable clients and witnesses to communicate and collaborate with the State Counsel, provide witness statements, replying affidavits, responses and documents once mapped for a particular matter.
Status Update	Clients should have access to real-time case status updates as mapped.
Security	Files should be able to be stored and backed-up both on premise and offsite.
	Compliance with local and international data protection laws (e.g., Data Protection Act of Kenya, EU GDPR) to ensure privacy for clients and case data.

Document management	Access to documents from anywhere.
	Securely access, edit, and store your case files from anywhere with legal document software (case management system).
Permissions Control	The bidder shall demonstrate the implementation of user access management, including controls to regulate who can view, edit, and modify documents. The solution should support configurable permission settings to enforce access restrictions as required.
Advanced Search	Documents should be easily searchable either using keywords, clients, file reference, word, pdf and any other word processing document.
	Conflict search enabled using broad search terms such as subject matter, title, text content, or parties.
	Metadata search enabled (e.g. The size of the document, time it was created, author etc.)
	Ability to sort files by different categories e.g. department, parties, authors, dates, subject matter expandable.
Version Control	· The system must allow tracking of previous and updated versions of documents. · Must support "Track Changes" functionality similar to MS Word for document edits and updates.
Document automation tools	a) Automatically create letters and other key documents from predesigned templates (the Users will detail the design).
	b) Automate routine legal documents e.g. memorandum of appearance.

	c) Auto-fill and generate court returns and documents with pre-populated and synced data thus reducing risks of errors when completing forms.
	d) Convert existing Word files into reusable online templates.
Electronic Signatures	The system must support electronic signing of legal documents.
	a) Ensure that electronically signed documents are legally binding and admissible in court, meeting all jurisdictional requirements.
	b) Implement security measures to safeguard electronically signed documents from unauthorized access or tampering.
	c) Support access to electronically signed documents from anywhere, enhancing collaboration and efficiency in legal proceedings.
	d) Ensure compliance with established legal standards and robust security measures for electronic signatures.
Task management/ Workflow	
	a) Task allocation
	b) Review, prepare, and send documents for signature. No need to download, print or scan documents.
	c) Workflow enabling users to send tasks to the next user as required.
	d) Allow tracking of task progression

	e) Calendar editing and setting deadlines on tasks.
	f) Prioritize and sort tasks depending on urgency and importance.
	g) Schedule tasks and set reminders for deadlines to ensure that critical tasks are not overlooked and deadlines are met.
	h) Collaborate on legal documents and easily manage documents as a team.
	i) Create standardized task lists
	j) Build a series of tasks based on standard operating procedures for the office.
	k) Pre-define and order timing of pre-trial preparation.
	l) Set task deadlines, duplicate lists and assign task lists related to particular cases.
Integrations	Ability to integrate with other applications used in the office and internationally accepted ones.
	a) Integrations: Ability to integrate with other applications used in the office and internationally accepted ones.
	b) Integrations: Ability to integrate with other applications used in the office and internationally accepted ones.
	c) Integrate with the Kenya Judiciary Case Management System (appropriate name and requirements shall be provided by the Users).

Billing and invoice	) Requests for travel approval and payment of expenses.
	b) Payment for Court Travel payment etc link accounts with IFMIS and finance department.
	c) Payment vouchers for clients and cases with decretal awards against the government.
	d) Track the status of unpaid matters, or add automated interest to late payments as required.

Module 2: Legal Advisory Database

The bidder must demonstrate the proposed approach for implementing the Legal Advisory Database System.

Clean and Intuitive Interface	
Minimalist Design	· Keep the interface clean with minimal clutter. Use neutral colors (e.g., white, gray, and blue) to create a professional look.
Clear Navigation	· Implement a straightforward navigation system with main categories like "Search Opinions," "Saved Searches," "Recent Opinions," "Submit New Opinion," and "Profile Settings."
Breadcrumbs	· Display breadcrumbs to help users easily track their location within the database and navigate back to prior pages.
User Dashboard	· A personalized dashboard with quick access to recent searches, most-referenced opinions, and saved opinions should be displayed upon login.
c) Advanced Search and Filtering	

Keyword Search	· Implement a search bar that supports keyword search across metadata (e.g., case name, date, topic, jurisdiction) and full-text search within opinions.
Advanced Filters	· Users should be able to filter opinions based on various criteria, such as: ➢ **Date:** (e.g., year of issuance) ➢ **Type of Legal Matter:** (e.g., civil, criminal, administrative) ➢ **Department/Agency:** (e.g., Ministry of Health, Ministry of Finance) ➢ **Attorney General Signature:** (e.g., opinions authored by a specific AG)
Boolean Search Operators	· Allow the use of Boolean operators (AND, OR, NOT) for complex search queries.
Search Results Sorting	· Results should be sortable by relevance, date, agency, or case type.
d) Metadata and Categorization	

Opinion Metadata:	· Each opinion entry should include metadata such as: ➢ Title of Opinion ➢ Opinion Date ➢ Attorney General (author) ➢ Government Department or Agency involved ➢ Summary of the legal matter ➢ Status (e.g., active, withdrawn, amended)
Tagging System	● Allow tagging of opinions with multiple keywords or tags (e.g., "Constitutional Law," "Labor Dispute") to improve categorization and searchability.

e) Opinion View and Details Page

Structured Format	· Display opinions in a readable, structured format with clear headings (e.g., "Facts," "Legal Questions," "Opinion Conclusion").
Downloadable Formats	· Allow users to download opinions in PDF or Word format for offline review or sharing.
Cross-Referencing	· Display related opinions or previous precedents within the same page (e.g., "This opinion cites Opinion #123").

Version Control	· If opinions have been revised, ensure version history is available, with a clear comparison tool highlighting the changes.

f) Collaboration and Notes

Comments and Notes	❖ Enable users to add private notes to opinions for future reference, with an option to mark important sections of the document.
Collaboration Tools	· Implement collaborative tools (if required) for government attorneys to discuss opinions, share insights, or flag important cases internally.

g) Security and Compliance

Secure Access	· Implement multi-factor authentication (MFA) to ensure that only authorized personnel can access the system.
Data Encryption	· Ensure all legal opinions and associated data are encrypted, both at rest and in transit.
Audit Trail	· Keep an audit trail of who accesses and edits opinions to maintain accountability and transparency.

h) Mobile-First and Responsive Design

Mobile-First Approach	· Ensure that the database is fully responsive and can be accessed on various devices, including mobile phones and tablets, as attorneys may need access on the go.
Simplified Mobile UI	· For mobile devices, focus on simplifying the search and opinion retrieval process with

	fewer on-screen elements and larger buttons for touch input.

i) Error Handling and Feedback

Clear Error Messages	● Display meaningful error messages if users input incorrect search parameters or if there are system issues.
Loading States	● Show a loading indicator when search queries are processing, especially if large datasets are being queried
Autosave and Drafts	● For those submitting or editing opinions, auto-save should be enabled to prevent loss of work

j) Performance and Speed

Fast Search	● The system must be optimized for fast retrieval of documents, even when querying large datasets
Pagination or Infinite Scroll	● To handle large search results efficiently, consider using pagination or infinite scroll for result pages.

k) Training and Support

Help Section	● Provide an easily accessible help section or FAQs with common questions and user guides.
Tutorials:	● Onboarding tutorials or tooltips for first-time users explaining key features (e.g., how to filter opinions or save searches).

l) Integration with Other Legal Systems

● **APIs for Integration**	● The system must be capable of integrating with other government or legal databases, as needed, to ensure seamless data exchange. This includes, but is not limited to, linking with court databases, legal precedent databases, and other relevant legal information sources. The integration should be smooth, secure, and allow for real-time data synchronization and retrieval to enhance the system's functionality and user experience.

m) User Feedback and Reporting

● **Feedback Mechanism**	● Include a feedback tool for users to report issues, suggest features, or request changes.
● **Usage Analytics**	● Admins should be able to access usage analytics to understand how the system is being used and optimize it further.

9. Summary of Salient Features

The proposed legal advisory database or portal should possess the following salient features:

Comprehensive indexing	● Implement a robust indexing system to categorize legal advisories by topic, legal issue, date, and other relevant criteria.
Full-text search	● Allow users to search the full text of legal advisories for efficient retrieval of specific information.
Advanced search capabilities	● Offer options for filtering search results by date range, issuing department, and other criteria.
Headnote and summary	● Include clear and concise headnotes and summaries for each legal advisory to provide a quick overview of the key points.

Internal citations	● Enable easy navigation between interconnected legal advisories through internal citations and links.
Annotation capabilities	● Allow authorized users to annotate legal advisories for internal reference and knowledge sharing.
Version control	● Track changes made to legal advisories and maintain a history of all versions for audit purposes.
Security measures	● Implement robust security measures to restrict unauthorized access and ensure data confidentiality. This may include role-based access control, encryption, and audit logging.
User roles and permissions	● Establish a user role management system to grant different access levels (e.g., read-only, edit) based on user needs.
User interface	● Provide a user-friendly and intuitive interface that is easy to navigate and search.
Accessibility	● Ensure the system complies with accessibility standards to accommodate users with disabilities.
Reporting tools	● Generate reports on usage statistics, search trends, and other relevant data to inform decision-making and system optimization.
Integration capabilities	● Consider potential for future integration with existing OAG&DOJ systems for centralized information management.
Mobile	● Compatibility to access the system from mobile devices.
Category	**Specifications/Requirements to be Met by the Bidder**

Document Upload & Storage	● System should accept uploads of legal advisories in multiple formats (PDF, Word, etc.).
	● Ability to upload new legal advisories and categorize them based on criteria such as date, subject matter, issuing department, and clients.
Metadata & Categorization	● Allow for easy addition of metadata to each legal advisory, including date, subject matter, issuing department, keywords, and case citations.
Version Control	● Facilitate version control to track changes made to legal advisories.
Access Control & Security	● Implement a secure access control system with user roles and permissions.
System Integration	● Capability to integrate with existing Electronic Documents and Records Management Systems (EDRMS) for seamless data transfer.
-	● Integrate with existing Office of the Attorney General & Department of Justice (OAG&DOJ) knowledge management systems and Case Management System.
	● Ability to integrate with other e-repositories locally and internationally recognized (e.g., Lexis Nexis, Kenya Law).
Legal Opinion Submission	● An interface for State Counsel in the MDAs to upload their preliminary legal opinions.
Collaboration & Annotations	● Ability to add sticky notes and send notes to self or staff as necessary.

Tagging & Quick Reference	● Implement Virtual Tags and Stickers to enable staff to find relevant information quickly and make User Briefs responsive.
Research & Legal References	● Research Element: System should allow attachment of List of Authorities and other relevant research to matters.
	● Legal Research Library: Maintain a user's legal research in one place with other integrated legal research libraries
	● System must integrate with paid electronic legal research databases (e.g., LexisNexis, Thomas Legal).
	● Allow users to create legal research globally and attach it to matters to create effective precedents.

Module 3: **Legislative Drafting Information Management System (LDIMS)**

Functional Requirements/Business Requirements	
1. Bill and Subsidiary Legislation Management:	
	● Register and track requests for legislative drafting from MCDAs.
	● Assign and track tasks to Parliamentary Counsel based on expertise, workload, and type of legislation (Bill or subsidiary legislation).
	● Manage the progress of drafts through various stages (instructions received, research, drafting, review, approval).

	● Track and display information on existing legal acts to be altered or implemented by the draft law or regulation.
	● Generate detailed feedback loops (e.g., surveys, performance dashboards, and user satisfaction metrics) ● The system should generate a unique reference number for each file recorded, specific to the Offices, Ministries, Agencies, and other Institutions from which the instructions are received.
	● Compliance Validation: Validate drafts against statutory requirements and legal standards.
	● Comparisons: See how drafts will change the law in clear details
	● Links and reference to laws appear as the user is drafting
	● Access the law in effect as the user is drafting
	● Identify and alert users to potential conflicts or duplications with the current draft - (by use of Business Intelligence)
	● Record and manage requests for legal opinions.
	● Collaboration between Parliamentary Counsels working on the same draft.
	● Incorporate workflow automation tools (e.g., task assignment, review cycles with built-in approval mechanisms, and automated task progression) to further enhance the legislative drafting process.
	● Integrate with version control systems to track changes made to drafts.

	● Integrate robust proofreading tools (e.g., grammar and legal structure checks) to further enhance the quality of legislative drafts
	● Automated legal proofreading to check for formatting, citation, and statutory compliance to reduce human error.
	● Maintain a record of revisions and changes made to drafts.
	● Maintain an archive of finalized Bills and subsidiary legislation.
	● The system must allow the categorization of files into Bills, Proclamations, Regulations, Government Notices, General Notices, and other future inputs. This can be achieved using dropdown menus or tabs for different types of instructions, with each instruction having its own template.
2. Document Management:	
	● Automate core processes of the legislative drafting workflow as defined in the LDD SOP (e.g., routing drafts for review, amendments, and managing approvals).
	● Automated Comparison: The system should compare sections in a legislative proposal with the master statute databases.
	● Change Detection: Detect any changes that have not been correctly formatted and highlight discrepancies.
	● Generate reports on changes and amendments efficiently.

	● Secure storage of legislative documents, including draft Bills, subsidiary legislation, memoranda, instructions, revision notes, and communication records.
	● Maintain version histories for all drafts and amendments and automatically generate amendment instructions from a marked-up version of a bill.
	● The system should have the capability of uploading/scanning of related document to form part of the file.
	● Maintain version histories for all drafts and amendments and automatically generate amendment instructions from a marked-up version of a bill.
	● The system should have the capability of uploading/scanning of related document to form part of the file.
	● The system should have provision for additional fields to be added by user if needed.
	● The System must provide a method for automatically linking events, file status changes, documents, and correspondence. Summery reports (History of the tile from initial state lo date)
	● Enable easy retrieval of documents based on various criteria (Ministry, date, subject matter).
	● Integrate with existing document management systems or EDRMS within the OAG&DOJ
	● The system should provide customizable templates for bill drafting based on predefined legislative formats.

	● Automated Proof-reading: Check drafts for grammatical, typographical, and formatting errors. ● Automated notifications for pending tasks, approvals, and deadlines.
	● Document approval workflow with digital signatures.
3. Legislative Research:	
	● Provide access to a comprehensive legal research library containing Kenyan legislation, case law, parliamentary materials, and relevant international legal instruments.
	● The system should include advanced search functionalities to retrieve specific legal information efficiently.
	● Integrate with external legal databases e.g Kenya Law
	● The system should include analytical tools to generate reports on legislative trends and highlight key focus areas based on historical data.
4. Communication	
	● The system should enable seamless communication between Parliamentary Counsel, Ministries, and other stakeholders through integrated messaging and notification features.
	● Enable communication with requesting entities for clarifications, feedback, or updates.
	● The system should enable real-time collaborative document editing and annotations for authorized users

	● Track correspondences by individual and by individual involvement to a particular instruction
	● The system should allow one to set reminders/notifications/alerts escalated notification to immediate supervisor)
5. Reporting:	
	● Generate reports on the volume and types of legislative drafting requests received.
	● Generate reports on the status of requests, drafts, and approvals.
	● Record metadata on the legal basis for the adoption of laws or regulations. Store dates of adoption, entry into force, and application dates. ● Track performance metrics like turnaround time for completing drafts.
	● Dashboard for monitoring overall progress and key performance indicators (KPIs).
	● It should be capable of producing data and collective summaries, including a quarterly report of the completed work of legislative drafters based on agreed metrics. Additionally, the system should be able to monitor and manage workflow and produce summaries accordingly.
	● Historical Data Analysis: Support for historical data reporting and trend analysis to track legislative drafting performance over time and identify areas for improvement.

	● Options to export reports in various formats (e.g., PDF, Excel) for sharing with stakeholders, as well as secure sharing mechanisms within the system.
	● Ensuring that reporting features are aligned with role-based access controls, allowing appropriate access to reports based on user permissions.
6. Legislative Tracking:	
	● Track the progress of Bills through Parliament, including committee stages, second reading, and third reading.
	● Monitor further proposals to the Bills from MDAs for onward transmission to the parliament.
	● The system should track progress, have a section for comments of actions taken and Status of file.

Technical Requirements	
7. Security:	
	● Implement user authentication and role-based access control to restrict access to sensitive information.
	● Ensure data encryption for storage and transmission of legislative documents.
	● Adhere to relevant legal and regulatory requirements regarding data privacy (e.g., Kenya's Data Protection Act, GDPR, HIPAA) and security standards (e.g., ISO 27001).
	● Secure login with multi-factor authentication.
	● Implement logging mechanisms to track user activities and access attempts. Monitor login attempts for anomalies and potential security breaches.
	● Real-time monitoring of system performance, availability, and security metrics.

	● Automated alerting mechanisms to notify ICT personnel of potential issues or anomalies that may indicate a disaster or compromise.
8. Scalability**:**	
	● The system should be able to accommodate an increasing volume of legislative drafting requests and documents.
9. User Interface:	
	● Develop an intuitive user interface (UI) that is user-friendly and supports efficient navigation and task completion. Consider customizable views and dashboards tailored to different user roles and tasks.
	● Implement session timeout controls and mechanisms to prevent unauthorized access due to idle sessions. Provide options for users to securely log out and manage their active sessions.
	● Offer support for Kiswahili (in addition to English) to enhance accessibility.
	● The system should have a language tool (Grammar and spell check)
10. Integration:	
	● Compliance and Standards Integration: Ensure integration with regulatory compliance standards such as the Statutory Instruments Act, 2013, and other legal frameworks relevant to legislative drafting and publication processes.
	● Workflow Integration: Implement integration of workflow processes to facilitate smooth transitions between drafting stages, review cycles, and approval procedures. This ensures that all stakeholders are informed and involved at each step of the legislative drafting process.
	● Reporting and Analytics Integration: Integrate reporting and analytics capabilities to generate insights into legislative drafting timelines, efficiency metrics, and compliance with legal requirements. This supports decision-making and process improvement initiatives.
	● Incorporate advanced data analytics (e.g., predictive trends, drafting efficiency patterns, and

	real-time legislative impacts) to enhance decision-making.
	● Implement AI-driven insights to help identify drafting bottlenecks and opportunities for process improvement.
	● Integrate with existing government ICT systems like email, calendar, and document management systems.
	● Integrate with e-Parliament platform (if applicable) for tracking Bill progress
11. Accessibility:	
a) Accessibility Standards:	● Ensure compliance with accessibility standards (e.g., WCAG 2.1) to accommodate users with disabilities. This includes support for assistive technologies such as screen readers and keyboard navigation.
b) Secure Remote Access:	● Enable secure remote access to the system, possibly through VPN or secure web portal, ensuring encrypted communication channels to protect data in transit.
	● Optimize the system for mobile devices to facilitate access from smartphones or tablets, ensuring responsiveness and usability across different screen sizes. It should also have offline capabilities (Given the nature of legislative work, drafters might need access to documents or drafting features in areas with limited connectivity).
12. Audit Trail:	
	● Maintain a comprehensive audit trail to track all actions performed within the system, including user activity and changes made to documents.
	● Log the identity of the user performing the action, including their username or unique identifier, to attribute actions accurately.
	● Implement measures to ensure that logged events cannot be altered or deleted by users, maintaining data integrity and accountability.

	● Provide authorized personnel with the ability to review and search through audit logs efficiently for investigation and compliance purposes.
	● Define a retention policy for audit logs that complies with regulatory requirements and organizational policies, ensuring logs are available for audits and investigations.
	● Integrate audit trail data with system monitoring tools to detect anomalies or suspicious activities in real-time.
	● Set up alerts or notifications for critical events or deviations from normal user behavior, prompting immediate review and response.
13. **UI/UX Guidelines:**	
a) User Roles & Permissions	
	● Implement a clear role-based access control (RBAC) system. Different users (attorneys, researchers, administrators, clerks) should have access only to relevant data and features.
	● Display only the necessary tools/features for each user's role to reduce clutter.
	● Provide visual cues or restrictions on actions for users with limited permissions (e.g., grayed-out options for restricted actions).
b) Dashboard for Quick Access	
	● Develop a customizable dashboard with an overview of pending, recent, and historical opinions. Users should quickly access recent opinions, popular requests, and active matters.
	● Use widgets or panels that show recent activities, deadlines, and popular topics.
	● Allow customization based on user preferences (drag-and-drop widgets or filtering options).
	● Provide search summaries for frequently referenced legal matters.
c) Advanced Search & Filtering	
	● Create an intuitive, robust search engine with advanced filters (e.g., by date, issue area, opinion number, attorney, department). Users need to retrieve legal opinions and documents quickly and accurately.

	● Include autosuggestions as user's type keywords, making searches faster and more intuitive.
	● Allow complex query building (e.g., Boolean search) for power users.
	● Enable filtering by metadata such as date range, type of opinion, relevance to specific laws, or department requested by.
d) Document Management System (DMS)	
	● Implement a document management interface where users can view, download, or annotate opinions. Users will need quick access to both digital and historical records.
	● Provide document previews or snippets for fast scanning.
	● Include version control for opinions and track amendments or supplements to legal opinions.
	● Add features for attaching related documents or linking opinions to specific cases or laws.
e) Opinion Creation Workflow	
	● The system should include customizable templates to standardize the drafting of legal opinions and legislative documents.
	● Streamline the drafting process to ensure uniformity and ease of use across the system.
	● Use guided steps or a wizard for the drafting process, with drop-down options for categorizing opinions (legal area, government entity, etc.).
	● Autosave functionality to prevent data loss.
	● Option for users to input citations and related case laws through an integrated library or reference system.
f) User-Friendly Interface with Legal Jargon	
	● Simplify complex legal terminologies without sacrificing accuracy. Users of varying legal expertise will use the system.
	● Tooltips or info popups to explain specific legal terms or jargon.
	● Allow tagging of documents with user-generated keywords to assist non-legal personnel in searching documents.

	● Simplify labels and form field instructions, using plain language where possible.

g) Access to Historical Opinions	
	● Ensure historical opinions are well organized and easily searchable by year, topic, or issuing attorney. State Counsels often reference older legal opinions when drafting new ones.
	● Archive views with pagination or infinite scrolling for large datasets.
	● Filter by administration (presidential terms) or key events (e.g., constitutional amendments).
h) Audit Trails & Document History	
	● Track and display edits, reviews, and approvals of legal opinions. Legal documents need a detailed audit trail for accountability and transparency.
	● Provide a "Document History" tab showing who edited what and when.
	● Allow comments, approvals, or rejections within the opinion draft workflow, making collaboration easier.
	● Notifications for changes in critical legal documents.
i) Collaboration Features	
	● The system should provide features to enable collaborative drafting and reviewing of legal opinions among authorized users.
	● Integrate real-time document editing or comment sections for peer review and discussion.
	● Allow "mentions" or task assignments within the document for team collaboration.
	● Enable tracking of who has viewed and signed off on an opinion.

j) Responsiveness and Mobile Access	
	● Ensure that the system is mobile-friendly for access on tablets and smartphones. Legal professionals often work remotely or need quick access to documents outside of their offices.
	● Design for touch interaction with large buttons and dropdowns that are easy to navigate on small screens.
	● Ensure seamless transition from desktop to mobile for continued document access.
	● Provide offline access for essential documents or opinion drafts.
k) Data Security & Privacy	
	● Prioritize security features like encryption, two-factor authentication (2FA), and access logs. Legal opinions contain sensitive governmental information.
	● Make sure access logs and warnings about unauthorized access are easily visible.
	● Use visual alerts for data sensitivity classifications (e.g., confidential, public).
	● Ensure that secure login screens and document encryption protocols are visible but not intrusive to the user experience.
l) Legal Reference Integration	
	● Integrate external legal references, case law databases, and relevant statutes. Legal opinions often cite laws, statutes, and previous cases.

	● Offer cross-referencing capabilities to pull in relevant legal precedents or statutory laws within the drafting interface.
	● Provide a side-by-side view or pop-up when referencing laws or statutes in an opinion.

m) Notifications and Alerts

	● Include notifications for updates, pending approvals, or deadlines related to opinions. Time-sensitive legal matters need proactive alerts.
	● Implement email and system notifications for users on important updates (opinion finalizations, due dates, etc.).
	● Ensure critical alerts are prominent on the dashboard, such as opinions due for review or response deadlines.

n)   Visual Consistency & Branding

	● Use consistent branding and styling throughout the application to reflect the Attorney General's Office. Maintain a professional and cohesive look that reflects authority and trust.
	● Utilize the office's official color scheme and typography.
	● Keep layout clean, with sufficient white space and standardized button styles, fonts, and icons for easy navigation.

o)   Accessibility Standards (WCAG)

	● **Guideline:** Follow WCAG (Web Content Accessibility Guidelines) to make the system accessible to all users. Legal systems must be accessible to people with disabilities.

	● Ensure compatibility with screen readers.
	● Use high-contrast designs and larger fonts for readability.
	● Enable keyboard navigation for users with mobility impairments.

14. Training:

	● The system should incorporate user training modules and self-learning resources to facilitate capacity building for Parliamentary Counsel and other users.
	● The system should be accompanied by structured technical documentation and user manuals to enable ICT personnel to conduct first-line support.

15. Technical **Support:**

	● New systems should be able to operate in a virtual environment.
	● The system should be able to run on multiple operating systems e.g. Windows, Linux.
	● The system should have lifetime licensing, including free updates for the first five years from the time the entire system goes live.
	● ICT staff should be granted full privileges.
	● The system should include a structured support mechanism for a period of 24 months, with detailed service-level requirements to be fulfilled by the implementing entity.
	● Client support should be available through technical support, email, and telephone.
	● Clear and detailed maintenance activities and duties should be performed on the system (quarterly, bi-annually, annually).

16. **Disaster Recovery:**

	● The system must include a disaster recovery mechanism to ensure business continuity in case of system outages or data loss.

	● The system should have inbuilt capacity for regular and automated backups of all system data, configurations, and documents.
	● The system should have built in mechanism that restores data quickly to minimize downtime in case of data loss.

17. Data Migration:	
	● The system should include tools and functionalities to facilitate the migration of existing legislative drafting data while ensuring data integrity.
	● The system should support data extraction, integrity validation, and lineage tracking to ensure seamless transition from legacy systems.
	● The system must include automated validation processes to ensure data migration meets predefined quality standards and business rules set by the OAG&DOJ.
	● The system should support automated testing functionalities to verify the accuracy, completeness, and consistency of migrated data, including the use of sample data sets and edge cases.
	● The system should include built-in rollback mechanisms, backup functionalities, and data recovery tools to address potential migration failures or data corruption.
	● The system should provide logging and troubleshooting tools to address data integrity issues post-migration.

18. Key deliverables	
	a) The supplier must deliver a system that meets the predefined functional and non-functional requirements.
	b) The system must be designed to integrate all components seamlessly as per the approved specifications.
	c) **Source Code and Compiled Software**: The supplier should deliver the system together

	with its source code to enable future maintenance and upgrades.
	d) **User and Technical Documentation**: The system should include built-in manuals, guides, and help files that assist end-users in operating the system effectively.
	e) **Training Materials and Sessions**: The system provider should deliver structured training materials and facilitate initial user training to ensure proficiency in system use.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

FUNCTIONAL REQUIREMENTS FOR KENYA PRISON SERVICES

Integrated Correctional Management Information System

(ICMIS), Kenya Prisons Service

1.0	RECEIVING A PRISONER	(FS,PS,CR,NS)	REMARKS
1.1	a. The system should be able to capture prisoner's name, prisoner number, case number, source (transfer, court or hospital), and status i.e. remand, convicted, Borstal, Youth Correctional Training Centre (YCTC) and capture all the information in the warrant. b. Ability to knockout/ knock in movement of prisoners.		

	c. Ability to capture CAM10 (children under the age of 4yrs accompanying their mothers). d. Ability to auto generate and alert on the number of times the prisoner has been detained.		
1.2	a. The system should be able to identify and verify the prisoner details captured during the search process. b. The system should be able to Capture biometric data.		
1.3	c. Ability to assign admission number		
1.4	d. Ability to view and clear the prisoner to be admitted into prison (by the duty officer during the day and sleeping-in officer during the night). e. Ability to timeout the duty officer after		

	final lockup, and sleep-in officer after unlock. f. Ability to show status of a prisoner who has been denied entry into prison, reasons and the clearance (authorization) by the officer in charge.		
2.0	**ADMISSION**		
2.1	a. The system should have ability to categorize prisoner into: male, female, Intersex; Convicted, remand; Borstal boys, Borstal Girls; Youth Correctional Training Centre (YCTC); Terrorism and terrorism related; serious organized crime.		
2.2	b. Ability to capture result of medical screening using PF10 register and notify the medical officer for medical attention.		

| 2.3 | c. Ability to capture additional information upon profiling using PF1 form, Property, valuable, cash, weight, photo, transfer information, initial assessment results, details of accommodation assigned and personal items issued, appeal status if convicted, pending cases, previous convictions, and multiple cases for convicted.

Ability to have prisoner cash management module

d. Ability to verify the captured details with prisoner's biometrics. | | |
| 2.4 | e. Ability to capture and categorize prisoner's disposable items, action taken and who authorized the action.

f. Biometric approval by the prisoner of his/her items on actions taken above. | | |

2.5	g. Ability to capture next of kin details and notify them.		
3.0	**RISK ASSESSMENT**		
3.1	a. Ability to categorize risk assessment, and ability to share risk assessment report upon transfer b. Ability to capture risk factors based on risk assessment tools c. Ability to capture results of each assessment i.e. high/medium/low based on risk assessment reporting template. d. Ability to add and identify security interventions based on risk assessment input, age, health, sentence etc. e. Ability to identify the appropriate security infrastructure based on the risk level. f. Ability to generate risk assessment report		

4.0	**NEED ASSESSMENT**		
4.1	a. Ability to capture criminogenic factors b. Ability to capture results of need assessment based on needs assessment reporting template. c. Ability to identify interventions based on "b" above. d. Ability to generate needs assessment report		
5.0	**CLASSIFICATION OF PRISONERS**		

5.1	a. Ability to retrieve prisoner's details including risk assessment report and intervention plan in-order to classify them based on risk level. b. Ability to assign and categorize security regime i.e. restricted/normal regime. c. Ability to select proposed security interventions and management plans. d. Ability to allocate accommodation. e. Ability to alert in event there is change in accommodation. f. Ability to use access control and CCTV to regulate and monitor movement within the facility. g. Ability to notify any irregular movement within the facility. h. Ability to send alerts in case of any emergency to the relevant authorities.	

	i. In case of serious incidents like riots it should deactivate all control rooms and activate the main command center to take control.		
	j. The system should allocate the next station to a prisoner and time limit upon clearance and give alerts in the event of exceeding the time limit or change in the allocated station.		
	k. Ability to capture the details of a prison officer escorting the prisoner in and out of an accommodation unit.		
	l. Ability to discharge prisoners from the accommodation unit.		
6.0	**DISENGAGEMENT, DE-RADICALIZATION, REHABILITATION, EMPOWERMENT**		

6.1	a. Ability to categorize Disengagement, De-radicalization, Rehabilitation and Empowerment.		
	b. Ability to retrieve prisoner's details including needs assessment reports and sentence plans.		
	c. Ability to assign the intervention, measures, programs and deployments to be undertaken then match with the intervention provider.		
	d. Ability to capture intervention progress reports provided by the provider.		
	e. Ability to show intervention status.		
	f. Ability to generate a report		
7.0	**COMPUTATION AND REMISSION OF SENTENCE**		

7.1	a. Ability to sort those who are eligible or not eligible for remission.		
	b. Ability to categorize types of sentence computation		
	i. Normal sentence		
	ii. Concurrent sentences		
	iii. Consecutive sentence		
	iv. Overlapping sentences		
	v. After Recapture where a prisoner has been apprehended within 30 days		
	vi. Recapture where a prisoner has been at large for more than a month		
	vii. Computation for substantive sentence		
	viii. After loss of remission		
	ix. Upon appeal		
	x. Commutation		

	xi. Revision xii. Petition xiii. Upon grant of further remission xiv. After deprivation of remission. (standing order No.92, there are other formulas dictated by court) c. Ability to allow customized computations based on orders and directives (Above customized computation should have a workflow with different levels of approvals).		

8.0	**RECEPTION BOARD**		
8.1	a. Ability to review prisoner's details and reports. e.g. dashboard b. Ability to capture board's resolutions and assign them to respective officers for action. c. Ability to notify reception board members to conduct a reception board d. Generate reception reports		
9.0	**DISCHARGE BOARD**		
9.1	a. Ability to review prisoner's details and reports. e.g. dashboard b. Ability to capture board's resolutions and assign them to respective officers for action. c. Ability to assign a proposed person/institution that will support the prisoner upon release.		**Discharge board is composed of internal and external stakeholders.**

	d. Ability to automatically notify and refer to external agencies and generate a report for notification e. Ability to automatically notify and refer to external agencies and generate a report for notification. f. Generate discharge reports		
10.0	**PRISONERS DISCIPLINE**		
10.1	a. Ability to retrieve prisoner's information b. Ability to add, update and retrieve offences and sanctions. c. Ability to capture sanctions and automatically compute new release dates.		
11.0	**COURT PRODUCTION**		

| 11.1 | a. Ability to categorize different productions

b. Ability to retrieve/add/update court related information for both physical and virtual court sessions.

c. Ability to send notifications on due court production.

d. Ability to track prisoner movement out of prison.

e. Generate production reports | | **Notifications to be sent at least a day before the due date.** |
| 12.0 | **TRANSFER OF PRISONER** | | |

12.1	a. Ability to categorize transfer type into on-court order or upon request by OIC through form PF17 attaching form PF43, assessment reports, PF10 , PF1 and relevant documents		
	b. Ability to retrieve /capture and update prisoner's transfer details.		
	c. Ability to notify OIC of the receiving station.		
	d. Ability to generate transfer requests		
	e. Ability to track prisoner's transfer history.		
	f. Ability for the system to integrate with the Fleet Management System.		
	g. Ability to generate reports.		
13.0	**REMOVAL OF A PRISONER FROM PRISON**		

13.1	a. Ability to categorize removals e.g. hospital, mental facility, leper settlement.		
	b. Ability to retrieve/ add and update medical information.		
	c. Ability to track prisoner movement and location.		
	d. Ability to show prisoners treatment status.		
	e. Ability to generate reports with relevant institutions		
	f. Ability to generate removal reports.		
14.0	**BORSTAL**		

| 14.1 | a. Ability to select and confirm availability of a vacancy

b. Ability to receive and process requests

c. Ability to categorize Borstal facility.

d. Ability to track availability of vacancy.

e. Ability to allocate a Borstal facility.

f. Ability to alert in event there is change in accommodation.

g. Ability to use access control and CCTV to regulate and monitor movement within the facility.

h. Ability to notify any irregular movement within the facility.

i. Ability to send alerts in case of any emergency to the relevant authorities.

j. In case of serious incidents like riots it should deactivate all control rooms and activate the main command center to take control. | | |

<table>
<tr><td></td><td>

k. The system should allocate the next station and time limit upon clearance and give alerts in the event of exceeding the time limit or change in the allocated station.

l. Ability to capture the details of an officer escorting the Borstal girl/ Borstal boy out of the accommodation unit.

m. Ability to discharge Borstal girl/ Borstal boy from the accommodation unit.

</td><td></td><td></td></tr>
<tr><td>**15.0**</td><td>**PRESIDENTIAL PARDONS**</td><td></td><td></td></tr>
</table>

| 15.1 | a. Ability to retrieve prisoners' details.

b. Ability to review prisoners' petitions to confirm eligibility.

c. Ability to capture petition requests.

d. Biometrics approval by the prisoner.

e. Ability to forward the request to Power of Mercy

f. Ability to capture and track status.

g. Ability to track the petition status .

h. Ability to generate pardon reports | | |
| **16.0** | **OTHER PARDONS** | | |

16.1	a. Ability to retrieve prisoners' details.		
	b. Ability to review prisoners previous pardon status for eligibility.		
	c. Ability to capture the pardon request.		
	d. Biometrics approval by the prisoner.		
	e. Ability to submit the pardon request.		
	f. Ability to capture and track status.		
	g. Ability to capture the decision about the requested pardon.		
	h. Ability to generate reports.		
17.0	**ESCAPE**		
17.1	a. Ability to categories escapes		
	b. Ability to retrieve prisoner's details		
	c. Ability to capture reports		
	d. Ability to generate reports on escape.		

	e. Ability to track the status of escape and if recaptured the system should compute new dates of release.		
18.0	**DEATH OF A PRISONER**		
18.1	a. Ability to retrieve details b. Ability to capture death reports c. Ability to discharge the body d. Ability to generate reports		
19.0	**DISCHARGE OF A PRISONER**		

19.1	a. Ability to categorize types of discharge		
	b. Ability to retrieve details		
	c. Ability to capture discharge report		
	d. Ability to notify OIC and CGP.		
	e. Ability to notify other agencies upon discharge		
	f. Ability to generate reports		
	g. Ability to generate certificate of completion for the prisoners		
20.0	**VISITATION**		

20.1	a. Ability to categorize types of visits. b. Ability to capture visitors' details. c. Ability of a visitor to make visitation request d. Ability to process requests and notify the visitor on progress e. Ability to track the visitor movement and notify them of the time allocated. f. Ability to map prisoners' details to the visitor. g. Ability to notify the OIC and the duty officer of any visitors who have exceeded time allocated. h. Ability to generate reports		
21.0	**LOCKUPS AND UNLOCKS**		

21.1	a. Ability to categorize different types of counts (morning unlock, midday lockup, Midday unlock). b. Ability to confirm the number of prisoners' tally with biometrics counts. c. Ability to use biometrics for lockups and unlocks.		
22.0	**YCTC (Youth Corrective Training Center)**		
22.1	a. Ability to capture details of youthful offenders b. Ability to allocate activities. c. Ability to capture time management scheduleAbility to capture report d. Ability to generate report		

23.0	**INTEGRATED COMMAND AND CONTROL CENTER (C&CC)**		
23.1	a. The Integrated command and control center at the prison headquarters should be linked to other command centers within the stations. b. Ability to provide a unified view of the prisons. c. Ability to communicate with other intelligent components of ICMIS. d. Ability to disable all other sub command and control centers (within the stations). e. Ability to notify the C&CC controller and Commissioner General of Prisons (CGP) in the event of a security breach. f. Ability to detect and notify the C&CC controller and CGP		

	in the event of attempted penetration to the system. g. Ability to integrate a 3D view of every prison. h. Ability to generate customized alerts to other security agencies. i. Ability to integrate with access control systems.		
24.0	**MEDICAL TREATMENT OF PRISONERS INSIDE THE PRISON**		
24.1	a. Ability to retrieve/ add and update medical information. b. Ability to track prisoner movement and location.		

	c. Ability to show prisoners treatment status. d. Ability to generate referral reports.		
25.0	**RATION STORE MANAGEMENT**		
25.1	a. Ability to retrieve prisoners' details. b. Ability to capture the amount and type of food received in a ration store. c. Ability to compute amount and type of food allocated to each prisoner on daily basis d. Ability to compute the cumulative amount of food to be released per day based on the number of prisoners In a prison e. Ability to ascertain food balance in the store		
26.0	**USER MANAGEMENT AND PRIVILEGES**		

26.1	a. The system must utilize username and password to authenticate users and support two-factor authentication to strengthen access control when necessary.		
	b. Role-based access control shall be used to define content and functionality applicable to users. This must be in line with the user's job function or role.		
	c. Reports must only be accessed by authenticated and authorized users in line with their job function or role. Only authorized users must be able to edit or make changes to data.		
27.0	**REPORTS**		
27.1	a. Ability to generate reports for all the modules above		
	b. Ability to show report in different graphical representation		

	c. Ability to export the reports to different formats e.g. excel etc. d. Ability to have a dashboard with Analytics presentations.		
28	**Kenyan Offenders Incarcerated Abroad**		
28.1	a. Ability to capture all person details including and not limited to Name , Age, Passport number, ID number, Photo, Language Spoken, and Biometrics b. Ability to capture the Next of kin details c. Ability to capture the crime committed and the sentencing		

10.0   FUNCTIONAL   REQUIREMENTS   FOR   PROBATION   AND AFTERCARE SERVICE (CASE MANAGEMENT SYSTEM)

No.	Requirements	(FS, PS, CR, NS)	Remarks

1.0	**Social Inquiries and Offender Assessment**		
1.1	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts (bail reports, Victim Impact Statement, Presentence, Diversion, Plea bargaining, Resentencing and any other report)		
1.2	Ability to allocate and reallocate the case to a Probation Officer to undertake.		
1.3	Ability to retrieve and view historical records of the Offender including criminal records		
1.4	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office and link up with Kenya Police and Kenya Prisons in future .		

1.5	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources)		
	Ability to track and monitor progress of case to conform to timelines		
	Ability to input changes, edit arising from new information obtained		
1.6	Ability to flag accused child, accused violent extremist/ suspected accused violent extremist		
	Ability to flag child suspected of Sexual offences		
1.7	Ability to assess the accused risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
1.8	Ability to request and schedule case conference		

1.9	Ability to allow supervisor to approve and select officers to participate in case conference Ability for supervisors to monitor progress of report online		
1.10	Ability to input the recommendations of the case conference		
1.11	Ability to input Report		
1.12	Ability to approve Reports at various levels (Station, County, Region, Headquarters) Ability to input feedbacks from the various levels quality control		
1.13	Ability to digitally sign and generate Bail Information Report (Ability to print, sign, upload) Ability to digitally generate and sign Bail/Bond Information Report, Pre-sentence reports, Victim Impact Statement, Diversion, Plea – Bargaining, Resentencing report, Home Final Report,ity to digitally sentences, Victim Impact Statement, Diversion, Plea –Bargaining,		

	Resentencing report, Home Final Report		
1.14	Ability to submit report to Court		
1.15	Ability to record court outcome (bail granted, denied, reviewed or sustained)		
2.0	**PROBATION SERVICE**		
	Probation Orders		
2.1	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts		
2.2	Ability to allocate and reallocate the case to a Probation Service Officer the case to		
2.3	Ability to generate and view historical records of the Offender		
2.4	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office)		

2.5	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources)		
2.6	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
2.7	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
2.8	Ability to request and schedule case conference		
2.9	Ability to allow supervisor to approve and select officers to participate in case conference		
2.10	Ability to input the recommendations of the case conference		
2.11	Ability to input pre-sentence Report		

2.12	Ability to approve Pre-sentence Report at various levels (Station, County, Region, Headquarters)		
2.13	Ability to digitally sign and generate pre-sentence Report (Ability to print, sign, upload)		
2.14	Ability to submit pre-sentence Report to Court		
2.15	Ability to record court outcome		
2.16	Supervision in the Community (triggered by a Court Order)		
2.17	Ability to upload Court Order into the system		
2.18	Ability to register the case and generate serial number		
2.19	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
2.20	Ability to update offender details (PR2 from)		

2.21	Ability to capture supervision notes (Recording of offender's reporting, day, time, discussions, progress in PR2A Form)		
2.22	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)		
2.23	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Offenders with special needs(SNO) ,Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
2.24	Ability to develop individual treatment, supervision and rehabilitation plans		
2.25	Ability to capture reintegration, resettlement and rehabilitation interventions used		

2.26	Ability to allow Community Probation Volunteer comments Ability to allow CPVs should be looked into such that some limits on the accessibility rights to the system are addressed.		
2.27	Ability to generate summary reports of the progress made during supervision (after every 6 months)		
2.28	Ability to compute sentence period (start date/ time and end date/ time)		
2.29	Ability to capture Form PR 9		
2.30	Ability to generate Form PR 9 Report		
2.31	Ability to upload and submit Case Committee Minutes		
2.32	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)		

2.33	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office		
2.34	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case) Ability to generate exit summary report of the offender under community supervision		
2.35	Ability to choose mode of completion (successful, unsuccessful, absconded)		
2.36	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence		
2.37	Ability to monitor offenders electronically (GPS)		
2.38	Ability to capture Probation Officer's supervisor's comments/ evaluation/ inspection of case work		
2.39	Ability to request for empowerment (tools, education, start-up capital, etc)		

2.40	Ability to record empowerment granted to offender		
2.41	Probation Hostel		
2.42	Social inquiry and report preparation		
2.43	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Court		
2.44	Ability to allocate the case to a Probation Officer to undertake the case, and ability to re-allocate to an alternative Probation Officer		
2.45	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
2.46	Ability to generate and view historical records of the Offender		
2.47	Ability to request for records from other jurisdictions		
2.48	Ability to capture interview/ social inquiry data (e.g. Interview of accused person, accused family, victim and victims' family, community, other independent sources)		

2.49	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
2.50	Ability to request and schedule case conference		
2.51	Ability to allow supervisor to approve and select officers to participate in case conference		
2.52	Ability to input the recommendations of the Case Conference		
2.53	Ability to input Pre-sentence Report		
2.54	Ability to approve Pre-sentence Report at various levels (Station, County, Region, Headquarters)		
2.55	Ability to request approval for application for vacancy to Probation Hostel (Station, County, Region, Headquarters)		

2.56	Ability to apply and receive confirmation for vacancy to Probation Hostel (Station, County, Region, Headquarters)		
2.57	Ability to sign and generate Pre-sentence Report (Ability to print, sign, upload)		
2.58	Ability to submit Pre-sentence Report to Court		
2.59	Ability to record Court outcome		
	Application for vacancy		
2.60	Ability to apply for a vacancy to Probation Hostel		
2.61	Ability to receive availability and non-availability from Probation Hostel		
	Admission to Probation Hostel		
2.62	Ability to upload escort documents to the system (Presentence Report, Court Order, Variation Order, Notice to Offender, Medical Report, School documents, Birth Certificate/ National Identity Card Number, and other documents not listed herein)		

2.63	Ability to compute sentence period (start date/ time and end date/ time), and to compute sentence period added (occasioned by a Court Order)		
2.64	Ability to perform full body screening of probationer		
2.65	Ability to confirm date and time of arrival of probationer to the Probation Hostel (this information to be relayed to the Probation Station/ County Probation Office)		
2.66	Ability to update probationer details in (PR2 Form – Home directions, nearest school/ market, landmark)		
2.67	Ability to fill Hostel Admission Form		
2.68	Ability to allocate probationer to a Probation Officer for supervision		
2.69	Ability to input items issued to a probationer		
	Supervision at a Probation Hostel		
2.70	Ability to confirm orientation		

2.71	Ability to capture work/ tasks assigned to probationer		
2.72	Ability to capture offender's biometric data		
2.73	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
2.74	Ability to capture supervision notes in (PR2A Form - Recording of probationer's reporting, day, time, discussions, progress)		
2.75	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)		
2.76	Ability to assess the probationer's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		

2.77	Ability to develop individual treatment,		
2.78	Ability to capture rehabilitation interventions used		
2.79	Ability to capture Form PR 9		
2.80	Ability to generate Form PR 9 report		
2.81	Ability to upload and submit Case Committee Minutes		
2.82	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)		
2.83	Ability to input and transmit reports from the Probation Hostel to Probation Stations/ County Probation Offices, and back (Summary Assessment Report, Initial Environmental Adjustment Report, First Progress Report, First Progress Report, Final Environmental Adjustment Report, Final Report)		
	Exit process from a Probation Hostel		
2.84	Ability to input returned items issued to probationer		

2.85	Ability to transfer case to Probation Station/ County Probation Station for supervision		
	Supervision in the community		
2.86	Ability to upload Court Order into the system		
2.87	Ability to register the case and generate a serial number		
2.88	Ability to capture offender's biometric data		
2.89	Ability to compute Supervision period (start date/ time and end date/ time) Ability to capture extension of supervision order		
2.90	Ability to update probationer details in PR2 Form		
2.91	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
2.92	Ability to capture supervision notes in PR2A Form (Recording of offender's reporting, day, time, discussions, progress)		

2.93	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)		
2.94	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
2.95	Ability to develop individual treatment, supervision and rehabilitation plans		
2.96	Ability to capture reintegration, resettlement and rehabilitation interventions used		
2.97	Ability to allow Community Probation Volunteer comments		
2.98	Ability to generate summary reports of the progress made during supervision (after every 6 months)		
2.99	Ability to capture Form PR 9 report		

2.100	Ability to consolidate Form PR 9 (collect all PR 9s for each individual case and Probation Officer, and consolidate into one form)		
2.101	Ability to upload and submit Case Committee Minutes		
2.102	Ability to monitor, select and report breach of Court Order/ (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)		
2.103	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office		
2.104	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)		
2.105	Ability to choose mode of completion (successful, unsuccessful, absconded)		
2.106	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence		
2.107	Ability to monitor offenders electronically (GPS)		

2.108	Ability to capture Probation Officer's supervisor's comments/ evaluation/ inspection of case work		
2.109	Ability to request for empowerment (tools, education, startup capital, etc)		
2.110	Ability to record empowerment granted to offender		
2.111	Community Resource and Training Centre		
	Ability for course application and admission		
	Ability to capture trainer details		
2.112	Ability to capture course details		
2.113	Ability to capture course calendar		
2.114	Ability to assess/ monitor learning (assessment forms)		
2.115	Ability to issue and return reading materials, case studies, journals, etc		
2.116	Ability to store and retrieve audio and video lectures		

2.117	Ability to generate certificates		
	Probation half way houses		
	Application for admission		
2.118	Ability to apply for admission (Ability to upload Application Form)		
2.119	Ability to notify applicant of acceptance or decline of application		
2.120	Admission to Probation and Aftercare HalfWay House		
2.121	Ability to upload documents to the system (e.g. National Identity Card, Court Order, etc)		
2.122	Ability to compute period of stay (start date/ time and end date/ time), and to compute extended period		
2.123	Ability to perform full body screening		
2.124	Ability to update housemate details in (PR2 Form – Home directions, nearest school/ market, landmark)		
2.125	Ability to fill Admission Form		

2.126	Ability to allocate house mate to a Probation Officer for monitoring		
2.127	Ability to input items issued to a house mate and returned by house mate		
2.128	Ability to confirm orientation		
	Stay at Probation and Aftercare Half Way House		
2.129	Ability to capture work/ tasks assigned to a house mate		
2.130	Ability to capture house mate's biometric data		
2.131	Ability to flag recovering violent extremist offender/ suspected violent extremist		
2.132	Ability to capture notes in (reintegration progress, incidences, occupation)		
2.133	Ability to develop reintegration and resettlement plan		
2.134	Ability to capture reintegration and resettlement interventions used		

2.135	Ability to report breach of House Rules (this should trigger disciplinary measures or termination of residency)		
	Exit process from a Probation and Aftercare Half Way House		
2.136	Ability to input returned items issued to house mate		
2.137	Ability to transfer housemate to another half-way house		
3.0	**COMMUNITY SERVICE ORDER**		
	Social Inquiry and Report Preparation		
3.1	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts(CSO presencence, sentence review)		
3.2	Ability to allocate the case to a Community Service Officer to undertake, and to re-allocate to an alternative Community Service Officer		
3.3	Ability to generate and view historical records of the Offender		

3.4	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office)		
3.5	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources)		
3.6	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
3.7	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		

3.8	Ability to capture work agencies and availability of work suitable for offender Ability to capture skills transferred to clients Ability to capture work profile -work agencies at station level Ability to capture tangible projects at station level		
3.9	Ability to request and schedule case conference		
3.10	Ability to allow supervisor to approve and select officers to participate in case conference		
3.11	Ability to input the recommendations of the case conference		
3.12	Ability to input CSO Pre-sentence Report		
3.13	Ability to approve CSO Pre-sentence Report at various levels (Station, County, Region, Headquarters)		
3.14	Ability to digitally sign and generate CSO Pre-sentence Report (Ability to print, sign, upload)		

3.15	Ability to submit CSO Pre-sentence Report to Court		
3.16	Ability to record court outcome (Probation Order, Community Service Order, Fine, Imprisonment, Conditional Discharge, Unconditional Discharge, Other-specify)		
3.17	Supervision in the community (triggered by a court order)		
3.18	Ability to upload court order into the system		
3.19	Ability to register the case and generate a serial number		
3.20	Ability to capture offender's biometric data		
3.21	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
3.22	Ability to update offender details		
3.23	Ability to capture supervision notes (Recording of offender's reporting, day, time, discussions, progress)		

3.24	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)		
3.25	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, offenders with special needs(SNO),Child Sexual Offenders RNR, Violent Extremist Offenders – PKRAVET)		
3.26	Ability to develop individual treatment, supervision and rehabilitation plans		
3.27	Ability to capture reintegration, resettlement and rehabilitation interventions used Ability to capture crime prevention activities done at the Regional, County and Station level Ability to upload evidence for crime prevention activities Ability to capture Community Service Order partners		
3.28	Ability to allow Community Probation Volunteer comments		

3.29	Ability to assign to an offender in a work agency and notify agency		
3.30	Ability to confirm arrival of an offender to a work agency		
3.31	Ability to capture Form CS 6		
3.32	Ability to generate summary reports of the progress made during supervision (after every 6 months) Ability to upload CSO supervision forms (capture CS 2 Work placement confirmation form, capture CS3 Reporting instructions form, capture CS 4 Work attachment report form)		
3.33	Ability to compute sentence period (start date and/or time and end date and/or time)		
3.34	Ability to compute work quantification (number of hours worked x wage rate as per area)		
3.35	Ability to capture Form CS 7 summary report		
3.36	Ability to generate Form CS 7 report		

3.37	Ability to upload and submit Case Committee Minutes		
3.38	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders) Ability to upload CSO breach of order forms CS B & C		
3.39	Ability to transfer offender to another Community Service Officer/ Probation Station/ County Probation Office 4Ability to upload CSO supervision forms(CS D Notice to offender of substitution of CS Officer, CS E – application for review and variation)		
3.40	Ability to delegate case (where a Community Service Officer is temporarily unable to undertake the case)		
3.41	Ability to choose mode of completion satisfactorily, absconded, unsatisfactorily		

3.42	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence		
3.43	Ability to monitor offenders electronically (GPS) Ability to capture location of tree nurseries and number of trees planted at station level (GPS)		
3.44	Ability to capture Community Service Officer supervisor's comments/ evaluation/ inspection of case work		
3.46	Ability to request for empowerment (tools, education, start-up capital, etc)		
3.47	Ability to record empowerment granted to offender		
4.0	**AFTERCARE**		
	Borstal Report Preparation And Supervision In The Community		
4.1	Social inquiry and report preparation		

4.2	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Court		
4.3	Ability to allocate the case to a Probation Officer to undertake the case, and ability to re-allocate to an alternative Probation Officer		
4.4	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
4.5	Ability to generate and view historical records of the Offender		
4.6	Ability to request for records from other jurisdictions		
4.7	Ability to capture interview/ social inquiry data (e.g. Interview of accused person, accused family, victim and victims' family, community, health records, other independent sources)		

4.8	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET) Ability to refer for specialized assessments		
4.9	Ability to request and schedule case conference		
4.10	Ability to allow supervisor to approve and select officers to participate in case conference		
4.11	Ability to input the recommendations of the Case Conference		
4.12	Ability to input Pre-sentence Report		
4.13	Ability to approve Pre-sentence Report at various levels (Station, County, Region, Headquarters)		
4.14	Ability to request approval for application for vacancy to Borstal Institution (Station, County, Region, Headquarters)		

4.15	Ability to apply and receive confirmation for vacancy to Borstal Institution (Station, County, Region, Headquarters)		
4.16	Ability to sign and generate Pre-sentence Report (Ability to print, sign, upload)		
4.17	Ability to submit Pre-sentence Report to Court		
4.18	Ability to record Court outcome		
4.19	Application for vacancy		
4.20	Ability to apply for a vacancy to Borstal Institution		
4.21	Ability to receive feedback on availability and non-availability		
4.22	Supervision in the community		
4.23	Ability to upload Borstal Release License into the system		
4.24	Ability to register the case and generate a serial number		
4.25	Ability to capture offender's biometric data		

4.26	Ability to compute sentence period (start date/ time and end date/ time)		
4.27	Ability to update probationer or ex-Borstal inmate details		
4.28	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender Ability to flag specialized needs offenders		
4.29	Ability to capture supervision notes (Recording of offender's reporting, day, time, discussions, progress)		
4.30	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity) Ability to apply for supervision extension		
4.31	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		

4.32	Ability to develop individual treatment plan		
4.33	Ability to capture reintegration, resettlement and rehabilitation interventions used		
4.34	Ability to allow Community Probation Volunteer comments		
4.35	Ability to generate summary reports of the progress made during supervision (after every 6 months)		
4.36	Ability to capture Progress report		
4.37	Ability to consolidate Progress reports (collect all Progress reports for each individual case and Probation Officer, and consolidate into one report)		
4.38	Ability to upload and submit Case Committee Minutes		
4.39	Ability to monitor, select and report breach of Release License (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)		

4.40	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office		
4.41	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)		
4.42	Ability to choose mode of completion (successful, unsuccessful, absconded)		
4.43	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence		
4.44	Ability to monitor offenders electronically (GPS)		
4.45	Ability to capture Probation Officer's supervisor's comments/ evaluation/ inspection of case work		
4.46	Ability to request for empowerment (tools, education, startup capital, etc)		
4.47	Ability to record empowerment granted to offender		

4.48	Power of Mercy Advisory social inquiry, report preparation and supervision in the community		
4.49	Social Inquiry and Report Preparation		
4.50	Ability to capture notification and registration of referral of case from Power of Mercy Advisory Committee at the Headquarters		
4.51	Ability to allocate the case to a Probation Officer to undertake (Headquarters), and to re-allocate to an alternative Probation Officer (County Probation Office)		
4.52	Ability to retrieve and view historical records of the petitioner		
4.53	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
4.54	Ability to request for records from other jurisdictions (that is, other County Probation Offices)		

4.55	Ability to capture interview/ social inquiry data (e.g. Interview of petitioner, petitioner's family, victim and victims' family, community, other independent sources)		
4.56	Ability to assess the petitioner's risks and needs and classify the risks/ needs into high, medium, low. (Types of assessment tools: (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET) Ability to refer for specialized assessment		
4.57	Ability to request and schedule Case Conference		
4.58	Ability to allow supervisor to approve and select Probation Officers to participate in Case Conference		
4.59	Ability to input the recommendations of the Case Conference		
4.60	Ability to input Power of Mercy Advisory Report		

4.61	Ability to approve Power of Mercy Advisory Report at various levels (Region, Headquarters)		
4.62	Ability to sign and generate Power of Mercy Advisory Report Category Report (Ability to print, sign, upload)		
4.63	Ability to submit Power of Mercy Advisory Report/ Power of Mercy Advisory Special Category Report to headquarters Ability to access and update Pomac PMR 1 and 2a reports.		
4.64	Ability to record outcome (Presidential Order, Pardoned, Not pardoned, Other-specify) Ability to record pending outcome		
4.65	Supervision in the Community (triggered by a Presidential Order)		
4.66	Ability to upload Presidential Order into the system		
4.67	Ability to register the case and generate serial number		
4.68	Ability to capture pardonee's biometric data		

4.69	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
4.70	Ability to Compute supervision period (start date/ time and end date/ time)		
4.71	Ability to update Pardonee details		
4.72	Ability to capture supervision notes Recording of pardonee's reporting, day, time, discussions, progress)		
4.73	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)		
4.74	Ability to assess the pardonee's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
4.75	Ability to develop individual treatment, supervision and rehabilitation plans		

4.76	Ability to capture reintegration, resettlement and rehabilitation interventions used		
4.77	Ability to allow Community Probation Volunteer comments		
4.78	Ability to generate summary reports of the progress made during supervision (after every 6 months)		
4.79	Ability to capture Progress Report		
4.80	Ability to generate Progress Report		
4.81	Ability to upload and submit Case Committee Minutes		
4.82	Ability to transfer pardonee to another Probation Officer/ County Probation Office		
4.83	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)		
4.84	Ability to choose mode of completion (successful, unsuccessful, absconded)		

4.85	Ability to generate Certificate of Completion for pardonee that have successfully completed their sentence		
4.86	Ability to monitor pardonee electronically (GPS)		
4.87	Ability to capture supervisor's comments/ evaluation/ inspection of case work		
4.88	Ability to request for empowerment (tools, education, start-up capital, etc)		
4.89	Ability to record empowerment granted to offender		
4.90	Special category psychiatric, leniency, capability social inquiry, and special needs offenders, report preparation and supervision in the community		
4.91	Social Inquiry and Report Preparation		
4.92	Ability to capture notification and registration of referral of case from the Psychiatrist (Mathari Hospital)		

4.93	Ability to allocate the case to a Probation Officer to undertake the case, and ability to re-allocate to an alternative Probation Officer		
4.94	Ability to retrieve and view historical records of the Offender		
4.95	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
4.96	Ability to request for records from other jurisdictions (that is, other Probation Stations, County Probation Offices)		
4.97	Ability to capture interview/ social inquiry data (e.g., Interview of accused person, accused family, victim and victims' family, community, health records, other independent sources)		

4.98	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Types of assessment tools: Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET) Ability to refer for specialized assessment		
4.99	Ability to request and schedule Case Conference		
4.100	Ability to allow supervisor to approve and select Probation Officers to participate in case conference		
4.101	Ability to input the recommendations of the case conference		
4.102	Ability to input Capability Report/ Leniency Report		
4.103	Ability to approve Capability Report/ Leniency Report at various levels (Probation Station, County Probation Office, Region, Headquarters)		

4.104	Ability to sign and generate Capability Report/ Leniency Report (Ability to print, sign, upload)		
4.105	Ability to submit Capability Report/ Leniency Report to Psychiatrist		
4.106	Ability to record outcome (Probation Order, Community Service Order, Fine, Imprisonment, Conditional Discharge, Unconditional Discharge, Other-specify)		
4.107	Supervision in the Community (triggered by a Court Order)		
4.108	Ability to upload Court Order into the system		
4.109	Ability to register the case and generate serial number		
4.110	Ability to capture offender's biometric data		
4.111	Ability to compute sentence period (start date/ time and end date/ time)		
4.112	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
4.113	Ability to update offender details		

4.114	Ability to capture supervision notes (recording of probationer's reporting, day, time, discussions, progress)		
4.115	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)		
4.116	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Types of assessment tools: Substance abuse disorders, female offenders, offenders with mental disorders, child offenders, adult sexual offenders, child sexual offenders, violent extremist offenders)		
4.117	Ability to develop individual treatment		
4.118	Ability to capture reintegration, resettlement and rehabilitation interventions used		
4.119	Ability to allow Community Probation Volunteer comments		
4.120	Ability to generate summary reports of the progress made during supervision (after every 6 months)		
4.121	Ability to capture Progress Report		

4.122	Ability to consolidate Progress (collect all Progress Reports for each individual case and officer, and consolidate into one form)		
4.123	Ability to upload and submit Case Committee Minutes		
4.124	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)		
4.125	Ability to transfer probation to another Probation Officer/ Probation Station/ County Probation Office		
4.126	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)		
4.127	Ability to choose mode of completion (successful, unsuccessful, absconded)		
4.128	Ability to generate Certificate of Completion for offenders that have successfully completed their sentence		
4.129	Ability to monitor probationer electronically (GPS)		

4.130	Ability to capture supervisor's comments/ evaluation/ inspection of case work		
4.131	Ability to request for empowerment (tools, education, startup capital, etc)		
4.132	Ability to record empowerment granted to offender		
4.133	ALTERNATIVE DISPUTE RESOLUTION / RESTORATIVE JUSTICE AND VICTIM-OFFENDER MEDIATION SOCIAL INQUIRY, REPORT PREPARATION AND SUPERVISION IN THE COMMUNITY		
4.134	Social Inquiry and Report Preparation		
4.135	Ability to capture notification and registration of referral of case from Court of Appeal, High Court, Magistrate Courts		
4.136	Ability to allocate and reallocate the case to a Probation Officer		
4.137	Ability to retrieve and view historical records of the Offender		

4.138	Ability to request for records from other jurisdictions (Probation Station/ County Probation Office)		
4.139	Ability to capture interview/ social inquiry data (e.g. Interview of offender, offender's family, victim and victims' family, community, other independent sources)		
4.140	Ability to flag child offender, violent extremist offender/ suspected violent extremist offender		
4.141	Ability to assess the offender's risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
4.142	Ability to request and schedule case conference		
4.143	Ability to allow supervisor to approve and select officers to participate in case conference		
4.144	Ability to input the recommendations of the case conference		

4.145	Ability to input Alternative Dispute Resolution Report/ Restorative Justice and Victim-Offender Mediation Report		
4.146	Ability to approve Alternative Dispute Resolution Report/ Restorative Justice and Victim-Offender Mediation Report at various levels (Station, County, Region, Headquarters)		
4.147	Ability to digitally sign and generate Report (Ability to print, sign, upload)		
4.148	Ability to submit report to Court		
4.149	Ability to record court outcome (Agreement, specify other)		
4.150	Supervision in the Community (triggered by a Court Order)		
4.151	Ability to upload Court Order into the system		
4.152	Ability to register the case and generate a serial number		

4.153	Ability to compute supervision period (start date/ time and end date/ time) Ability to capture extension of supervision order		
4.154	Ability to capture offender biometric data		
4.155	Ability to flag child offender, offender violent extremist / suspected accused violent extremist offender		
4.156	Ability to update offender details		
4.157	Ability to capture supervision notes (recording of probationer's reporting, day, time, discussions, progress)		
4.158	Ability to categorize intensity of supervision (High intensity, moderate intensity, low intensity)		
4.159	Ability to assess the accused risks and needs and classify the risks/ needs into high, medium, low. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		

4.160	Ability to develop supervision plan		
4.161	Ability to capture reintegration and resettlement Ability to capture interventions engaged		
4.162	Ability to allow Community Probation Volunteer comments		
4.163	Ability to generate summary reports of the progress made during supervision (after every 6 months)		
4.164	Ability to capture Progress Report		
4.165	Ability to generate Progress Report		
4.166	Ability to upload and submit Case Committee Minutes		
4.167	Ability to monitor, select and report breach of Court Order (this should trigger application for Warrant of Arrest or Discharge of Supervision Orders)		
4.168	Ability to transfer offender to another Probation Officer/ Probation Station/ County Probation Office		

4.169	Ability to delegate case (where a Probation Officer is temporarily unable to undertake the case)		
4.170	Ability to choose mode of completion (successful, unsuccessful, absconded)		
4.171	Ability to generate Certificate of Completion for offenders that have successfully completed their supervision		
4.172	Ability to monitor offender electronically (GPS)		
4.173	Ability to capture Probation Officer's supervisor comments/ evaluation/ inspection of case work		
5.0	**PROBATION STAFF TRAINING**		
5.1	Ability for course application and admission		
5.2	Ability to capture trainer details		
5.3	Ability to capture training details		
5.4	Ability to capture training calendar		

5.5	Ability to assess/ monitor learning (assessment forms)		
5.6	Ability to issue and return reading materials, case studies, journals, etc		
5.7	Ability to store and retrieve audio and video lectures		
5.8	Ability to generate certificates		
6.0	**REPORTS**		
6.1	Ability to generate Offender Assessment Report and categorize it as High Risk, Medium Risk, Low Risk, Unfavorable or committal to institutions. (Substance Abuse Disorders - CAGE-AID, Female Offenders - RNR, Offenders with Mental Disorders - MSE, Child Offenders - RNR, Adult Sexual Offenders - RNR, Child Sexual Offenders RNR, Violent Extremist Offenders - PKRAVET)		
6.2	Ability to generate the Case Conference recommendation		

6.3	Ability to generate CSO Pre-sentence Report/ Resentencing Report/ Sentence Review Report/ Power of Mercy Advisory Report/ Power of Mercy Advisory Special Category Report/ Capability Report/ Leniency Report/ Bail Information Report/Plea Bargaining Report/ Victim Impact Assessment Report/ Alternative Dispute Resolution Report/ Restorative Justice and Victim-Offender Mediation Report /Probation Presentence Report/Diversion Report		
6.4	Ability to generate data in different formats (No. of cases per officer/ station/ county/ region/ national, most prevalent offences per station/ county/ region/ national, No. of cases per male/ female/ boy/ girl/ adult vs children, etc)		
6.5	Ability to analyze data and give reports (per Probation Station/ County Probation Office/ Region/ National)		
6.6	Ability to generate CS 7 and CS 9 Reports		
6.7	Ability to generate a supervisor inspection report at various levels (Station, County, Region, Headquarters)		

6.8	Ability to input and transmit reports from the Probation Hostel to Probation Stations and County Probation Offices, and back (Summary Assessment Report, Initial Environmental Adjustment Report, First Progress Report, First Progress Report, Final Environmental Adjustment Report, Final Report)		

1.3   Architectural Requirements to be met by the Information System

1.3.1   The Information System MUST be supplied and configured to implement the following architecture.

1.3.1.2 <u>Software Architecture</u>: *[specify: features (use diagrams as appropriate)]*.

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

The software Architecture consists of the following modules:

a) Registration Module:• A client facing web-based system to enable data controllers and processors to register in line with the data protection act ,2019 and the attendant regulations, Platform for generating and publishing a list of registered data controllers and processors on the website in conformity with the regulations (14. (1) and subject to section 21 of the Act, Dashboard for tracking applications and their statuses in line with the act and the ODPC service charter, Provision for revocation of an entity's certificate of registration and automatic cancellation from the record and the register upon revocation, Provision for change or variation of registrations, Integration with BRS system for validation and due diligence of both local and foreign companies operating in Kenya during registration, Backend for review of applications, approvals as per the defined workflows and policies, Provision for renewal of certificates prior or upon expiry, Emails and SMSs integration for push of notifications and reminders on action items relating to registrations, Auto generation of certificate for printing upon approval, Categorization of application based on the counties, regions and the defined approval matrix, Integration with the existing systems and the approved payment platforms & gateways which include but not limited to mobile money paybills and bank to ensure efficiency in payment of registration fees, Inclusion of a ticketing module linked to ODPC call

center to ensure tracking and timely resolution of registration requests, Provision for querying and validation of a certificate.

b) Data Breach: Creation of a data breach reporting module on the system, Mapping of reported data breaches for actions as per the defined user roles and matrices, Tracking of data breaches and their respective statuses.

c) compliance module: Creation of a Data Privacy Impact Assessment (DPIA) module in line with the requirements, A sub module for submission and approval of a data transfer request, Provision for making requests for data protection advisories and tracking of advisories issued by the office, Submission of Data Protection Impact Assessments, Emails and SMSs integrations for acknowledge receipt of Data Breach Notifications, advisory request, cross border transfer requests and DPIAs.

d) Data Audits Module: Provision for data audit planning and reporting on the number of audits performed, Randomized selection of entities to audit, Provision for sending notifications/reports of data audits to controllers/processors.

e) Quality Assurance Certification Module: Provision for a module for offer/issuance of certification of data protection seals and marks to encourage data protection compliance by controllers and processors.

f) Complaints, Investigation and Enforcement Module: End to end complaints module to enable data subjects lodge complaints and allow internal staff to review the complaints as per the complaints handling procedure, Provision for acknowledgement of a complaint by the office, Provision for preliminary review of a complaint, Notification of a complaint to a respondent, Provision for investigation of a complaint as per the defined procedures, Assignment of tasks to officers and tracking of their statuses, Generation of automated register of complaints and their statuses, Provision for withdrawal of a complaint by a data subject, Discontinuation and notification of the same to the data subject and/or a respondent, Transcription/ Hansard module to take complaints made over the phone through ODPC call center, Automatic assignment of tracking numbers once a complaint has been lodged and if the complaint is against a DP or DC, the complaint can be linked to that that particular entry, Inclusion of the Alternative Dispute Resolution (ADR) mechanisms on to the enforcement sub -modules, • Provision for reinstitution of a complaint after a decline/discontinuation, Ability for joint handling of a complaint, Provision for submission of determinations before the enforcement processes, Facilitate issuance of enforcement, penalty notices and administrative fines to data processors and / or controllers, • Provision for appeals of determination, enforcement notices and penalty notices, Provision for referral to ODPP for prosecution, Generation of automatic Enforcement registers, Provision for automated summons, Provision for submission of an investigation report for approval, Application for review of enforcement notice(s) by a data subject, Integration with the existing systems and the approved payment platforms & gateways which include but not limited to paybills and bank to ensure efficiency in payments for administrative fines and penalty fees, Provision for prompts/alerts/notifications with time-based escalations incorporated in the workflow

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for Office of the Attorney General

1. Software Architecture Overview

The software architecture must be modular, scalable, and secure, designed to handle the current and future needs of the OAG&DOJ. The key principles that must guide the design of the software architecture are:

- Modularity: The core modules (e.g., Legal Case Management System (LCMS), Legal Opinion Database, Legislative Drafting and Information Management System (LDIMS)) must operate independently, be scalable, and have the capacity to integrate additional modules in the future.
- Scalability: The architecture must support both horizontal (across multiple servers) and vertical (increasing server capabilities) scaling, enabling it to handle growing data, users, and system demands.
- Security: The architecture must comply with relevant data protection laws, including Kenya's Data Protection Act and GDPR. It should include strong encryption, authentication, and access control mechanisms to safeguard sensitive legal data.
- High Availability: The system must be designed for continuous operation, with mechanisms in place for redundancy, backup, and disaster recovery.
- Open-Source Technologies: The system will prioritize open-source solutions to ensure flexibility, community support, and cost-effectiveness.

2. Key Architectural Components

a) System Architecture Overview

The software system will adopt a three-tier architecture model:

- Presentation Layer: A responsive, intuitive user interface for various users, including legal officers, paralegals, and management. The UI should be mobile-friendly and accessible on desktop devices.
- Business Logic Layer: The core functionality of the system will process case management, legal opinions, legislative drafting, and other workflows.

- Data Layer: A secure and efficient database layer will store case data, legal opinions, legislative drafts, user information, and other essential data.
- Integration Layer (API Gateway, External Systems)

b) Technology Stack

- Frontend: The presentation layer will utilize modern frameworks such as ReactJS or VueJS, optimized for mobile and desktop devices.
- Backend: The business logic layer will be implemented with open-source technologies, such as Java Spring Boot, Django, or Node.js, ensuring scalability and robustness.
- Database: PostgreSQL will be used for structured data, while MongoDB will handle unstructured data. ElasticSearch will be employed for advanced search capabilities.
- Cloud Infrastructure: The system will be deployed on cloud platforms (e.g., AWS, Azure, or Google Cloud) with Docker and Kubernetes for containerization and orchestration.
- Security Technologies: Authentication via OAuth 2.0, JWT for token-based authentication, and TLS for encryption will be implemented. Role-based access control (RBAC) will ensure fine-grained user access.
- Support for data exchange protocols (e.g., SOAP/XML, REST/JSON)

c) Integration Architecture

The system must integrate with both internal and external systems, such as:

- Internal Systems: Existing OAG&DOJ case management, document management, and billing systems, etc.
- External Systems: Judiciary case management systems, Kenya Law Database, Human resource Management system, and financial integration systems like IFMIS etc.
- The integration will rely on RESTful APIs to ensure seamless communication with external platforms. Data synchronization mechanisms must be implemented to ensure consistency across integrated systems.

d) Data Architecture

The data architecture must ensure:

- Data Storage: Secure cloud-based databases with encryption both in transit and at rest.
- Data Integrity: Validation checks at both input and storage levels to ensure data accuracy and consistency.
- Backup and Recovery: Support automated backups, including off-site storage, disaster recovery protocols, and data integrity checks
- Data Compliance: Compliance with the Data Protection Act of Kenya, GDPR, and other relevant regulations.
- Versioning: The system will support document versioning and metadata tagging for enhanced document retrieval and traceability.

e) Security Architecture

The system architecture will enforce high standards of security, incorporating:

- Authentication and Authorization: The system will support Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) to ensure secure and granular user access.
- Encryption: AES-256 encryption for data at rest and in transit, and TLS for secure communication.
- Audit Logging: Detailed and tamper-evident audit logs for tracking user activity and system changes.
- Zero Trust Security Model: Validate every request
- Password policies, session timeout
- Self-service user portal
- Disaster Recovery: Backup and recovery mechanisms for data protection.

f) DevOps and Continuous Integration/Continuous Deployment (CI/CD)

The development process will follow DevOps best practices to ensure reliable and efficient deployment:

- CI/CD Pipeline: Automated build, test, and deployment pipelines using tools such as Jenkins, GitLab CI, or CircleCI.
- Infrastructure as Code (IaC): Tools like Terraform will be used to define and manage cloud infrastructure in a version-controlled manner ensuring consistency and repeatability in deployments.

- Automated Testing: Automated testing for unit, integration, and user acceptance testing to ensure system quality.

3. Compliance and Standards

The system must comply with the following standards and regulations:

- Kenya's Data Protection Act: Compliance with local data privacy and protection laws.
- GDPR: Ensure compliance for European Union citizen data processing.
- ICT Authority Standards: Adherence to the ICT Authority's guidelines on software development and acquisition for government systems.
- Industry Standards: Follow international standards such as ISO 27001 (Information Security) and ISO 9001 (Quality Management).

4. Reporting and Analytics Architecture

The system must include capabilities for real-time reporting and analytics:

- Dashboards: Real-time dashboards for monitoring case progress, legal opinions, and system health.
- Analytics: Integration with AI-powered tools for insights on case outcomes and document trends.

5. System Monitoring and Maintenance

The system must include comprehensive monitoring and maintenance protocols:

- Monitoring: Use tools like Prometheus and Grafana for real-time system performance and activity monitoring.
- Maintenance: Regular updates, security patches, and performance tuning as part of an ongoing maintenance plan.

6. User Interface (UI) and Experience (UX)

The UI/UX should be designed with ease of use in mind:

- Accessibility: The system must be accessible on both desktop and mobile devices.
- User-Friendly Dashboard: A dashboard that tracks case status, legal opinions, and legislative progress.

● Role-Based Customization: The UI should adapt based on user roles and permissions.

7. Scalability and Performance

The architecture should ensure the system can scale efficiently:

● Horizontal Scaling: To handle increasing users and data volume.
● Performance Optimization: Caching mechanisms and load balancing to optimize system response times.
● Automated Alerts: Automated performance monitoring to preemptively address system bottlenecks.

8. Search & Conflict Check

● The system shall implement a full-text search functionality to allow users to search for specific keywords or phrases across documents.
● Integrate OCR technology to extract text from scanned documents, images, or PDFs that are not already in machine-readable format.
● The system shall allow for the filtering of search results based on metadata (e.g., document type, creation date, author).
● The system shall implement a Conflict of Interest (COI) search functionality to identify potential conflicts based on predefined criteria.
● The system shall include a document similarity check feature to identify documents with similar content or themes.

9. Backup and Disaster Recovery

The architecture should include:

● Automated Backups: Regular, secure backups of critical data.
● Disaster Recovery: A geographically distributed disaster recovery plan for business continuity.

Module 1: Case Management System

A. Case Management Module

- Dashboard with filters
- Timeline tracking
- Virtual tags and sticky notes
- Cause of Action categorization
- Judgment/Award logs
- AI-based trend analysis

B. Document Management System

- Secure cloud + local storage
- Bulk upload/download
- OCR & metadata tagging
- Document automation
- E-signatures with audit trails

C. Legal Research & Precedent Module

- Integration with LexisNexis, Thomas Reuters etc
- Precedent case flagging
- Research notes per case
- AI-based search and summarization

D. Client & Witness Portal

- Submit affidavits, evidence, responses
- Track case status
- Secure communication channel

E. Task & Workflow Management

- Task allocation and Standard Operating Procedures (SOP)-based templates
- Calendar integration (court dates, deadlines etc)
- Workflow automation (e.g., for pre-trial prep)

F. Billing & Financial Tracking

- Travel, payment vouchers
- Integration with IFMIS
- Award & claim tracking

- Case-cost analytics

G. Reporting & Analytics

- Case aging, type, success rates
- Employee performance
- Custom reports (Performance Appraisal System (PAS), audit, policy)
- AI trend prediction

H. Search & Conflict Check

- Full-text search, OCR, metadata filters
- Conflict of interest search
- Document similarity checks

I. User & Role Management

- Role-based access control (RBAC)
- Password policies, session timeout
- Self-service user portal
- Audit logs and user activity tracking

J. External Integration Gateway

- Open APIs for:
  - Judiciary CMS
  - Integrated Population Registration System (IPRS)
  - Finance systems (IFMIS)
  - Other gov systems
- Support for data exchange protocols (e.g., SOAP/XML, REST/JSON)

K. Deployment Considerations

- Phased rollout: Department-wise or region-wise
- Offline mode: Desktop sync for offline areas
- Load balancing: For high-volume court periods
- Disaster recovery: With defined RPO/RTO metrics

L. Documentation & Support

- Comprehensive system design documentation
- User manuals + in-app help guides
- Online knowledge base and video tutorials
- Training workshops for lawyers and staff

Module 2: Legal Advisory/Opinions Database

1. **User Management Module**
   - Role-based access control (RBAC)
   - Multi-factor authentication (MFA)
   - Password policy enforcement
   - User audit logs
2. **Legal Advisory Content Management**
   - Uploads and metadata tagging
   - Document conversion and storage (PDF, Word)
   - Version control and revision history
   - Categorization by legal themes, departments, dates
3. **Advanced Search & Retrieval**
   - Full-text and metadata-based search
   - Boolean logic support
   - Filtering by date, department, tags, case type
   - Sorting and pagination
4. **Legal Research Integration**
   - Research Library with tagging and attachments
   - Integration with external paid APIs (e.g., Lexis Nexis, Kenya Law)
   - Cross-referencing and internal citations
5. **Notifications & Alerts**
   - Alerts for new advisories, deadlines, changes
   - Configurable email/SMS/web push notifications
6. **Reporting & Analytics**
   - Usage statistics and trend dashboards
   - Exportable reports (PDF, Excel)
   - Data-driven legal gap analysis
7. **Calendar and Event Tracking**
   - Statutory reminders
   - Dashboard for department and user-level events
   - Multiple notification triggers (SMS, email, popups)
8. **Audit Logging & Monitoring**
   - Immutable logs for actions (create, read, update, delete)

- Real-time system monitoring
- Integration with SIEM tools for anomaly detection

9. **System Integration Module**
   - API Gateway for third-party integrations (RESTful APIs)
   - Middleware for connecting to:
     - EDRMS
     - Legal Case Management System
     - Knowledge Management Tools

10. **UI/UX Guidelines**
   - WCAG 2.1 AA compliance for accessibility
   - Responsive and mobile-first design
   - Simple dashboards with filtering widgets
   - Tooltips and onboarding for new users
   - Auto-save functionality on forms
   - User feedback interface

Module 3 : Legislative Drafting Information System

a. Legislative Drafting Module

- Bill/subsidiary legislation lifecycle tracking
- Collaborative editing and workflow automation
- Integration with statutes for real-time legal referencing
- Conflict checks, validation, and auto-proofreading using AI

b. Document Management System (DMS)

- Version control, file categorization, and metadata tagging
- Secure uploads, archiving, Optical Character Recognition (OCR), and linkage of correspondence
- Automated generation of legal templates and comparison views

c. Legal Research Module

- Advanced search across internal/external databases (e.g., Kenya Law)
- Embedded law library with citations and precedent links

d. Reporting & Analytics

- Role-based dashboards
- KPIs, performance tracking, historical trends
- Export capabilities (Excel, PDF)

e. Communication & Notifications

- Internal messaging and annotation tools
- Automated email/SMS alerts and escalations
- Supervisor-level tracking of assignments

f. Integration Requirements

The system will integrate with the following:

- e-Parliament system for tracking bills
- Kenya Law database and IPRS (if applicable)
- Existing OAG&DOJ Electronic Document & Records Management System (EDRMS), email, and calendar systems
- Identity management with government single sign-on (SSO)

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

KPS MODULES

1.1. Inmate Management Module

This module tracks the entire lifecycle of an inmate, from admission to release.

Key Features:

- Inmate Registration: Capturing personal details, biometrics, and crime history.
- Classification & Security Level Assignment: Categorization based on offense type, behavior, and risk level.
- Sentence Management: Tracking court decisions, appeals, sentence durations, and parole eligibility.
- Transfers & Movements: Managing transfers between prisons and tracking inmate locations.
- Inmate Tracking: Tracks movements, transfers, and status of inmates (e.g., parole, medical leave, etc.).

- Release Management: Automating conditional releases, parole, and discharge documentation.

1.2. Case & Legal Proceedings Module

This module integrates legal case tracking with correctional services.

Key Features:

- Court Case Management: Logging court appearances, verdicts, and appeals.
- Legal Representation Tracking: Assigning lawyers, tracking public defenders, and legal aid support.
- Case Appeals & Reviews: Monitoring pending appeals and legal status updates.
- Parole Tracking: Manages parole applications, approvals, and hearings.

1.3. Prisoner Welfare & Rehabilitation Module

Designed to manage programs that help inmates reintegrate into society.

Key Features:

- Educational Programs: Enrollment in literacy programs, vocational training, and exams.
- Health & Medical Records: Managing inmate medical history, medications, and doctor visits.
- Psychological & Counseling Services: Tracking therapy sessions, mental health assessments, and progress reports.
- Rehabilitation Programs: Monitoring participation in rehabilitation activities, including drug rehabilitation and skill development.

1.4. Security & Incident Management Module

A module for monitoring security risks and handling emergency situations.

Key Features:

- Incident Reporting: Documenting fights, escapes, contraband discoveries, and other violations.
- Surveillance Integration: Connecting CCTV footage and AI-based anomaly detection.
- Security Alerts & Notifications: Automatic alerts for suspicious activities, lockdowns, or security breaches.

1.5. Staff Management & HR Module

This module manages correctional officers and administrative staff.

Key Features:

- Staff Records & Profiles: Maintaining personal details, ranks, promotions, and assignments.
- Shift & Duty Rosters: Scheduling guards and administrative personnel.
- Performance Tracking: Recording disciplinary actions, awards, and work efficiency.
- Payroll & Leave Management: Handling salaries, overtime, and staff leave schedules.

1.6. Facility & Resources Management Module

This module ensures efficient use of resources within correctional facilities.

Key Features:

- Cell & Bed Allocation: Assigning inmates to specific cells based on classification.
- Food & Supplies Management: Tracking inventory, food rations, and daily consumption.
- Maintenance & Repairs: Managing facility repair requests, infrastructure updates, and inspections.

1.7. Communication & Visitations Module

Facilitates controlled communication between inmates, staff, and external parties.

Key Features:

- Visitor Management: Pre-approval system for inmate visits and visitor registration,visitor scheduling,visitor check-in/check-outs.
- Call & Communication Tracking: Monitoring and approving phone calls, emails, or letters.
- Inmate Complaint & Request System: Digital submission of inmate complaints and requests.

1.8. Financial & Budgeting Module

Tracks financial activities related to correctional services.

Key Features:

- Prisoner Accounts: Managing deposits, fines, and expenditures.

1.9. Parole & Probation Management Module

Manages inmates eligible for parole or probation.

Key Features:

- Eligibility Assessment: Monitoring behavior and parole conditions.
- Case Officer Assignments: Assigning parole officers to monitor released inmates.
- Compliance Tracking: Ensuring parolees meet conditions such as regular check-ins and community service.

1.10. Reports & Analytics Module

Provides real-time insights into correctional facility operations.

Key Features:

- Dashboards & Visualization: Graphical representation of inmate statistics, security incidents, and staff performance.
- Custom Reports: Generating reports on inmate demographics, parole success rates, and operational efficiency.
- Predictive Analytics: AI-driven forecasting of security risks and resource needs.

1.11. System Integration & Security Features

- Integration with National Databases: Police records, court databases, and biometric systems.
- Role-Based Access Control: Restricting access based on user roles (e.g., guards, administrators, legal teams).
- Data Encryption & Cybersecurity Measures: Protecting sensitive data from breaches.
- Audit Logs & Monitoring: Recording all activities for accountability and compliance.

1.12 Escape and Threat Management

- Escape Alerts: Tracks and alerts in case of escape attempts or breakouts.
- Threat Analysis: Analyzes potential threats or dangerous inmates, based on behavior and intelligence.
- Tracking and Investigation: Helps authorities track inmates in case of an escape or potential harm.

1.13 Compliance & Audits

- Regulatory Compliance: Ensures the prison operates in accordance with local laws, regulations, and standards.
- Audit Trails: Keeps detailed logs of system access and modifications for auditing and accountability.

1.14 Alerts and Notification System

- Automated Notifications: Sends alerts or notifications to relevant parties (inmates, visitors, staff, etc.) for various events like appointments, violations, etc.
- Emergency Alerts: Sends notifications in case of emergency situations or lockdowns.

PACS

2.1 Offender Registration & Profiling Module

- Capture and manage detailed offender information, including:
  - Personal details (Name, ID, Age, Gender, Contact)
  - Offense details (Crime committed, court ruling, sentence)
  - Risk assessment and classification
  - Biometric & photo records
- Maintain historical records for repeat offenders.

2.2. Court Orders & Sentence Management Module

- Court order processing – Digitally record and track judicial sentencing decisions.
- Types of sentences supported:
  - Probation
  - Community Service Order (CSO)
  - Supervised Release
- Integration with Judiciary & Prisons – Automatic updates from court systems and prison databases.

2.3. Supervision & Compliance Monitoring Module

- Assign probation officers to offenders based on jurisdiction.
- Track offender check-ins (physical, virtual, or biometric verification).
- Automated compliance alerts for:
  - Missed check-ins
  - Violation of probation terms
  - Risk assessment updates

- Generate case progress reports for court updates.

2.4. Rehabilitation & Reintegration Module

- Offender rehabilitation tracking:
  - Counseling sessions
  - Drug and alcohol rehabilitation programs
  - Skills development & vocational training
- Employment & community reintegration support:
  - Job placement for rehabilitated offenders
  - Community involvement initiatives

2.5. Community Service Orders (CSO) Management Module

- Assign community service tasks based on offender skill sets.
- Location tracking of assigned work areas.
- Monitor and update task completion progress.
- Generate CSO completion reports for submission to courts.

2.6. Case Management & Document Handling Module

- Centralized digital storage for case files, court rulings, and documents.
- Secure document access control based on role permissions.
- Digital signature and approval workflow for official records.
- Audit trail to track document modifications.

2.7. Reporting & Analytics Module

- Generate customized reports for:
  - Offender statistics (age, gender, crime types)
  - Probation success rates
  - Rehabilitation program effectiveness
- Dashboard visualization of case trends, compliance rates, and workload distribution.
- Automated monthly, quarterly, and annual reports for government agencies.

2.8. Integration with Other Systems Module

- Court Systems – Automate offender record retrieval from judicial platforms.
- National Police & Prisons – Sync offender status for those under probation.
- Community & Rehabilitation Centers – Data sharing for support programs.
- Biometric & Identification Systems – Fingerprint and facial recognition for identity verification.

2.9. User Management & Role-Based Access Control Module

- Different access levels for:
    - Probation officers
    - Judges & magistrates
    - Community service supervisors
    - Government agencies
- Multi-factor authentication (MFA) for enhanced security.
- Log tracking and audit trails for user activity monitoring.

2.10. Alerts & Communication Module

- Automated SMS & email reminders for:
    - Offender check-ins
    - Upcoming court dates
    - Community service schedules
- Secure in-app messaging between stakeholders.
- Public awareness campaigns for rehabilitation programs.

2.11. Mobile & Web Access Module

- Mobile application for probation officers to update case details on-site.
- Web-based portal for easy access across different locations.
- Offline data entry with synchronization once internet is available.

2.12. Implementation Plan & Considerations

2.12.1 Security & Compliance

- Ensure compliance with Kenya Data Protection Act for offender records.
- Encryption & secure cloud storage for sensitive case files.
- Role-based access control (RBAC) to restrict data exposure.

2.12.2 Training & Capacity Building

- Conduct training for probation officers, court staff, and community service supervisors.
- Provide user manuals and helpdesk support for smooth adoption.

2.12.3 System Scalability & Maintenance

- Design system to support increasing number of cases over time.
- Establish technical support channels for troubleshooting and upgrades.

2.13 Encryption Module

This is a critical security component designed to ensure confidentiality, integrity, and authenticity of sensitive data. This module will implement strong encryption algorithms to protect inmate records, staff information, financial

transactions, and other critical data within the correctio**nal system.**

2.13.1 Encryption Requirements

Data Types to be Encrypted

Personal Identifiable Information (PII): Names, ID numbers, biometric data.

Inmate Records: Criminal history, medical records, court documents.

Staff Information: Employee details, access credentials.

Financial Transactions: Payments, procurement records.

Communication Logs: Emails, internal memos.

2.13.2 Security Standards Compliance

AES-256 (Advanced Encryption Standard) for data at rest.

TLS 1.2/1.3 for data in transit.

FIPS 140-2 validated cryptographic modules (if applicable).

GDPR & Kenya Data Protection Act compliance.

2.13.3 Encryption Architecture

a. Data-at-Rest Encryption

Database Encryption:

o Transparent Data Encryption (TDE) for SQL databases (e.g., MySQL,

PostgreSQL).

o Field-level encryption for highly sensitive data (e.g., medical records).

File Storage Encryption:

o AES-256 encryption for documents, images, and backups.

o Secure key management using Hardware Security Modules (HSMs) or Key

Management Service (KMS).

b. Data-in-Transit Encryption

Secure Communication Protocols:

o HTTPS (TLS 1.2/1.3) for web applications.

o SFTP/SCP for file transfers.

o VPN for inter-facility communications**.**

c. Key Management

Centralized Key Management System (KMS) for encryption keys.

Key Rotation Policy: Automatic key rotation every 90 days.

HSM Integration for secure key storage (optional for high-security needs).

d. Authentication & Access Control

Multi-Factor Authentication (MFA) for system administrators.

Role-Based Access Control (RBAC) to limit decryption privileges.

Digital Certificates for secure user authentication.

2.14 Community Service Order (CSO) Module

Objective: Facilitate non-custodial sentencing through structured community service.

a. Sub-modules: Placement Management

CSO eligibility assessment

Assignment to community service sites (NGOs, govt. projects)

Work hour tracking (digital logbooks)

b. Monitoring & Compliance

Site supervisor feedback integration

Non-compliance alerts (missed hours, misconduct)

Adjustments & reassignments

c. Completion & Certification

Automated completion certificates

Court notifications

Post-CSO follow-up

2.15 Aftercare & Reintegration Module

Objective: Support ex-offenders in post-release rehabilitation.

Sub-modules:

a. Release Planning

Pre-release assessments (housing, employment, counseling needs)

Linkage to aftercare programs

b. Reintegration Support

Job placement & vocational training tracking

Counseling & mentorship records

Family reintegration support

c. Post-Release Monitoring

Recidivism risk tracking

Success metrics (employment stability, sobriety)

2.15 Alternative Dispute Resolution (ADR) Module

Objective: Promote restorative justice and mediation.

Sub-modules:

a. Case Referral & Screening

Eligibility checks for ADR (minor offenses, victim-offender mediation)

Case assignment to mediators

b. Mediation Management

Virtual & in-person mediation scheduling

Agreement drafting & digital signing

Compliance tracking

c. Outcome Reporting

Success/failure rates

Recidivism impact analysis

2.16 Public & Stakeholder Portal

Objective: Enhance transparency and community engagement.

Sub-modules:

a. Victim-Offender Communication

Secure messaging for restorative justice

b. Community Service Opportunities

NGOs/government partners can register projects

c. Public Awareness

Success stories, FAQs, policy updates

1.3.1.2 <u>Hardware Architecture</u>: *[specify: features (use diagrams as appropriate)]*.

The minimum requirements for the systems are as detailed below;

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. Application Server- (Test and Live Environment)

  a) Cloud hosting

  b) On Premise-Hosting

- Processor: Intel Xeon Silver 4314 (or equivalent) with 16 cores, 2.4 GHz
- RAM: Minimum 128GB DDR4 ECC
- Storage: 2TB SSD (RAID 1) + 4TB HDD (RAID 5)

- Operating System: Windows Server 2019 or Higher
- Security: TPM 2.0, Secure Boot, built-in firewall
- Network: Dual 10GbE Ethernet Ports

1.2 Database Compatibility

- Database Compatibility: MySQL, PostgreSQL, Microsoft SQL Server.
- Backup Solution: Automated daily backups on cloud, and offsite replication.

1.3 Storage Server.

- Storage Capacity: Minimum 20TB (expandable)
- RAID Configuration: RAID 6 for data protection
- Backup: Cloud-based integration for offsite storage

2. Network Infrastructure

2.1 Firewalls & Security Appliances

- Firewall Type: Enterprise-Grade Next-Gen Firewall (NGFW),, Web Application Firewall.
- Features: Intrusion Detection & Prevention (IDP), VPN, Anti-Malware, Web Filtering.

2.2 Network Switches

- Core Switch: 10GbE Layer 3 Switch with VLAN Support
- Access Switches: 1GbE PoE

2.3 Wireless Infrastructure

- Wi-Fi Standard: Wi-Fi 6 (802.11ax)
- Access Points: Dual-band Aps.

3. End-User Computing Devices

3.1 Desktop Computers.

- Processor: Intel Core i7 or higher
- RAM: 16GB DDR4
- Storage: 1TB SSD
- Operating System: Windows 11 Professional
- Display: 24" FHD Monitor

3.2 Laptops

- Processor: Intel Core i7
- RAM: 16GB DDR4

- Storage: 1TB SSD
- Security: BitLocker encryption, fingerprint scanner

4.2 Surveillance Equipment

- CCTV Cameras with night vision & motion detection
- Network video recorder-
- Access Control: Biometric & RFID-enabled door entry system.

4.3 Uninterruptible Power Supply (UPS)

- Capacity: 30kVA data center, 1.5kVA for workstations
- Battery Backup Time: Minimum 45 minutes

5. Software & Virtualization

- Virtualization Platform: VMware ESXi / Microsoft Hyper-V
- Security Tools: Endpoint Detection & Response (EDR), Multi-Factor Authentication (MFA).

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for Office of the Attorney General

An ideal hardware architecture for hosting the Case Management System (LCMS), Legal Advisory Database, and Legislative Drafting Information Management System (LDIMS)—both on-premise at the OAG&DOJ and at a selected National Data Center (NDC)—should prioritize security, availability, scalability, and interoperability.

1. Overall Architecture Overview

Hybrid Deployment Model

- **On-Premise (OAG&DOJ):** Primary use for frontend services, local access, and sensitive document handling.
- **Cloud Hosting at a recognized data center:** Acts as main backend infrastructure, DR site, and long-term secure data storage and services hosting.

2. Core Hardware Components

A. On-Premise (OAG&DOJ HQ)

Component	Specification	Purpose
Application Server	2 x Intel Xeon Gold, 128GB RAM, 2TB SSD RAID 10	Hosts web apps (LCMS, LDIMS, Legal DB) locally
Database Server	2 x Intel Xeon Silver, 256GB RAM, 8TB HDD RAID 10 + SSD cache	Local PostgreSQL/MongoDB/MS SQL for fast legal data retrieval
File/Document Server	64GB RAM, 16TB NAS storage, with RAID 6	Stores EDRMS-linked docs, scanned advisories, legal drafts
Load Balancer (HAProxy/Nginx)	Dual-node failover pair	Distributes traffic among web/app servers
Firewall/UTM	Fortinet or equivalent	Ensures network security, VPN access to Konza
Backup Appliance	Veeam or Commvault + 20TB backup storage	Automated nightly backups of all legal data
UPS Power Backup	2 hours runtime minimum	Ensures safe shutdown in power failures

B. Cloud Hosting

Component	Specification	Purpose

Virtualized Server Cluster	3–5 VM Nodes, 256–512GB RAM/node, SAN backend	Redundant virtual infrastructure to host production or DR
Database Cluster	High-availability PostgreSQL/MS SQL cluster	Stores full dataset + backups from OAG&DOJ
Storage System (SAN/NAS)	50TB scalable SAN with snapshots	Long-term secure storage of legal opinions, case files
Disaster Recovery (DR) Site	Active-passive failover setup	Replicates key systems from HQ for DR/BCP
Cloud Load Balancer & API Gateway	For external access, integration with APIs (LexisNexis, KenyaLaw)	

3. Network Architecture

Network Zone	Description
DMZ (Demilitarized Zone)	Hosts public-facing services (login portal, APIs) with web application firewall
Internal Network	Secure internal LAN with application, DB, and file servers
VPN Connectivity	Site-to-site VPN tunnel between OAG&DOJ and the selected National Data Center
Active Directory/LDAP	Centralized user authentication and role-based access

4. Integration & Middleware Layer

- Message Queue (e.g., RabbitMQ/Kafka): For inter-module

  communication (LCMS ↔ LDIMS ↔ Legal DB)
- API Gateway: For secure access to external platforms (Kenya Law, E-Gov platforms etc)
- OCR Engine (e.g., Tesseract or ABBYY): Deployed on the document server or AI node for processing scanned legal opinions.

5. Security Infrastructure

- Multi-Factor Authentication (MFA)
- Intrusion Detection and Prevention Systems (IDS/IPS)
- SIEM (Security Information and Event Management) integration for audit logs
- SSL/TLS Certificates for all web-based traffic
- Data Encryption at Rest and in Transit

6. High Availability and Redundancy

- Dual-NIC on critical servers for network failover
- Database replication between OAG&DOJ and Konza
- Scheduled failover testing every quarter
- SAN snapshotting and hourly incremental backups

7. Scalability Recommendations

- Use containerization (e.g., Docker + Kubernetes) for microservices flexibility
- Deploy horizontal scaling for web/app servers
- Add cold storage tier for archiving old advisories or inactive legal drafts

8. Special Additions for Each Module

LCMS:

- Case metadata storage server (case IDs, court references)
- Legal document template engine

LDIMS:

- Legislative versioning repository (Git-style document tracking)
- AI-driven legal language checker (optional)

Legal Advisory DB:

- AI-powered legal opinion search engine
- Indexing and NLP server (for keyword tagging, case similarity)

9. Suggested Phases for Deployment

1. Phase 1: On-Premise Setup and Initial Data Migration
2. Phase 2: Cloud Integration and Failover Configuration
3. Phase 3: Security Hardening and UAT
4. Phase 4: Go-Live and Performance Monitoring

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

Server Infrastructure

1.1 Application Server

- Processor: Intel Xeon Silver 4314 (or equivalent) with 16 cores, 2.4 GHz

- RAM: Minimum 64GB DDR4 ECC

- Storage: 2TB SSD (RAID 1) + 4TB HDD (RAID 5)

- Operating System: Windows Server 2022 / Ubuntu Server LTS

- Security: TPM 2.0, Secure Boot, built-in firewall

- Network: Dual 10GbE Ethernet Ports

1.2 Database Server

- Processor: Intel Xeon Gold 5318Y, 24 cores, 2.1 GHz

- RAM: Minimum 128GB DDR4 ECC

- Storage: 4TB SSD (RAID 1) + 6TB HDD (RAID 5)

- Database Compatibility: MySQL, PostgreSQL, Microsoft SQL Server

- Backup Solution: Automated daily backups, offsite replication

1.3 Storage Server (NAS/SAN Solution)

- Storage Capacity: Minimum 20TB (expandable)

- RAID Configuration: RAID 6 for data protection

- Backup: Cloud-based integration for offsite storage

- Access Protocols: NFS, SMB, iSCSI

2. Network Infrastructure

2.1 Firewalls & Security Appliances

- Firewall Type: Enterprise-Grade Next-Gen Firewall (NGFW)

- Features: Intrusion Detection & Prevention (IDP), VPN, Anti-Malware, Web Filtering

2.2 Network Switches

- Core Switch: 10GbE Layer 3 Managed Switch with VLAN Support

- Access Switches: 1GbE PoE+ Managed Switches

2.3 Wireless Infrastructure

- Wi-Fi Standard: Wi-Fi 6 (802.11ax)

- Access Points: Dual-band APs with WPA3 encryption

- Coverage: Prison administration blocks, visitor areas, and secured zones

3. End-User Computing Devices

3.1 Desktop Computers (For Correctional Offices & Administration)

- Processor: Intel Core i7, AMD Ryzen 7 or higher

- RAM: 16GB DDR4

- Storage: 512GB SSD

- Operating System: Windows 11 Professional / Ubuntu 22.04

- Display: 24" FHD Monitor

- Security: Biometric authentication, TPM 2.0

3.2 Laptops (For Mobile Use & System Administration)

- Processor: Intel Core i7 or Apple M1/M2 Chip

- RAM: 16GB DDR4

- Storage: 512GB SSD

- Battery Life: Minimum 10 hours

- Security: BitLocker encryption, fingerprint scanner

3.3 Tablets (For Field Officers & Mobile Data Entry)

- Processor: Qualcomm Snapdragon 8cx Gen 2 / Apple A15 Bionic

- RAM: 8GB

- Storage: 256GB SSD

- Security: Facial Recognition, Secure Enclave

4. Peripherals & Specialized Devices

4.1 Printers & Scanners

- Multi-Function Printers (MFPs) for document processing

- High-Speed Scanners for inmate records digitization

4.2 Surveillance Equipment

- CCTV Cameras: AI-powered night vision & motion detection

- Access Control: Biometric & RFID-enabled door entry systems

4.3 Uninterruptible Power Supply (UPS)

- Capacity: 10kVA for servers, 2kVA for workstations

- Battery Backup Time: Minimum 30 minutes

5. Software & Virtualization

- Virtualization Platform: VMware ESXi / Microsoft Hyper-V

- Backup & Disaster Recovery: Veeam Backup & Replication

- Security Tools: Endpoint Detection & Response (EDR), Multi-Factor Authentication (MFA)

1.4   Systems Administration and Management Functions Required to be met by the Information System.

1.4.1   The Information System MUST provide for the following management, administration, and security features at the overall System level in an integrated fashion.

1.4.1.2 Installation, Configuration and Change Management: *[specify: features].*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

The specifications for the installation, configuration and change management is as follows:

1. System installation, implementation, unit testing, and integrated end-to-end system testing on all modules.

2. Tests reports and functionality for all modules on a test environment before pushing updates to the live environment.

3. UAT plan and User Acceptance Testing

4. System vulnerability Assessment and penetration testing (VAPT).

5. Code maintenance and upgrade on security management. This includes fine tuning of errors, closure of existing bugs and security vulnerabilities.

6. Patch management , system upgrades including versioning and up to date licensing for any purchased softwares and implemented modules.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion/Advisory Database for the OAG&DOJ

1. Installation, Configuration, and Change Management

1.1 Installation

The installation phase will involve setting up the Case Management System (CMS), Legal Opinion/Advisory Database (LOD), and Legislative Drafting Information Management System (LDMIS). The contractor will be responsible for the installation of the following:

- **System Deployment**: Deploy the CMS, LOD, and LDMIS on a secure and scalable server infrastructure that meets OAG&DOJ's operational and performance needs.
- **Database Setup**: Set up and configure the underlying databases for each system (e.g., SQL, NoSQL, or other relevant database technologies) based on the technical requirements and data models defined during the system design phase.
- **Software Setup**: Install necessary software components (e.g., application servers, databases, web servers) and ensure all required system dependencies are met.

- **Security Setup**: Implement security protocols, including firewall configurations, encryption, multi-factor authentication (MFA), and role-based access control (RBAC), to protect sensitive legal data.
- **Integration Setup**: Integrate each system with existing OAG&DOJ infrastructure, including other relevant applications, legacy systems, and third-party tools (e.g., Document Management Systems, Case Management Systems).
- The installation will be completed in stages, beginning with testing in a controlled environment (development or staging) and subsequently moving to production after successful testing and validation.

1.2 Configuration

Following installation, the configuration phase will involve the customization of each system to meet the specific operational needs of OAG&DOJ. Configuration will include:

- **System Configuration**:
    - **Case Management System (CMS)**: Configure workflows, case life cycle stages, and user roles to reflect the OAG&DOJ's operational processes and legal case management procedures.
    - **Legal Opinion Database (LOD)**: Configure metadata schemas, document types, indexing structures, and full-text search capabilities to ensure efficient retrieval and management of legal opinions.
    - **Legislative Drafting Information Management System (LDMIS)**: Configure templates, legislative workflow processes, and document management rules for creating and reviewing legal drafts.
- **User Roles and Permissions**: Configure user accounts, roles, and permissions across the three systems to ensure access control is aligned with OAG&DOJ's security requirements and job responsibilities (e.g., administrative, legal staff, paralegals, etc.).
- **System Customization**: Customize the user interface (UI) and user experience (UX) based on feedback from OAG&DOJ

stakeholders, ensuring the design is intuitive and aligns with user personas, workflows, and accessibility standards.

- **Data Migration Configuration**: Configure data import and export procedures for migrating legacy data from existing OAG&DOJ systems into the new CMS, LOD, and LDIS. This may involve mapping data fields, cleaning legacy data, and verifying the accuracy of data transfer.
- **Integrations**: Configure integration points with external legal systems (e.g., LexisNexis, Kenya Law) and internal systems such as document management systems, case management platforms, or knowledge-sharing tools.
- **Performance Tuning**: Optimize the system's performance to handle large volumes of data, users, and requests efficiently, ensuring fast search results, low latency, and high availability.

1.3 Change Management

Change Management ensures that all changes, whether system updates, enhancements, bug fixes, or integrations, are carefully planned, tested, and documented to minimize operational disruption and maintain system integrity. The following steps will guide the change management process:

- **Change Request Process**: Define a formal process for submitting, reviewing, and approving change requests. This will include any updates to functionality, system configuration, integrations, and user roles.
- **Impact Analysis**: Conduct a thorough analysis of the potential impact of any change request on system functionality, performance, security, and user operations. This includes identifying potential risks, dependencies, and the need for additional resources.
- **Version Control**: Implement version control mechanisms for system configurations, code changes, and documentation. Each change will be tracked with detailed records of the version history to ensure traceability and accountability.
- **Testing and Validation**:

- ○ Unit Testing: Test individual components after any change to ensure they function correctly.
- ○ Integration Testing: Verify that all integrated systems and components continue to work seamlessly after a change.
- ○ User Acceptance Testing (UAT): Involve OAG&DOJ staff in UAT for major changes to ensure the system meets their needs and expectations. Any issues identified will be resolved before the change is deployed to production.

- **Deployment and Rollback Plan**: Develop and follow a structured deployment plan for rolling out changes. This includes backup and rollback plans to ensure that any issues encountered during deployment can be resolved quickly without compromising system stability.
- **Communication**: Communicate all changes clearly to the OAG&DOJ staff, including potential impacts, timelines, and any required actions on their part (e.g., system downtime, new features to be used). Regular updates will be provided on the status of major changes.
- **Documentation**: Ensure that all changes are fully documented, including updated system configurations, code changes, and new functionalities. This will be stored in the system documentation and will be made accessible to the OAG&DOJ staff and technical teams.
- **Training and Support**: Provide training sessions and user guides to OAG&DOJ staff for any new system features, functionalities, or configurations introduced by the change. Offer ongoing support through a ticketing system to address any issues raised post-deployment.
- **Monitoring and Continuous Improvement**: After the change is deployed, continuously monitor the system's performance and user feedback. Analyze any issues and identify areas for improvement to refine the system.

1.4 Post-Deployment Support and Maintenance

After successful installation, configuration, and change management implementation, the contractor will provide ongoing support and maintenance for the systems. This will include:

- **Helpdesk Support**: A dedicated support team available to address any operational issues or user queries related to the CMS, LOD, or LDIS.
- **System Updates and Patches**: Regular updates to ensure the systems remain secure and up to date with the latest technologies. This includes applying patches for software vulnerabilities and providing feature enhancements based on user feedback.
- **Performance Monitoring**: Proactive monitoring of system performance to identify potential issues, such as slow queries, hardware failures, or data discrepancies.
- **Backups and Disaster Recovery**: Regular backups of the system and associated data, along with a disaster recovery plan to ensure business continuity in case of unexpected system failures.

1.5 Documentation and Reporting

- **Installation and Configuration Documentation**: Provide detailed documentation of the installation and configuration process, including system architecture, integrations, and customizations made.
- **Change Management Reports**: Maintain a record of all changes made to the system, including approvals, testing outcomes, and deployment details. Provide quarterly reports summarizing system performance, change requests, and ongoing issues.
- **User Manuals**: Provide comprehensive user manuals that outline system features, configuration options, and procedures for managing changes and troubleshooting.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

Installation, Configuration and Change Management:

- The set of applications shall be by one software manufacturer. Different software vendors are not accepted.

- The bidder shall develop a dummy environment to allow users to test the system before full implementation and the test environment shall be similar to the live environment.

- The proposed solution shall be capable of importing data from files formatted in common formats such as XML, MS Word, PDF, Excel, CSV, Access, etc.

- The proposed solution must integrate with other third-party active directories and to allow for the sending of alerts and other information to integrations targeted recipients.

- The proposed ICMIS solution shall have an interface with the ability to integrate with other systems.

1.4.1.3 <u>Operational Monitoring, Diagnostics, and Troubleshooting</u>: *[specify: **features**]*.

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

a) The system design should be able to perform the following tasks:

1. Automatically assign tasks to officers and monitor tickets based on the service charter and generate tickets for each task.

2. Tracking of workflows and escalation matrix of tasks to ensure compliance and adherence to legal timelines.

3. Integration with call center services for timely resolution of enquiries as per the act and the service charter.

4. A platform for reporting of incidents and tracking of their resolution status.

5. A platform for customer feedback on ODPC services.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

To ensure sustained performance, security, and reliability of the system, the contractor shall implement comprehensive operational monitoring, diagnostics, and troubleshooting capabilities across all platforms. These will include:

1. Real-Time System Monitoring

- Implement centralized dashboards to track system health, uptime, response times, and usage metrics.
- Monitor key components such as databases, application servers, APIs, storage, and integrations with external systems.
- Enable performance thresholds and automated alerts for abnormal behaviors or system degradation.

2. Logging and Diagnostics

- Maintain detailed logs for all user actions, system errors, and integration events.
- Provide centralized log management for real-time analysis and historical review.
- Enable drill-down diagnostics to identify root causes of system or user issues efficiently.

3. Automated Alerting and Notification

- Configure automated email/SMS alerts for critical system events, including:

  o System outages or crashes

  o Unauthorized access attempts

  o Failed integrations or data processing jobs

- Ensure alerts are directed to designated IT personnel or system administrators.

4. Self-Healing and Recovery Mechanisms

- Implement auto-recovery mechanisms for minor faults (e.g., restarting services upon failure).
- Maintain redundant system components to minimize downtime.

5. Incident and Issue Tracking

- Integrate with or deploy an IT Service Management (ITSM) platform or helpdesk module.
- Allow users to report bugs or performance issues directly from within the system.
- Track issue resolution time, responsible personnel, and escalation levels.

6. Analytics and Reporting

- Generate regular reports on system performance, usage trends, and incident patterns.
- Use analytics to identify recurring issues and inform system optimization strategies.

7. Security Monitoring

- Monitor security-related events (e.g., login attempts, data access patterns, role modifications).
- Enable audit trail reviews and anomaly detection tools for suspicious behavior.

8. Maintenance Dashboard

- Provide an administrator console with tools for:

    o Viewing system status and service uptime

    o Executing maintenance tasks (e.g., re-indexing, log purging, backup status)

    o Reviewing recent errors and system alerts

9. Support and Escalation Protocols

- Define clear procedures for issue prioritization, escalation, and response time.
- Ensure 24/7 or business-hours support options based on SLA requirements.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

Key Features:

1. **Inmate & Staff Monitoring**

    ○ Tracks prisoner movements, transfers, and release schedules.

    ○ Monitors staff attendance, shift allocation, and assignments.

2. **Incident Reporting & Case Management**

    ○ Digital incident reporting system for security breaches or misconduct.

    ○ Keeps records of court cases, parole applications, and rehabilitation progress.

3. **Security & Surveillance**

    ○ CCTV monitoring with real-time alerts for suspicious activities.

    ○ RFID tracking for monitoring inmate and staff movement.

    ○ Access control systems to restrict unauthorized entry.

4. **Health & Rehabilitation Tracking**

    ○ Keeps medical records and alerts for check-ups or emergencies.

    ○ Tracks rehabilitation programs and skills training.

5. **System Monitoring & Troubleshooting**

    ○ Automated system health checks to detect failures.

    ○ Alerts for performance issues and security threats.

    ○ Detailed log records for audits and investigations.

1.4.1.4 <u>User Administration and Access Control</u>; User and Usage Monitoring and Audit Trails: *[specify: features]*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. system administration:

    a) the system should be able to allow user set-up and administration,

    b) provide for automated backups and restore. s

    c) Security administration including application for security filters and privileges,

    d) Help desk, Incident reporting, ticketing and support,

    e)   Database Management, User Setup and Administration, Roles and access privileges administration,

    f) Workflow Configuration and Management, Audit Trails, Archiving, Automated backups and Restore and Reporting.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. User Administration and Access Control

● **Role-Based Access Control (RBAC):** Implement a flexible RBAC framework to define and manage access privileges based on user roles (e.g., Administrator, State Counsel, Paralegal, Drafter, Reviewer).

- **Granular Permissions:** Configure permissions at module, document, and action levels (view, edit, delete, approve) to ensure strict data control.
- **Authentication Mechanisms:** Enforce strong user authentication protocols, including username/password, and support for Multi-Factor Authentication (MFA) for enhanced security.
- **User Management Dashboard:** Provide an administrative interface for account creation, role assignment, status management (active/inactive), and password resets.
- **Single Sign-On (SSO):** Enable secure and unified login experience across the CMS, LOD, and LDIMS through integration with government authentication infrastructure.

2. User and Usage Monitoring

- **Activity Logging:** Capture all user interactions with the system, including login/logout events, document views, edits, deletions, and downloads.
- **Usage Analytics Dashboard:** Provide real-time statistics and usage reports to understand system utilization trends, high-traffic modules, and document access patterns.
- **Session Monitoring:** Track user sessions to detect anomalies and enhance user support and compliance checks.

3. Audit Trails

- **Immutable Logs:** Maintain tamper-proof audit logs for all critical actions and data modifications to ensure accountability and traceability.
- **Searchable Logs:** Include a log viewer interface to filter logs by date, user, document ID, and action type for quick access during audits or investigations.
- **Automated Alerts:** Configure alerts for unusual or unauthorized access attempts, failed login attempts, or data export activities.

- **Data Retention and Compliance:** Define retention periods for logs based on national data protection and compliance standards (e.g., Kenya Data Protection Act, ISO 27001).

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

User Administration and Access Control

- The System should provide Multi-factor Authentication of users using OAuth 2.0

- Each user must be authenticated with a unique user-id / username, password and one-time login code generated by the application while logging on the application. The User IDs / Usernames should be case-sensitive

- User accounts management activities include but are not limited to new user creation, user maintenance, and user authentication (during login)

- All new user accounts must have a system-generated random password when created. A secure way of communicating the initial password to the user should be utilized, e.g. via an email account or SMS

- The system must support password expiry features with a configurable frequency. This should be parameterized to allow flexibility in adjusting this value as required (from non-expiry to activation of expiry).

- The system should not support automatic logins to guard against brute force attacks. The login page should include a code-generating mechanism.

- The system shall generate a code at log-in. The code shall be sent to the registered e-mail or SMS through a registered mobile phone number. The code shall be entered on the login page to grant authentication.

- These password features should be configurable to support future complexity requirements.

- The solution should implement a secure self-service password recovery mechanism in the event the user forgets their password using verification of existing parameters.

- The login page and all subsequent authenticated pages must be exclusively accessed over Transport Layer Security (TLS). All active sessions must be encrypted.

- The solution should support expiring of newly created accounts if not used for a configurable period of time. This should be parameterized to allow flexibility in adjusting this value as required. An auto generated alert should be sent to the users some set days before the account is deactivated.

- The password must be changed after a configurable duration. This should be parameterized for flexibility. An auto generated password change alert should be sent to the users some set days before the password expires.

- The solution must support password lockout after a configurable number of unsuccessful login attempts. This should be parameterized to allow flexibility in adjusting this value as required.

- The solution must log out a user account after the session has been idle for a configurable duration. This should be parameterized to allow flexibility in adjusting this duration as required.

- The solution must not allow the re-use of a past password until a set period and a set number of password changes have been made. This should be parameterized to allow flexibility in adjusting this value as required.

1.4.1.5 <u>System and Information Security and Security Policies</u>: *[specify:*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. Code maintenance and upgrade on security management- The bidder should during and post implementation provide for fine tuning of system errors, closure of any existing bugs and security loopholes ,proactive security updates and patching.

2. The System should have systems & application security configuration and administration , audits trails and archival of system logs.

3. The bidder should carry out proactive security updates and patching.

4. The system should ensure seamless user experience while ensuring security and privacy of information collected in line with the Data Protection Act, 2019 & Data protection Regulations, 2022.

5. The Vendor should perform a vulnerability assessment and submit a report for independent verifications by ODPC prior to rollout of the system.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion Database for the Office of the Attorney General & Department of Justice

To protect the confidentiality, integrity, and availability of sensitive legal information handled by the OAG&DOJ, all systems—CMS, LOD, and LDIMS—must be designed and implemented in alignment with global best practices and national regulations. The solution provider shall ensure robust information security mechanisms are embedded at every level of development and deployment:

1. **Core Security Requirements**
   - **User Authentication & Access Control**: Implement Multi-Factor Authentication (MFA), strong password policies, and role-based access control (RBAC) to ensure only authorized users access specific functionalities and data.
   - **Data Encryption**: All sensitive data must be encrypted during transmission (using HTTPS/TLS) and at rest (using AES-256 or equivalent).
   - **Audit Logging**: Enable tamper-proof audit logs capturing login attempts, data modifications, document access, and administrative actions.

- **Network Security**: Use secure communication protocols, firewalls, intrusion detection/prevention systems (IDS/IPS), and Virtual Private Network (VPN) support for remote access.

- **Endpoint and Application Security**: Systems must be protected from malware and unauthorized software through application whitelisting, endpoint protection tools, and secure coding practices (OWASP standards).

- **Data Backup & Disaster Recovery**: Implement automated backups, versioning, and a documented disaster recovery plan to ensure rapid recovery in the event of data loss or system failure.

- **Security Monitoring & Incident Response**: Real-time monitoring of systems for anomalies, with automatic alerting and predefined incident response procedures.

2. **Compliance & Security Governance**

- Align system security with OAG&DOJ's internal ICT and data protection policies.

- Ensure adherence to national and international data protection and cybersecurity regulations.

- Conduct regular security assessments and penetration testing before go-live and periodically thereafter.

- Provide documentation on security architecture, controls, and compliance evidence.

- Train end-users and administrators on security awareness, privacy, and safe system usage.

3. **Deliverables**

- Security architecture design and documentation.

- Risk assessment and mitigation strategy.

- Security testing reports (including vulnerability and penetration testing).

- User and admin security training materials.

- Incident response and disaster recovery plans.

- Security compliance certification or audit report (if applicable).

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

System and Information Security and Security Policies:

- The system MUST have an inbuilt System Administrator Role with the ability to monitor all the requests submitted in the system.

- The system MUST support multiple levels of security. This includes protecting certain fields from unauthorized access. In addition, access to certain functions and data MUST be protected until they are approved by policymakers.

- Application security MUST be integrated with database security and Active Directory.

- The system parameters, including application controls, authorizations and standard security configuration MUST be clear, well defined and can allow processing in an efficient and controlled manner while protecting valuable data.

- The System MUST have the ability to provide adequate audit trails that can be reviewed for information.

- These records MUST be non-editable and be secured from unauthorized access.

- Electronic records MUST maintain the old and new values to the change and the transaction used to generate the record.

- The system MUST allow one to define security events / incidents which upon occurrence, the system generates an email and sends it to a defined distribution list to notify the security administration "in an immediate and urgent manner".

- The messaging system MUST also have the capability of being interfaced to send this message externally.

- The system MUST have the flexibility to create user defined responsibilities / profiles to which different requests /functions / reports can be attached.

- The system MUST be able to define policies for different levels of users e.g. a "High Security" profile for power users whose requirements are stricter than "Medium Security" profile for business end users Clear segregation of privileges must be presented and implemented by security matrix of roles against authority.

- Security matrix will be gathered and created by the vendor during the project analysis phase. Data masking/encryption of sensitive data MUST be supported.

- The system MUST have an option to support digital signatures.

1.4.1.6 <u>Back-up and Disaster-Recovery</u>: *[specify:* **features***]*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. The bidder in collaboration with ODPC will ensure the IDMIS's backups are up to date and are able to restore the IDMIS System in case of failure or an incident.

2. The System should provide for both offsite and onsite backup capabilities across multiple environments including cloud.

3. The backup should include backups for both the live and test environment.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. the bidder in collaboration with OAG&DOJ will ensure the AGis backups are up to date and are able to restore it incase of failure or an incident

2. the system should provide for both off site and on premise backup capabilities across multiple environments including cloud

3. the backup should include backups for both the live and test environment

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

Back-up and Disaster Recovery:

- ICMIS Application shall have in-built capability to manage application software backups and restore with Source Control and the solution shall have in-built software to manage automated database backups and restore.

- The ICMIS Must have the ability to create scheduled backups of system data.

- System should allow different backups including daily, and weekly among others.

- The supplier MUST prepare all Technology policies and procedures related to the system including authorization, backups and restore manuals, table space maintenance, archival etc.

- Knowledge transfer documentation for the solution implemented should include, but not be limited to, operating system administration, database administration, application administration, modules management, troubleshooting, backup and restore.

- The system must provide for security backup facilities to enable complete file restore and recovery as well as remote backups, online backups and multiple backups.

1.5 Performance Requirements of the Information System

1.5.1   The Information System MUST reach the following performance levels.

Lot 1 : Data Management Systems for the Office of the Data Protection Commissioner.

The system should be a web based platform accessible 24 hours a day, 7 days a week from any part of the world with minimum if not zero downtime (99.9% availability), a seamless search functionality to enable users to easily filter and search contents and the Search Engine Optimization (SEO) functionalities . It should provide for unlimited concurrent users access and real time processing of data and information.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The system should be a web based platform accessible 24 hours a day, 7 days a week from any part of the world with minimum if not zero downtime (99.9% availability), a seamless search functionality to enable users to easily filter and search contents and the Search Engine Optimization (SEO) functionalities . It should provide for unlimited concurrent users access and real time processing of data and information.

The solution should be designed to remove all single points of failure. The solution should provide the ability to recover from failures, thus protecting against multiple component failures.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

The system should be a web based platform accessible 24 hours a day, 7 days a week from any part of the world with minimum if not zero downtime (99.9% availability), a seamless search functionality to enable users to easily filter and search contents and the Search Engine Optimization (SEO) functionalities . It should provide for unlimited concurrent users access and real time processing of data and information.

The solution should be designed to remove all single points of failure. The solution should provide the ability to recover from failures, thus protecting against multiple component failures.

C. SERVICE SPECIFICATIONS – SUPPLY & INSTALL ITEMS

2.1 System Analysis, Design and Customization/Development

2.1.1 The Supplier MUST perform the following Analysis and Design activities using a formal system analysis/development methodology with the following key activities and design deliverables.

Lot 1 : Data Management System for the Office of the Data Protection Commissioner

2.1.1.1 Detailed Analysis:

1. Develop design, integration and functional requirements document (FRD) as per the user request.

      2. List and structure of each module required.

   2.1.1.2 <u>Physical Design</u>:

      1. Develop design , graphical interface documents, process flow mapping ,database structures

   2.1.1.3 <u>Integrated System</u>:

      1. The system should have the capability to integrate to the existing systems and should also allow migration of data from the existing system where applicable.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. Detailed Analysis

- Develop a Functional Requirements Document (FRD) based on user needs.

- Identify and define all modules required, such as inmate management, staff allocation, security monitoring, health tracking, and case management.

2. Physical Design

- Create user-friendly graphical interfaces for seamless interaction.

- Develop process flow diagrams for each system module.

- Define database structures to store and manage prisoner records, incident reports, and security logs.

3. Integrated System

- Ensure compatibility with existing correctional systems for smooth integration.

- Enable secure migration of historical data from old systems where applicable.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

1. Detailed Analysis

- Develop a Functional Requirements Document (FRD) based on user needs.

- Identify and define all modules required, such as inmate management, staff allocation, security monitoring, health tracking, and case management.

2. Physical Design

- Create user-friendly graphical interfaces for seamless interaction.

- Develop process flow diagrams for each system module.

- Define database structures to store and manage prisoner records, incident reports, and security logs.

3. Integrated System

- Ensure compatibility with existing correctional systems for smooth integration.

- Enable secure migration of historical data from old systems where applicable.

- Ensure interoperability with biometric, access control, and surveillance systems.

2.2   Software Customization / Development

2.1.1   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.

Lot 1: Data Management System for the Office of the Data Protection Commissioner.

The bidder must be **knowledgeable in various software development methodologies**, including:

- Agile – For iterative development, continuous feedback, and flexibility.

- Waterfall – For structured and sequential development.

- Rapid Application Development – For faster prototyping and deployment.

Development must follow **best practices** and adhere to **open standards** for interoperability and scalability.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The bidder must be **knowledgeable in various software development methodologies**, including:

- Agile – For iterative development, continuous feedback, and flexibility.

- Waterfall – For structured and sequential development.

- Rapid Application Development – For faster prototyping and deployment.

Development must follow **best practices** and adhere to **open standards** for interoperability and scalability.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

The bidder must be **knowledgeable in various software development methodologies** including:

- **Agile** – For iterative development, continuous feedback, and flexibility.

- **Waterfall (Cascade)** – For structured and sequential development.

- **Rapid Application Development (RAD)** – For faster prototyping and deployment.

Development must follow **best practices** and adhere to **open standards** for interoperability and scalability.

2.3   System Integration (to other existing systems)

2.3.1   The Supplier MUST perform the following Integration Services

Lot 1: Data Management System for the Office of the Data Protection Commissioner.

1.   Email and SMS Integration

2. Integration with approved payments modes – bank, paybills, cards, mobile money etc.

3. Process workflow, alerts and notifications.

4. Business Intelligence, reporting and analytics.

5. High availability, reliability and security.

6. API integrations with existing systems and platforms.

7. Integration with the e-Citizen platform and other relevant systems.

8. Integration with Business Registration Services platforms for validation of clients.

9. Integration with existing Information Security tools deployed by the Office.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. Email and SMS Integration

2. Integration with approved payments modes – bank, paybills, cards, mobile money etc.

3. Process workflow, alerts and notifications.

4. Business Intelligence, reporting and analytics.

5. High availability, reliability and security.

6. API integrations with existing systems and platforms.

7. Integration with the e-Citizen platform and other relevant systems.

8. Integration with Business Registration Services platforms for validation of clients.

9. Integration with existing Information Security tools deployed by the Office.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

System Integration

Integration of the ICMIS with other relevant government systems such as:

1. Email and SMS Integration
2. Integration with approved payments modes – bank, paybills, cards, mobile money etc.

3. Integration with the e-Citizen platform and other relevant systems.
4. Integration with existing Information Security tools deployed.
5. National Registration Bureau System.(National ID)
6. Civil Registration (Registration of births and deaths).
7. National Health System.
8. ERP System(IFMIS,HRIS-KE).
9. Integrated Security Management System.
10. Judiciary System.
11. National Police System
12. National Education System.
13. TVET System.
14. Electronic Monitoring System.
15. API integrations with existing systems and any other government API.

2.4 Training and Training Materials.

2.4.1   The Supplier MUST provide the following Training Services and Materials.

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. **Training and Skills/Knowledge Transfer**

a) Technical Skills Assessment**:** The tenderer is expected to explicitly state the technical skills of its staff required to successfully implement and sustain the System. Attach CVs and certificate copies.

b) Methods of Training and Skill Transfer**:**The tenderer is expected to elaborate on their proposed training methods to be used for skills transfer who will ensure that ODPC has enough internal capacity to maintain and use the System

c) Training Curriculum**:** The tenderer is expected to provide the training curriculum to be used to train all users in HQ on use of the system. These users will then train other end users (Training of Trainers concept) The training curriculum shall adhere to the functional requirements.

d) Admin/Technical Training**:** The tenderer is expected to provide the training curriculum to be used to train at least twenty (20) IT technical staff (administrators and technical support staff). This should be comprehensive to ensure that the system administrators and technical staff can fully manage and support the solution.

e) Training Evaluation: The tenderer is expected to provide a methodology of evaluation of the training, learning and skills transfer.

f) Experienced trainers**:** The tenderer should have trainers to be able to transfer knowledge to ODPC's staff. The successful tenderer should provide a detailed Training Schedule for their solution, detailing the training approach and

methods, location, and curriculum as well as indicate the cost of training in the price schedule.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

Training and/Knowledge Transfer

1. Technical Skills Assessment**:** The tenderer is expected to explicitly state the technical skills of its staff required to successfully implement and sustain the System. Attach CVs and certificate copies.

2. Methods of Training and Skill Transfer**:**The tenderer is expected to elaborate on their proposed training methods to be used for skills transfer who will ensure that Office of the Attorney General has enough internal capacity to maintain and use the System

3. Training Curriculum**:** The tenderer is expected to provide the training curriculum to be used to train users in HQ and regional offices on use of the system. These users will then train other end users (Training of Trainers concept) The training curriculum shall adhere to the functional requirements.

4. Admin/Technical Training**:** The tenderer is expected to provide the training curriculum to be used to train IT technical staff (administrators and technical support staff). This should be comprehensive to ensure that the system administrators and technical staff can fully manage and support the solution.

5. Training Evaluation: The tenderer is expected to provide a methodology of evaluation of the training, learning and skills transfer.

6. Experienced trainers**:** The tenderer should have trainers to be able to transfer knowledge to the staff of the Office of the Attorney General. The successful tenderer should provide a detailed Training Schedule for their solution, detailing the training approach and methods, location, and curriculum as well as indicate the cost of training in the price schedule.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

TRAINING MODULE

1	TRAINING & KNOWLEDGE TRANSFER	(FS,PS,CR,NS)	REMARKS
1.0	The bidder is expected to explicitly state the technical skills of its staff required to successfully implement and sustain the System. Attach CVs and certificate copies		
2	Methods of Training, Change management and Skill Transfer		
2.0	The bidder is expected to elaborate on their proposed training methods to be used for skills transfer which will ensure that SDCS has enough internal capacity to maintain and use the System. Conduct a structured change management approach to transitioning users and teams within SDCS to effectively adopt and utilize a new system		
3	Training Curriculum		
3.0	The bidder is expected to provide the training curriculum to be used to train users on use of the system. These users will then train other end users (Training of Trainers concept) The training curriculum shall adhere to the functional requirements.		
4	Admin/Technical Training		

4.0	The bidder is expected to provide the training curriculum to be used to train technical support staff		
5	Training Evaluation		
5.0	The bidder is expected to provide a methodology of evaluation of the training, learning and skills transfer.		
6	Training facility		
6.0	All training must be provided at an accredited center. Bidders shall propose training site and location and this shall agree with the purchaser.		
7	Training materials		

| 7.0 | (i)   The Vendor shall develop training materials illustrated in English with screen shots of all user interfaces of the application. The training materials must be designed to also facilitate the Training for Trainers approach, and must be developed with a view that they can be used by SDCS staff in conducting future training. The bidder is expected to provide all trainees with training material both soft and hard copies.

(ii) The Vendor must maintain and update all documentation for any system changes performed by the Vendor during the contract period and any negotiated extensions at no cost to the client.

(iii)   The Vendor must agree that SDCS and shall have the right to copy all documents for internal distribution.

(iv) The Vendor shall propose a method of ensuring efficient document control. The Vendor shall provide the details of a Knowledge Coordination Approach which indicates the specific formats (versions) and procedures for all documentation to be | | |

disseminated amongst the client project team.

(v) The Vendor must ensure that a detailed User Guide is provided with the system. Context-sensitive Help screens (help narratives) within the system are also required.

(vi) In addition to the full User Guide referenced above, the Vendor will be required to provide a "Quick reference guide", preferably in the form of a small booklet. The objective is to provide a structured, user-friendly, means to help a user perform a task. It is expected that this guide will focus on providing "how-to" essentials of the key everyday functions without the user having to peruse the main document.

In order to ensure sustainability, it is expected that within the proposed twelve (24) months of post-implementation, knowledge transfer will be completed and identified ICT officials of the SDCS will be fully trained so that it is able to maintain and operate the system independently without Vendor support.

8	Experienced trainers		
8.0	The bidder should possess experienced trainers to be able to transfer knowledge to the Ministry's staff. The successful bidder should provide a detailed Training Schedule for their solution, detailing the training approach and methods, location, and curriculum as well as indicate the cost of training in the price schedule.		

2.4.1.1 <u>User</u>: *[for example, specify:* **minimum curricula, modes of training, modes of testing, and training materials for: the introduction to computers, the operation of the relevant equipment incorporated in the System, as well as the operation of the Software applications incorporated in the System;** *as appropriate, reference the relevant subsection in the Background and Informational Material Section containing any detailed information regarding the available training facilities; etc.]*

2.4.1.2 <u>Technical</u>: *[for example, specify:* **minimum curricula, modes of training, modes of testing (e.g., certification levels), training materials and training locations for: the key technology and methodology components of the Information System;** *etc.]*

2.4.1.3 <u>Management</u>: *[for example, specify:* **minimum curricula, modes of training, modes of testing, training materials and training locations for: the familiarization with the functionality, technology and methodology components of the Information System, corporate management of information systems;** *etc.]*

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.]*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. Data Migration: Bidders are required to create and submit a detailed technical proposal and duration for Data migration and conversion requirements from the

existing IDMIS to the new system that contain all the necessary deliverables that the bidder will follow to ensure smooth phased migration.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Supplier **MUST** provide all necessary services, resources, tools, and expertise to carry out data conversion and migration from existing systems to the new platform as applicable. The services must cover the following aspects:

a. Data Inventory and Scope

- Detailed inventory of all data sources, including legacy systems (databases, spreadsheets, physical records if digitized).
- Approximate **volume of data** to be migrated (e.g., number of records, size in GB/TB).
- Types and structures of data (e.g., structured – relational databases; unstructured – scanned documents or PDFs).

b. Data Mapping and Transformation

- Define how existing data fields will be mapped to the new system's data schema.
- Include necessary **data transformation logic** (e.g., date formats, codes, field normalization).

c. Data Cleansing

- Identify and remove duplicate, obsolete, or inconsistent records.
- Correct errors, standardize values, and ensure data integrity prior to migration.

d. Data Migration Tools and Methodology

- Description of migration tools to be used (custom scripts, ETL tools, middleware).
- Method of migration (e.g., one-time bulk load, phased migration, API-based migration).

- Mechanisms to ensure minimal disruption to ongoing operations.

e. Media and Storage

- Specify the media and format of source data (e.g., SQL Server database, CSV files, XML, SharePoint).
- Define secure temporary and final storage solutions for data in transit.

f. Migration Timing and Schedule

- Proposed timeline for migration (phases and milestones).
- Downtime windows (if required) and fallback/rollback procedures.

g. Validation and Quality Assurance

- Pre-migration data audits.
- Post-migration verification (record counts, checksum validation, referential integrity checks).
- Sign-off and user acceptance testing procedures.

h. Security and Compliance

- Ensure data is encrypted during migration.
- Comply with relevant data protection laws, including the **Kenya Data Protection Act** and **GDPR** (if applicable).
- Chain-of-custody documentation for sensitive data.

i. Documentation and Handover

- Full documentation of the conversion process, mapping rules, and validation results.
- Training of OAG&DOJ ICT team on migration processes and any reusable scripts or tools.

j. Post-Migration Support

- Provide a period of post-migration support to resolve any data-related issues.
- Availability of consultants or engineers during stabilization period.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

Bidders are required to create and submit a detailed technical proposal on how data should be migrated .

2.6   Documentation Requirements

2.6.1   The Supplier MUST prepare and provide the following Documentation.

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. Develop and provide an inception report.

2. undertake and provide a user acceptance report.

3. provide system documentation and user manuals.

4. provide a draft service level agreement.

5. user's functional requirement document (FRD).

6. technical support manual.

7. handover report and any other system related report that may be required.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Supplier **MUST** prepare and provide the following documentation, both in hard and electronic formats (editable and PDF), in English:

1. **System Architecture Documentation**
   - High-level and low-level architecture diagrams
   - Description of system components and their interactions
   - Technology stack and design rationale
2. **Functional Specifications**
   - Detailed description of all modules, features, and functionalities
   - User roles, workflows, and system behavior under different scenarios
3. **Technical Specifications**
   - Server and hosting requirements
   - APIs and integration interfaces

  - ○ Security architecture, encryption methods, and compliance standards
4. **Installation & Configuration Guides**
  - ○ Step-by-step instructions for system installation and deployment
  - ○ Environment setup requirements (test, staging, production)
5. **User Manuals**
  - ○ End-user manuals (with screenshots) for all user roles
  - ○ Client portal user guide (if applicable)
6. **Administrator Guides**
  - ○ Instructions for managing users, permissions, settings, and logs
  - ○ Maintenance procedures, backups, and recovery steps
7. **Training Materials**
  - ○ Training manuals, slide decks, and videos used during end-user and admin training sessions
  - ○ Frequently Asked Questions (FAQs)
8. **Testing & QA Reports**
  - ○ Test plans, test cases, and test results
  - ○ Security and performance testing reports
9. **Data Migration & Integration Plan**
  - ○ Documentation of any data migration processes
  - ○ Integration guidelines with existing systems (e.g., IFMIS, Judiciary CMS)
10. **Change Management & Version Control**
  - ○ Logs of changes made during development
  - ○ Version control strategy and release notes
11. **Maintenance & Support Plan**
  - ○ Post-deployment support schedule and contacts
  - ○ Service Level Agreement (SLA) details
12. **Compliance & Licensing Documents**
  - ○ Proof of compliance with local and international standards (e.g., Kenya's Data Protection Act, GDPR)
  - ○ Licenses for any third-party tools used

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

Comprehensive documentation of the systems technical architecture,user manuals and knowledge transfer capacity building to ensure sustainability.

> 2.6.1.1 <u>End-User Documents</u>: *[for example, specify: **type(s) of end-user documents; language; content; formats; quality control and revision management; medium; reproduction and distribution methods**; etc.]*
>
> 2.6.1.2 <u>Technical Documents</u>: *[for example, specify: **type(s) of technical documents; language; content; formats; quality control and revision management; medium;, reproduction and distribution methods**; etc.]*

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 <u>Supply and Installation Activities</u> under the Contract:

2.7.1.1 **Project Team Leader:**

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. Masters in Computer Science, Engineering, IT or related degree

2. Should have a minimum of 5 years of experience in the Management of IT Projects and a professional experience in developing, implementing and managing scalable systems with competencies in systems and information management and IT in general. Give a minimum of 2 projects.

3. ICT-related certification, PRINCE2/PMI /PMP or other equivalent project management certifications.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. Masters in Computer Science, Engineering, IT or related degree

2. Should have a minimum of 5 years of experience in the Management of IT Projects and a professional experience in developing, implementing and managing scalable systems with competencies in

systems and information management and IT in general. Give a minimum of 2 projects.

3. Certification in Project Management such as PRINCE2/PMP

4. Proven experience coordinating multi-disciplinary technical teams and managing stakeholder engagement in the public or legal sector.

5. Demonstrable experience in delivering similar projects

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

I. Masters in Computer Science, Engineering, IT or related degree
II. Should have a minimum of 5 years of experience in the Management of IT Projects and a professional experience in developing, implementing and managing scalable systems with competencies in systems and information management and IT in general. Give a minimum of 2 projects.
III. ICT-related certification, PRINCE2/PMI /PMP or other equivalent project management certifications.

2.7.1.2 **System designer and developer/System Engineer**

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. B.SC/ in Computer Science, Engineering or related degree

2. Have relevant certifications in systems development e.g. expert system engineering professional (ESEP), certified system engineering professional (CSEP) , etc. or have relevant certification in the area of web-based systems and certification in various Programming software and databases e.g. C, C++, ORACLE, MYSQL etc.

3. 4+ years of experience in ICT system design, development and implementation with a bias on database management. Give a minimum of 2 projects.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. Bsc in Computer Science, Engineering, IT or related degree

2. Should have a minimum of 5 years full-stack development, designing enterprise systems, systems implementation. Give a minimum of 2

projects.

3. Certifications in systems development such as expert system engineering professional (ESEP), certified system engineering professional (CSEP) , etc. or have relevant certification in the area of web-based systems and certification in various Programming software and databases e.g. C, C++, ORACLE, MYSQL etc.

4. Demonstrated experience in designing and developing enterprise-level information systems, preferably in government or legal sectors.

5. Proven track record of working on projects involving system integration, API development, and data migration.

6. Strong understanding of software architecture, design patterns, and modern development methodologies (e.g., Agile, DevOps). Proficient in relevant programming languages and frameworks (e.g., Java, .NET, PHP, Python, Node.js, React/Angular, etc.).

7. Familiarity with cloud infrastructure and deployment (AWS, Azure, GCP) is desirable.

8. Experience with database design and optimization (e.g., MySQL, PostgreSQL, Oracle, MongoDB).

9. Knowledge of security principles, including encryption, access control, and secure coding practices.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

I.   B.SC/ in Computer Science, Engineering or related degree

II.   Have relevant certifications in systems development e.g. expert system engineering professional (ESEP), certified system engineering professional (CSEP) , etc. or have relevant certification in the area of web-based systems and certification in various Programming software and databases e.g. C, C++, ORACLE, MYSQL etc.

III.   4+ years of experience in ICT system design, development and implementation with a bias on database management. Give a minimum of 2 projects.

2.7.1.3 **Security expert**

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. B.SC/ in Computer Science, Engineering or related degree

2. Have relevant certifications in the area of system security

3. 4+ years of experience in the ICT security field and should have experience in ICT systems security and design, development, and Implementation of security solutions. Give reference a minimum of four projects.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Supplier **MUST** provide a dedicated **Security Expert** as part of their technical team for the duration of the contract. The Security Expert shall be responsible for ensuring that all system components, data flows, and user access meet the highest standards of cybersecurity, data protection, and compliance with relevant laws and best practices.

1. Bsc in Computer Science, Engineering, IT or related degree

2. Certifications in systems security such CISSP, CISM, CISA, CEH or equivalent

3. 5+ years of experience in the ICT security field and should have experience in ICT systems security and design, development, and Implementation of security solutions. Give reference to a minimum of four projects.

4. Minimum of 5 years of hands-on experience in implementing and managing information security in large-scale ICT systems.

5. Demonstrated experience in securing web-based and cloud-based applications, including authentication, encryption, access control, and vulnerability management.

6. Experience with compliance frameworks such as ISO 27001, NIST, or GDPR, and preferably the Kenya Data Protection Act.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

I.   B.SC/ in Computer Science, Engineering or related degree
II.   Have relevant certifications in the area of system security
III. 4+ years of experience in the ICT security field and should have experience

in ICT systems security and design, development, and Implementation of security solutions. Give reference a minimum of four projects.

2.7.1.4 **Database Administrator**

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. B.SC/ in Computer Science, Engineering or related degree

2. Have relevant certifications in Database administration e.g. Oracle, SAP, Microsoft SQL Database administrator, etc. and have relevant certification in the area of web-based systems and certification in various Programming software e.g. C, C++, ORACLE, MYSQL, the area

3. 4+ years of experience in ICT database administration, development and implementation. Give a minimum of four projects.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Supplier MUST assign a qualified Database Administrator (DBA) as part of the technical team during the supply, installation, and commissioning phases of the contract.

1. Bsc in Computer Science, Engineering or related degree

2. Have relevant certifications in Database administration e.g. Oracle Certified Professional (OCP), MySQL/19c, SAP, Microsoft SQL Database administrator, etc. and have relevant certification in the area of web-based systems and certification in various Programming software e.g. C, C++, ORACLE, MYSQL

3. 5+ years of experience in ICT database administration, development and implementation including installation, configuration, and maintenance of RDBMS; Backup and recovery strategies; Performance tuning and optimization etc.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

I. B.SC/ in Computer Science, Engineering or related degree
II. Have relevant certifications in Database administration e.g. Oracle, SAP,

Microsoft SQL Database administrator, etc. and have relevant certification in the area of web-based systems and certification in various Programming software e.g. C, C++, ORACLE, MYSQL, the area

III. 4+ years of experience in ICT database administration, development and implementation. Give a minimum of four projects

2.7.1.5 System Integrator

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. B.Sc. in computer science/IT or relevant field.

2. 4 Years experience in integrating and deploying systems of diverse technologies. Experience in installing, maintaining and upgrading integrated systems, Give reference of 3 projects.

3. Have relevant certifications in systems Integration, Records Management and Certified Workflow designer.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. A degree in Computer Science, Information Technology, or a related field.
2. Minimum of 5 years of experience in system integration for enterprise-level IT systems.
3. Proven experience integrating diverse platforms including case management systems, document management systems, financial systems (e.g., IFMIS), identity management systems, and government databases.
4. Certification in system integration tools, middleware platforms (e.g., MuleSoft, Apache Camel), or service-oriented architecture (SOA) frameworks is an added advantage.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

I. B.Sc. in computer science/IT or relevant field and have relevant certifications in the area of ICT infrastructure (e.g. networks. Hardware etc.)

II. (6+ Years) experience in integrating and deploying systems of diverse technologies. Experience in installing, maintaining and upgrading integrated systems, Give reference of 3 projects.

III.   Have relevant certifications in systems Integration, Records Management and Certified Workflow designer

2.7.1.6 **Webmaster (designer and developer) and Mobile Application**

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. B.Sc. in computer science/IT or relevant field.

2. Certifications in website development/graphic design/mobile applications tools.

3. Experience: Give reference of 3 projects for reference.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Supplier MUST provide a qualified Webmaster with expertise in both web design and development, along with mobile application development skills.

1. B.Sc. in computer science/IT or relevant field.

2. Certifications in website development/graphic design/mobile applications tools.

3. Minimum of 5 years' experience in web development including mobile applications

4. Familiarity with responsive design, CMS platforms (e.g., WordPress, Drupal), and RESTful APIs.

5. Experience with version control (e.g., Git), testing tools, and CI/CD processes.

6. Demonstrated ability to deploy secure, scalable, and efficient mobile and web platforms.

7. Experience: Developed and delivered 3 key projects in web development, graphic design and mobile applications (provide brief reference).

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

  I.   B.Sc. in computer science/IT or relevant field.

 II.   Certifications in website development/graphic design/mobile applications tools.

III.   Experience: Give reference of 3 projects where the person has designed.

2.7.1.7 **Quality Assurance Expert**

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. A Bachelor's Degree in IT or related.

2. At least 8 years of experience in designing, developing and maintaining test cases and strategies for testing and quality assurance.Give reference of a minimum of 3 projects undertaken in the last 8 years

3. Professional Certifications in system quality assurance. (Certified quality engineer, certified quality auditor, Certified Test Engineer (CSTE) Certified Software Quality Analyst (CSQA), Certified Associate in Software Testing(CAST), CMSQ (Certified Manager of Software Quality (attach certificate)

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Bidder MUST provide a Quality Assurance (QA) Expert as part of their technical team during the Supply, Installation, Testing, and Commissioning activities under the Contract.

1. A Bachelor's Degree in IT or related.

2. At least 5 years of experience in designing, developing and maintaining test cases and strategies for testing and quality assurance.Give reference of a minimum of 3 projects undertaken in the last 7 years

3. Professional Certifications in system quality assurance. (Certified quality engineer, certified quality auditor, Certified Test Engineer (CSTE) Certified Software Quality Analyst (CSQA), Certified Associate in Software Testing(CAST), CMSQ (Certified Manager of Software Quality (attach certificate)

4. Demonstrated experience in **quality control processes** for both

hardware and software components in public sector or enterprise environments.

5. Familiarity with **ISO standards** (e.g., ISO/IEC 25010, ISO 9001) and quality assurance best practices.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

I. A Bachelor's Degree in IT or related. (Information System, Computer Science, Computer Engineering, Software Engineering Etc)

II. At least 8 years of experience in designing, developing and maintaining test cases and strategies for testing and quality assurance.Give reference of a minimum of 3 projects undertaken in the last 8 years

III. Professional Certifications in system quality assurance. (Certified quality engineer, certified quality auditor, Certified Test Engineer (CSTE) Certified Software Quality Analyst (CSQA), Certified Associate in Software Testing(CAST), CMSQ (Certified Manager of Software Quality (attach certificate)

D. TECHNOLOGY SPECIFICATIONS – SUPPLY & INSTALL ITEMS

3.0 General Technical Requirements

3.0.1 Language Support: All information technologies must provide support for the *[insert: **either national or business language(s) of the end-user(s)]**. Specifically, all display technologies and software must support the ISO [insert: **character set number**] character set and perform sorting according to [insert: **appropriate standard method**].*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

Language Support: All information technologies must provide support for the English Language. Specifically, all display technologies and software must support the ISO/IEC 12207 standard on software life cycle processes and perform sorting according to appropriate standard method.

Dates: All information technologies MUST properly display, calculate, and transmit date data, including, but not restricted to 21st-century date data. The date must be in the DDMMYYYY format and the time zone must be EAT.

Electrical Power: All active (powered) equipment must operate on 220v +/- 20v voltage range and frequency range, 50Hz +/- 2Hz. All active equipment must include power plugs standard in Kenya.

> **Environmental:** Unless otherwise specified, all equipment must operate in environments of 0-45 degrees centigrade temperature, 20-80 percent relative humidity, and 0-40 grams per cubic meter of dust conditions.
>
> **Safety:** Unless otherwise specified, all equipment must operate at noise levels no
>
> greater than *55* decibels.

All electronic equipment that emits electromagnetic energy must be certified as meeting *US FCC class B or END 55022 and END 50082-1,* or equivalent, emission standards.

> The system should be developed with trending technology standards. It should be
>
> based on open standards.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

All information technologies must provide full support for both **British English** and **Swahili**, which are the official business and national languages of the end-users within the Government of Kenya. Specifically:

1. All display technologies and software must support the **ISO/IEC 10646 (Unicode)** character set to ensure compatibility with a wide range of languages and scripts, including Latin characters used in both English and Swahili.

2. Sorting, collation, and text processing must follow the **Unicode Collation Algorithm (UCA)** or equivalent standards to ensure

accurate alphabetical ordering and search functionality, particularly for multilingual content.

3. User interfaces, system messages, help documentation, and error notifications should be available in **British English** and optionally in **Swahili**, depending on user context or departmental needs.

4. The solution must allow for **future localisation or translation** to other regional languages where applicable.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. Electrical Power: All active (powered) equipment must operate on 220v +/- 20v voltage range and frequency range, 50Hz +/- 2Hz. All active equipment must include power plugs standard in Kenya.

2. Environmental: Unless otherwise specified, all equipment must operate in environments of 0-45 degrees centigrade temperature, 20-80 percent relative humidity, and 0-40 grams per cubic meter of dust conditions.

3. Safety: Unless otherwise specified, all equipment must operate at noise levels no greater than *55* decibels.

4. All electronic equipment that emits electromagnetic energy must be certified as meeting *US FCC class B or END 55022 and END 50082-1,* or equivalent, emission standards.

5. The system should be developed with trending technology standards. It should be based on open standards.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

General Technical Requirements

- **Language Support:** All information technologies must provide support for the English Language. Specifically, all display technologies and software must support the ISO/IEC 12207 standard on software life cycle processes and perform sorting according to appropriate standard method.

- **Dates:** All information technologies MUST properly display, calculate, and transmit date data, including, but not restricted to 21st-century date

data. The date must be in the DDMMYYYY format and the time zone must be EAT.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

- **Electrical Power:** All active (powered) equipment must operate on 220v +/- 20v voltage range and frequency range, 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 of *[specify, **temperature, humidity, and dust conditions**, e.g., 10-30 degrees centigrade, 20-80 percent relative humidity, and 0-40 grams per cubic meter of dust]*.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

Unless otherwise specified, all equipment must operate effectively in environments with the following conditions:

- Ambient Temperature: 10°C to 30°C

- Relative Humidity: 20% to 80% (non-condensing)

- Dust Concentration: 0 to 40 grams per cubic meter

- Operating Altitude: Up to 2,000 meters above sea level

- Equipment must be suitable for standard office environments and must be installed in well-ventilated areas with adequate cooling.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

- **Environmental:** Unless otherwise specified, all equipment must operate in environments of 0-45 degrees centigrade temperature, 20-80 percent relative humidity, and 0-40 grams per cubic meter of dust conditions.

  3.0.4   Safety:

  3.0.4.1 Unless otherwise specified, all equipment must operate at noise levels no greater than *[insert: **maximum number**, e.g., 55]* decibels.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

Unless otherwise specified, all equipment must operate at noise levels not exceeding 55 decibels (dB), measured at a distance of 1 meter in a free-field environment under standard operating conditions. Compliance must be verified through certified acoustic test reports or in-situ testing, in accordance with ISO 11201 or equivalent recognized standards. This requirement is intended to ensure occupational health and safety for users and maintenance personnel. Any deviations must be formally approved and justified.

3.0.4.2 All electronic equipment that emits electromagnetic energy must be certified as meeting *[insert: **emission standard**, e.g., US FCC class B or END 55022 and END 50082-1],* or equivalent, emission standards.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

All electronic equipment supplied under this contract that emits electromagnetic energy must be certified as meeting internationally recognized electromagnetic emission standards to ensure safe and interference-free operation.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

- **Safety:** Unless otherwise specified, all equipment must operate at noise levels no greater than *55* decibels.

  o All electronic equipment that emits electromagnetic energy must be certified as meeting *US FCC class B or END 55022 and END 50082-1,* or equivalent, emission standards.

- The system should be developed with trending technology standards. It should be based on open standards.

3.1   Computing Hardware Specifications

3.1.1   Processing Unit Type 1: *[specify: **name of processing unit and technical function** (e.g., Central Database Server)]:*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

3.1.1 Processing Unit Performance-Host Machine

(a) Processing Power:

- The server should have at least two high-performance processors, each with 64 cores for fast and efficient processing.

(b) Input-Output Performance:

- Fast data transfer with at least 4 high-speed network ports.
- Supports modern storage connections for quick data access.

3.1.1.2 Processor Expandability

- Should allow for adding more processors in the future.
- At least 4 extra slots for upgrades like better storage or network cards.

3.1.1.3 Processor Memory and Storage

- RAM: At least 256GB memory, expandable to 1TB for smooth operations.
- Storage**:**
  - 10TB SSD (fast storage) for running applications.
  - 50TB HDD (large storage) for keeping records.
  - Backup system: A tape storage for long-term data retention.

3.1.1.4 Processing Unit Fault Tolerance

- Backup power supply to keep the system running during failures.
- Error-checking memory to prevent data corruption.
- Data backup features to protect against data loss.

3.1.1.5 Processing Unit Management Features

- Remote management support for IT administrators to monitor and fix issues.
- Security monitoring for tracking system performance and potential issues.

3.1.1.6 Processing Unit Input and Output Devices

- Network connectivity: At least 4 high-speed ports for fast and secure data access.
- User authentication devices: Support for smart card readers and biometric login.

3.1.2.2 Expandability

- Can support more RAM and storage upgrades if needed.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

Processing Unit Type 1: Central Database Server - To serve as the core data repository for all modules of the Legal Case Management System, LDIMS, Legal Opinion Database, supporting high transaction loads and ensuring 24/7 uptime.

- Processor: Dual Intel Xeon Silver 4314, 16 cores per CPU, 2.4GHz

- RAM: 128GB DDR4 ECC, expandable to 512GB

- Storage: 4TB SSD, RAID 10 configured

- Network: Dual 10GbE NICs

- Power Supply: Redundant (hot-swappable)

- Virtualization: Supports VMware ESXi and Hyper-V

- Operating System: Compatible with Windows Server 2022 and Linux

- Security: TPM 2.0, BIOS password, secure boot

- Form Factor: 2U Rack-mounted

- Warranty: 3-year onsite support, 4-hour SLA

- Compliance: ISO 27001, RoHS, Energy Star

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

3.1.1 Processing Unit Type 1: Central Database Server

This is the **main system** that stores and processes inmate records, ensuring smooth operations and data security.

3.1.1.1 Processing Unit Performance

(a) **Processing Power:**

- The server should have **at least two high-performance processors**, each with **64 cores** for fast and efficient processing.

- It should handle **at least 1,000 users** at the same time without delays.

(b) **Input-Output Performance:**

- **Fast data transfer** with at least **4 high-speed network ports**.

- **Supports modern storage connections** for quick data access.

3.1.1.2 Processor Expandability

● Should allow for adding **more processors in the future**.

● **At least 4 extra slots** for upgrades like better storage or network cards.

3.1.1.3 Processor Memory and Storage

● **RAM:** At least **256GB memory**, expandable to **1TB** for smooth operations.

● **Storage:**

  ○ **10TB SSD** (fast storage) for running applications.

  ○ **50TB HDD** (large storage) for keeping records.

  ○ **Backup system:** A **tape storage** for long-term data retention.

3.1.1.4 Processing Unit Fault Tolerance

● **Backup power supply** to keep the system running during failures.

● **Error-checking memory** to prevent data corruption.

● **Data backup features** to protect against data loss.

3.1.1.5 Processing Unit Management Features

● **Remote management support** for IT administrators to monitor and fix issues.

● **Security monitoring** for tracking system performance and potential issues.

3.1.1.6 Processing Unit Input and Output Devices

● **Network connectivity:** At least **4 high-speed ports** for fast and secure data access.

● **User authentication devices:** Support for **smart card readers and biometric login**.

3.1.1.7 Other Processing Unit Features

● **Power-saving mode** to reduce energy consumption.

● **Secure login options** such as fingerprint or smart card access.

3.1.2 Processing Unit Type 2: General Purpose Workstation

For Correctional Officers and Administrative Staff

This is the **everyday computer** used for data entry, reporting, and managing inmate records.

3.1.2.1 Processing Unit Performance

- **Fast processor:** Intel **Core i9** or **AMD Ryzen 9** for smooth multitasking.

- **Handles multiple applications** without slowing down.

3.1.2.2 Expandability

- Can support **more RAM and storage upgrades** if needed.

3.1.2.3 Memory and Storage

- **RAM: 32GB** for fast performance.

- **Storage:**

    - **1TB SSD** for quick system operation.

    - **4TB HDD** for additional file storage.

3.1.2.4 Fault Tolerance

- **Auto-save and recovery features** to protect data in case of crashes.

3.1.2.5 Management Features

- **Secure login** using a **fingerprint scanner or smart card reader**.

3.1.2.6 Input and Output Devices

- **24-inch Full HD monitor** for clear visuals.

- **Standard keyboard and mouse**.

- **Fast internet connection** for accessing the central database.

3.1.2.7 Other Features

- **Power-saving mode** to reduce electricity use.

3.2   Network and Communications Specifications

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

3.2.1 Local Area Network (LAN)

The LAN connects all computers, servers, and devices office(s), ensuring smooth internal communication and data sharing.

3.2.1.1 Equipment and Software

- Network Protocols: Supports TCP/IP, IPv4 & IPv6 for reliable data transmission.
- Performance: Minimum 1 Gbps speed, with support for 10 Gbps for core systems.
- Expandability: Should support adding more devices and users as needed.
- Fault Tolerance:
    - Auto failover to keep the system running in case of hardware issues.
- Administration & Security:
    - Centralized network monitoring with alerts for downtime and security threats.
    - Firewall and intrusion detection system (IDS) for cybersecurity protection.

3.2.1.2 Cabling

- Cable Type: Cat6a or Fiber Optic for fast and reliable data transfer.
- Cable Protection & Standards:
    - Cables should be enclosed in conduits to prevent damage.
    - Follows ANSI/EIA/TIA 598 cable labeling standards for easy identification.
    - Proper grounding and shielding to reduce electrical interference.

———

3.2.2 Wide Area Network (WAN)

3.2.2.1 Equipment and Software

- Protocols Supported: MPLS, VPN, HTTPS for secure remote access.

- Performance: Minimum 1 Gbps connection to external networks.

- Expandability: Should allow additional network locations as required.

- Fault Tolerance:

  ○ Dual ISPs (Internet Service Providers) for redundancy.

  ○ Auto failover to a backup network in case of primary connection failure.

- Administration & Security:

  ○ Firewall protection with deep packet inspection.

  ○ 24/7 network monitoring to detect and prevent cyber threats.

3.2.2.2 Telecommunications Services

- Media: Fiber optic with LTE/5G.

- Capacity: Minimum 1 Gbps dedicated bandwidth for stable communication.

- Security:

  ○ End-to-end encryption for all communication.

  ○ Two-factor authentication (2FA) for remote access.

- Administration & Management:

  ○ Automatic bandwidth allocation for high-priority services.

- **Network Requirements:**

  ○ Dedicated minimum 100 Mbps bandwidth for smooth video calls.

  ○ VPN protection for remote access security.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The solution should support both wired (Gigabit Ethernet) and wireless (Wi-Fi 6) connectivity to ensure high-speed data transmission across departments. Networking equipment, including routers, switches, and firewalls, must support VLAN segmentation, Quality of Service (QoS), and secure remote access through VPN. All hardware should comply with IPv6 standards and include redundancy features (dual power supply, link aggregation) to ensure high availability. The network should also support secure integration with external systems (e.g., Judiciary CMS, IFMIS) via encrypted protocols such as HTTPS, SFTP, or IPsec.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

3.2.1 Local Area Network (LAN)

The LAN connects all computers, servers, and devices within the correctional facility, ensuring smooth internal communication and data sharing.

3.2.1.1 Equipment and Software

- Network Protocols: Supports TCP/IP, IPv4 & IPv6 for reliable data transmission.

- Performance: Minimum 1 Gbps speed, with support for 10 Gbps for core systems.

- Expandability: Should support adding more devices and users as needed.

- **Fault Tolerance:**

    ○ Redundant switches and backup links to prevent network failures.

    ○ Auto failover to keep the system running in case of hardware issues.

- **Administration & Security:**

    ○ Centralized network monitoring with alerts for downtime and security threats.

    ○ Firewall and intrusion detection system (IDS) for cybersecurity protection.

3.2.1.2 Cabling

- Cable Type: Cat6a or Fiber Optic for fast and reliable data transfer.

- Topology: Star topology to allow direct connections between devices.

- Cable Protection & Standards:

    ○ Cables should be enclosed in conduits to prevent damage.

○ Follows ANSI/EIA/TIA 598 cable labeling standards for easy identification.

○ Proper grounding and shielding to reduce electrical interference.

3.2.2 Wide Area Network (WAN)

The WAN connects the correctional facility to external systems like government databases, law enforcement agencies, and cloud-based services.

3.2.2.1 Equipment and Software

● Protocols Supported: MPLS, VPN, HTTPS for secure remote access.

● Performance: Minimum 1 Gbps connection to external networks.

● Expandability: Should allow additional network locations as required.

● **Fault Tolerance:**

○ Dual ISPs (Internet Service Providers) for redundancy.

○ Auto failover to a backup network in case of primary connection failure.

● **Administration & Security:**

○ Firewall protection with deep packet inspection.

○ 24/7 network monitoring to detect and prevent cyber threats.

3.2.2.2 Telecommunications Services

● Media: Fiber optic with LTE/5G backup for reliability.

● Capacity: Minimum 1 Gbps dedicated bandwidth for stable communication.

● **Security:**

○ End-to-end encryption for all communication.

○ Two-factor authentication (2FA) for remote access.

● **Administration & Management:**

○ Automatic bandwidth allocation for high-priority services like emergency calls.

○ Cloud-based telecommunication management for easier control and monitoring.

3.2.3 Other Communications Equipment

● Modems & Routers: High-speed 5G and fiber optic modems for stable internet access.

● Facsimile Devices: Digital fax servers for secure document transmission.

● Public Address System (PA System): Integrated speakers for facility-wide announcements.

● Intercom System: Secure two-way communication between different facility zones.

3.2.4 Video Conferencing & Congress Equipment

For remote meetings, legal hearings, and high-security communications.

● **Video Conferencing System:**

○ 1080p HD cameras with AI tracking for clear visuals.

○ Noise-canceling microphones for clear audio.

○ Encrypted video calls for security.

- **Display Equipment:**

  ○ Large-screen monitors (55 inches) for conference rooms.

  ○ Projectors with wireless casting support.

- **Network Requirements:**

  ○ Dedicated minimum 100 Mbps bandwidth for smooth video calls.

  ○ VPN protection for remote access security.

3.3   Ancillary Hardware Specifications

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

3.3.1 Shared Data Storage Devices

- Main Storage:
  ○ Large-capacity storage (100TB or more) for data storage.
  ○ Fast access with SSD technology.
- Backup Storage:
  ○ Tape storage (50TB) for long-term backups.
  ○ Automatic backup and data security features.

3.3.2 Shared Output and Input Devices

3.3.2.1 General Requirements

- All printers and scanners should support A4 paper size.

3.3.2.2 Printers

Used for printing reports, legal documents, and facility notices.

- Fast Black & White Printer – prints 50 pages per minute
- Color Printer – high-quality color prints for official documents.

3.3.2.3 Scanners

Used for digitizing Records.

- Fast Scanner – scans 60 pages per minute (PPM).
- High-Resolution Scanner – for clear and detailed images.

3.3.3 Power Backup

3.3.3.1 Uninterruptible Power Supply (UPS)

Ensures power remains on during outages.

- Main Data Center UPS – supports servers for 3hrs
- Workstation UPS – 45-minute backup power for individual computers.
- Surge Protection – prevents damage from power fluctuations.

3.3.4 Security & Environmental Control

3.3.4.1 Equipment Cabinets

- Lockable server racks to protect equipment.
- Built-in cooling fans to prevent overheating.

3.3.4.2 Environmental Control

- Air conditioning for server rooms (keeps temperature stable).
- Humidity control to prevent equipment damage.

3.3.4.3 Physical Access Control

- Biometric & RFID door access – only authorized staff can enter.
- CCTV cameras – for 24/7 surveillance.

3.3.4.4 Digital Security

- Smart cards & fingerprint scanners for secure system login.
- Two-factor authentication (2FA) for extra security.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The system must be compatible with and support the following hardware specifications to ensure seamless integration and operation:

- **Servers:** Minimum specifications of Intel Xeon processors with at least 16GB of RAM and 500GB of SSD storage for high-performance data processing and storage. The system should be compatible with both on-premise and cloud-based servers, depending on deployment preference.

- **Workstations and Terminals:** Each user workstation should support Windows 10 or higher with a minimum of 8GB RAM, an Intel Core i5 processor, and a 500GB hard drive for smooth operation of the system. For remote users, the system must support secure access from devices such as laptops, desktops, and mobile devices running modern operating systems.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

3.3.1 Shared Data Storage Devices

Used for storing and backing up inmate records, surveillance footage, and reports.

- **Main Storage:**

  - Large-capacity storage (100TB or more) for data storage.

  - Fast access with SSD technology.

  - Backup system to prevent data loss.

- **Backup Storage:**

  - Tape storage (50TB) for long-term backups.

  - Automatic backup and data security features.

- **Connections & Features:**

  - Fast data transfer ports for quick access.

  - Remote access for backup management.

  - Self-monitoring system to detect issues early.

3.3.2 Shared Output and Input Devices

3.3.2.1 General Requirements

- **All printers and scanners should support A4 paper size.**

3.3.2.2 Printers

Used for printing reports, legal documents, and facility notices.

- Fast Black & White Printer – prints 50 pages per minute (PPM).

- Color Printer – high-quality color prints for official documents.

- Large-Format Printer – for maps and posters (A3 size).

3.3.2.3 Scanners

Used for digitizing inmate records, visitor logs, and paperwork.

- Fast Scanner – scans 60 pages per minute (PPM).

- High-Resolution Scanner – for clear and detailed images.

3.3.3 Power Backup

3.3.3.1 Uninterruptible Power Supply (UPS)

Ensures power remains on during outages.

- Main Data Center UPS – supports servers for 30 minutes.

- Workstation UPS – 15-minute backup power for individual computers.

- Surge Protection – prevents damage from power fluctuations.

3.3.4 Security & Environmental Control

3.3.4.1 Equipment Cabinets

- Lockable server racks to protect equipment.

- Built-in cooling fans to prevent overheating.

3.3.4.2 Environmental Control

- Air conditioning for server rooms (keeps temperature stable).

- Humidity control to prevent equipment damage.

3.3.4.3 Physical Access Control

- Biometric & RFID door access – only authorized staff can enter.

- Motion sensors & CCTV cameras – for 24/7 surveillance.

3.3.4.4 Digital Security

- Smart cards & fingerprint scanners for secure system login.

- Two-factor authentication (2FA) for extra security.

3.4   Standard Software Specifications

3.4.1   System Software and System-Management Utilities:

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

The tenderer shall state the proposed components of the platform in terms of:

1. Names and versions
2. The integration engine.
3. The database proposed.
4. Operating system proposed.
5. Client or end-user operating systems supported
6. The system must be scalable to accommodate growth in the user base as well as data analysis transactions. Comment on how this can be realized.
7. Elaborate on the open-endedness of the system to allow integration with other systems within Government
8. Describe the programming language/technology of the system.
9. Setup of necessary IT security measures for the system

For each specification, tenderers are requested to provide a clear and concise explanation and provide across-reference to where that explanation or supporting information can be found in other parts of the technical proposal. They are required to provide a system brochure that points out the functionalities that have been outlined in this tender document.

The Vendor should build and implement the IDMIS System on the latest platforms, technologies and software's.

Any charges such as annual maintenance, annual license fee and software support cost should be clearly stated and included in the bid price. The privileges that will be experienced by subscribing to such annual charges should be clearly stated. E.g. Product upgrade at no additional cost etc.

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The system should support an operating system that is compatible with the organization's hardware and facilitates the efficient operation of all software applications. It must support the latest versions of popular platforms such as **Windows Server** or **Linux** distributions, ensuring stability, security, and scalability. System management utilities, such as backup tools, disk management, and monitoring tools, should be included for managing system performance, troubleshooting, and ensuring minimal downtime.

For system management, the software should include utilities for centralized monitoring of system health, automatic patch management, and user management. The system should also integrate with existing network management tools and support automation for routine tasks like backups and system updates. Utilities for efficient resource allocation, such as memory and CPU monitoring, should be incorporated to ensure optimal system performance.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

3.4 Standard Software Specifications for Correctional Services

*This section outlines **the software required** for system operation, security, networking, and database management.*

3.4.1 System Software and System-Management Utilities

3.4.1.1 Processing Unit Type 1 (Servers - Central Database Server)

- ***Operating System:*** *Windows Server or Linux (Ubuntu Server, CentOS).*

- ***Security:*** *Enterprise-level **antivirus & firewall** protection.*

- ***Backup Tools:*** *Automatic data backup and recovery software.*

- ***System Monitoring:*** *Tools for **performance tracking & troubleshooting**.*

- ***Remote Access:*** *Secure access tools (e.g., **SSH, RDP**).*

3.4.1.2 Processing Unit Type 2 (Workstations - General Purpose PCs for Officers & Staff)

- *Operating System: Windows 11 Pro or Linux.*

- *Security: **Anti-virus & endpoint protection**.*

- *Maintenance Tools: Disk cleanup, defragmentation, and performance optimization software.*

- *Remote Troubleshooting: Software for remote assistance and updates.*

3.4.2 Networking and Communications Software

- *Network Protocols Supported: TCP/IP, IPv6, VPN, and Secure Sockets Layer (SSL).*

- *Network Security: Firewall, **intrusion detection/prevention systems (IDS/IPS)**.*

- *Remote Administration: **Secure VPN for external access** to the network.*

- *Failure Management: **Automatic alerts & logging** for system failures.*

- *Wireless Management: Support for **secure Wi-Fi protocols** (WPA3).*

3.4.3 General-Purpose Software

- *Office Software: Microsoft Office Suite (Word, Excel, PowerPoint, Outlook) or LibreOffice.*

- *Email and Communication: Secure email client (e.g., **Microsoft Outlook, Mozilla Thunderbird**).*

- *PDF and Document Handling: Adobe Acrobat or open-source alternatives.*

- *Web Browsers: Secure, policy-enforced browsers (Google Chrome, Mozilla Firefox).*

- *Programming Tools: **Python, SQL, Bash scripting** for automation and analysis.*

3.4.4 Database Software and Development Tools

- *Database Management System: PostgreSQL, MySQL, or Microsoft SQL Server.*

- *Security Features: Data encryption, access control, and audit logs.*

- ***Database Backup: Automated daily backups & cloud replication***.

- ***Development Tools:*** *SQL Workbench, pgAdmin, Microsoft SSMS.*

3.4.5 Business Application Software

- ***Inmate Management System:*** *Tracks inmate records, case history, and transfers.*

- ***Visitor Management System:*** *Manages **visits, approvals, and security checks**.*

- ***HR and Payroll Software:*** *Handles officer attendance, salary, and benefits.*

- ***Asset Management System:*** *Tracks prison equipment, vehicles, and supplies.*

- ***Incident Reporting System:*** *Logs security events and officer reports.*

3.5   Consumables

   3.5.1   Printer Ink / Toner – Printer Type 1:

3.6   Other Non-IT Goods

   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

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

1. **Inspection Criteria:**

   a. Performance Tests: Systems must meet minimum speed, storage, and processing requirements.

   b. Security & Compliance: All security features (encryption, access controls) must be enabled and functioning.

2. **Inspection Methods:**

   a. System Diagnostics – Running built-in hardware and software tests.

    b. Network & Connectivity Testing – Ensuring internet and internal connections work as expected.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

Inspections will be carried out at various stages of the project to ensure compliance with the specifications and standards outlined in the contract. The key points for inspections are:

1. **Inspection of Deliverables**: Ensure that all hardware, software, and documentation meet the specified requirements and quality standards.
2. **Inspection of Setup & Installation**: Verify that the installation of the system, hardware, and other infrastructure is completed as per the agreed standards.
3. **Third-party Inspections**: The Contractor shall allow and facilitate independent inspection by authorized third-party inspectors or representatives from the contracting entity to ensure compliance with all specifications and contractual requirements.
4. **Compliance to Standards**: The Contractor must ensure that the systems and components meet the relevant industry standards, local regulations, and safety requirements, including certifications such as ISO, IEC, or any other relevant certification.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

    4.1.1 Due Diligence

To be done at vendor site.

- *Inspection Criteria:*

  - *Performance Tests: Systems must meet **minimum speed, storage, and processing requirements**.*

  - *Security & Compliance: All security features (encryption, access controls) must be **enabled and functioning**.*

- *Inspection Methods:*

  - *System Diagnostics – Running built-in hardware and software tests.*

○ ***Network & Connectivity Testing*** *– Ensuring **internet and internal connections** work as expected.*

○ ***Software Verification*** *– Confirming correct **installation and licensing** of required applications.*

4.2   Pre-commissioning Tests

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.
The vendor will be required to perform the following documented tests before commissioning of the system.

1. General testing: create test cases and test data, ensure that all testing activities conform to the requirements.

2. unit testing: the vendor will carry out the unit testing in house to make sure each component and module of the systems functions as designed.

3. integration testing: After all modules of the system are developed, integration testing is carried out to make sure that all modules function and perform as expected when working in combination

4. load testing: Since the application will be used by a large number of users in future, load testing will be performed to see how the system performs under heavy loads. This may require fine tuning the web server, application, application server, and/or the database server or network configuration and load balancing.

5. recovery testing: One of the important aspects of an application is how well it can recover in case of a system failure, server shutdown, or service failure. Tests will be carried out to see how well the system recovers from crashes and hardware failures.

6. security testing: it is necessary to perform detailed security testing of the system. This involves a complete penetration test to make sure the application and the server is not vulnerable to any type of attacks such as SQL injection attack, XSS attacks etc. This will be done by using threat detection and vulnerability scanner software

7. Usability Testing: The client will test the navigation between screens, user-friendliness and workflows of each of the screens. Against this, if deficiencies are

identified the interface may be redesigned during this testing Stage based on feedback from the Client.

8. Functional Testing: A complete end to end functional testing cycle will run. During the functional test, actual processes, and all key services provided by the system will be tested against the business requirement, (end to end) to see if the system meets the requirements as described in the RFP document and stores data and generates reports properly.

9. Acceptance Testing: An end to end functional and quality of service testing (including security, performance and robustness) will be performed by the Ministry before any system sign off.

10. UAT Test Script: An end to end user functional and quality of service testing will be performed by the Ministry prior to any system sign off.

11.   In addition to the Supplier's standard check-out and set-up tests, the Supplier (with the assistance of the Purchaser) must perform the following tests on the System and its Subsystems before Installation will be deemed to have occurred and the Purchaser will issue the Installation Certificate(s) (pursuant to GCC Clause 26 and related SCC clauses).

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

Pre-commissioning tests are crucial to confirm that all components of the system are functioning correctly before it is fully deployed. The following tests will be conducted:

- Functional Testing: Validate that all features of the system function as expected, in line with the specifications outlined in the contract.
  - System startup and shutdown procedures.
  - Test the integration of system components (hardware, software, etc.).
- Performance Testing: Test the system under expected load conditions to ensure it meets performance criteria such as speed, scalability, and reliability.
  - Verify that the system can handle the required number of concurrent users and transactions.

- ○ Assess response times for various operations under normal and peak loads.
- Security Testing: Test the security features of the system to ensure data protection and access control measures are in place.
  - ○ Conduct penetration testing to identify vulnerabilities.
  - ○ Test encryption methods and data storage security.
- Backup and Recovery Testing: Test the system's backup and disaster recovery procedures to ensure data integrity and system resilience.
  - ○ Test automatic and manual backup procedures.
  - ○ Verify data recovery processes and verify system restoration.
- Compatibility Testing: Verify the system's compatibility with existing infrastructure, including hardware, software, and network systems.
  - ○ Test integrations with other systems (e.g., databases, applications).
  - ○ Check compatibility with various operating systems and devices (if applicable).
- User Acceptance Testing (UAT): Conduct testing with end-users to verify the system meets their requirements and is user-friendly.
  - ○ Involve relevant staff in real-world testing scenarios.
  - ○ Collect feedback and address any concerns or issues raised.
- Environmental Testing: Ensure that the system can operate in the designated environment (e.g., physical conditions, network conditions).
  - ○ Verify hardware's resilience to temperature, humidity, and other environmental factors.
  - ○ Check power redundancy and uninterruptible power supply (UPS) functionality.
- Compliance Verification: Ensure the system meets legal, regulatory, and contractual requirements.
  - ○ Validate compliance with data protection laws (e.g., Data Protection Act of Kenya, GDPR).
  - ○ Verify adherence to any industry-specific standards (e.g., ISO/IEC standards).

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

4.2.1 Subsystem 1: Network Infrastructure

Tests:

- *Connectivity Test: Verify that all **network devices (routers, switches, access points)** are correctly connected.*

- *Bandwidth & Speed Test: Ensure **minimum required data transfer rates** are achieved.*

- *Security & Firewall Testing: Confirm that **firewall rules, VPN access, and intrusion detection systems** are working correctly.*

Test Conditions:

- *Network devices powered on and connected.*

- *Configured security policies applied.*

Success Criteria:

- *Stable **network connectivity** across all sites.*

- *Secure access with **no unauthorized external connections detected**.*

4.2.2 Subsystem 2: Server & Storage Systems

Tests:

- *Server Boot & Performance Test: Ensure all **servers boot correctly** and operate without errors.*

- *Database Read/Write Speed Test: Check **data retrieval and processing speeds**.*

- *Backup & Disaster Recovery Test: Validate **automated backup system and restore process**.*

Test Conditions:

- *All servers are powered on with pre-installed software.*

- *Database contains test records for read/write operations.*

Success Criteria:

- *No **unexpected crashes or slowdowns**.*

● *Data is backed up and **can be successfully restored***.

4.2.3 Subsystem 3: Security & Access Control

Tests:

● ***CCTV Surveillance System Test:** Confirm **video feeds are active and stored correctly***.

● ***Biometric/Access Card Authentication:** Verify that **authorized personnel** can access secure areas.*

● ***Incident Response & Alarm Testing:** Simulate security incidents to ensure alerts function properly.*

Test Conditions:

● *Security system fully installed and activated.*

● *Staff access credentials provided.*

Success Criteria:

● *No unauthorized access is granted.*

● *All **alerts and logging mechanisms** are operational.*

4.2.N Pre-Commissioning Tests for the Entire System

Tests:

● ***Full System Integration Test:** Ensure all subsystems **(network, storage, security, workstations)** work together seamlessly.*

● ***Load Testing:** Simulate **peak usage** to confirm **system stability under stress***.

● ***User Acceptance Testing (UAT):** Correctional officers perform **test operations** on the system to verify usability.*

Test Conditions:

● *All hardware and software are installed.*

- *Simulated real-world workloads applied.*

Success Criteria:

- *No **critical failures** during integration.*

- *System meets operational requirements and **user expectations**.*

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 following tests on the System and its Subsystems following Installation to determine whether the System and the Subsystems meet all the requirements mandated for Operational Acceptance.

4.3.1   *[specify: Subsystem 1 (as defined in the Implementation Schedule) specify: **tests, test conditions, success criteria**, etc.]*

4.3.2   *[specify: Subsystem 2 (as defined in the Implementation Schedule) specify: **tests, test conditions, success criteria**, etc.]*

4.3. N   The Entire System: Pre-commissioning Tests for the entire System are: *[specify: **tests, test conditions, success criteria**, etc.]*

Note: *The complexity of the Operational Acceptance Testing needed will vary in accordance with the nature and complexity of the System being procured. For simpler Information Systems Operational Acceptance Testing may simply consist of requiring a specified period of trouble-free System or Subsystem operation under normal operating conditions. For more complex Systems, Operational Acceptance testing will require extensive, clearly defined tests under either production or mock-production conditions.*

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Operational Acceptance Test shall validate the following:

1. The system operates without critical or major errors under normal operating conditions.
2. Core modules (e.g., case tracking, document management, task workflows, client management) function as expected in the live environment.
3. User roles and access controls are implemented and functioning.
4. The system demonstrates readiness for live use by staff in production conditions.

5. The System must operate continuously and without failure for a minimum period of **30 consecutive calendar days** under normal working conditions (hereafter referred to as the "Stability Period").

6. The CMS, LDIMS and LAD, shall be deemed to have passed the Operational Acceptance Test if the following conditions are met during the Stability Period:
    - No **Critical Errors** (e.g., system crash, data loss, total unavailability of key modules).
    - No more than **three (3) Major Errors**, and any such issues must be resolved within **48 hours** of notification.
    - All **Minor Errors** are logged and included in the Post-OAT improvement plan.

7. The OAT shall be conducted in the **live production environment** using actual user data and typical daily workloads.
    - The supplier shall provide technical support throughout the OAT period, including response to any issues identified.

8. A detailed Operational Acceptance Test (**OAT) Plan** shall be submitted by the supplier at least one week prior to commencement. At the conclusion of the testing period, the supplier shall submit an **OAT Report** outlining:
    - Test results,
    - Issues encountered,
    - Resolutions provided,
    - Confirmation of system stability and operational readiness.

9. Final acceptance of the system shall be contingent upon successful completion of the Operational Acceptance Test. Any failure to meet the criteria shall result in the extension of the OAT period or remedial action at the supplier's cost.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

4.3.1 Subsystem 1: Network Infrastructure

Tests:

- **Connectivity Verification:** Ensure all network devices (routers, switches, firewalls) are functioning properly.

- **Latency & Bandwidth Testing:** Measure network speed and responsiveness under normal and peak loads.

- **Security & Firewall Audit:** Test firewall rules, VPN connections, and access control policies.

Test Conditions:

- Network fully deployed and configured.

- Security protocols and encryption enabled.

Success Criteria:

- **Stable and secure** connectivity across all facilities.

- **No unauthorized network access detected.**

4.3.2 Subsystem 2: Server & Storage Systems

Tests:

- **Server Load & Performance Test:** Assess system stability under peak workloads.

- **Data Integrity Check:** Validate that stored data remains **accurate and retrievable**.

- **Backup & Recovery Test:** Simulate a data loss scenario and ensure successful restoration.

Test Conditions:

- Live test data stored in the system.

- Scheduled backups enabled.

Success Criteria:

- **No data corruption or loss** detected.

- Backup and **disaster recovery process functions correctly.**

4.3.3 Subsystem 3: Security & Access Control

Tests:

- **CCTV Functionality Test:** Ensure all cameras provide **clear footage** and recordings are stored securely.

- **Biometric Access & Card Authentication:** Verify that only **authorized personnel** can enter restricted areas.

- **Intrusion & Alarm System Test:** Simulate unauthorized access attempts to check alarm responsiveness.

Test Conditions:

- Security systems activated and monitoring enabled.

- Access credentials provided to personnel.

Success Criteria:

- **No unauthorized access detected.**

- Alarms and notifications triggered in case of security breaches.

4.3.N Operational Acceptance Tests for the Entire System

Tests:

- **End-to-End System Testing:** Ensure all subsystems work **seamlessly together.**

- **Stress Testing:** Simulate **high usage** conditions to test system resilience.

- **User Acceptance Testing (UAT):** Correctional officers perform **real-world tasks** using the system.

Test Conditions:

- The system is **fully deployed** and in use.

- Test cases simulate **daily operational workflows.**

Success Criteria:

- **No major failures or slowdowns.**

- The system meets all **operational and security requirements.**

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 bidding documents).

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

5.1.1.1 Warranty Defect Repair Service

Coverage Period:

- The warranty shall cover software for a minimum of 1 year from the date of Operational Acceptance.

Response Time & Problem-Resolution Performance Standards:

- Critical Issues (e.g., system failure, security breach): Response time within 2 hours, resolution within 24 hours.
- Major Issues (e.g., performance degradation, data access issues): Response time within 4 hours, resolution within 48 hours.
- Minor Issues (e.g., UI bugs, configuration changes): Response time within 8 hours, resolution within 5 business days.

Modes of Service:

- On-Site Support: For critical hardware failures, a technician will be dispatched to the Correctional Services facility.

Remote Support: Software and network-related issues will be resolved remotely via secure access.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

5.1.1.1 Warranty Defect Repair Service

The Supplier MUST provide the following services under the Contract, or as appropriate, under separate contracts as specified in the bidding documents:

1. **Timely Defect Correction**
   The Supplier shall, at no additional cost, promptly diagnose and repair or replace any component, module, software, or system found to be defective or not functioning as specified during the warranty period.

2. **On-Site and Remote Support**
   Where applicable, the Supplier must provide both on-site and remote support for defect diagnostics and resolution within the agreed service levels.

3. **Response and Resolution Times**
   The Supplier must adhere to predefined service level agreements (SLAs) including:
   - Response time: e.g., within 4 hours of receiving a defect report.
   - Resolution time: e.g., defect must be repaired or part replaced within 48 hours.

4. **System Downtime Management**
   If the defect affects critical system operations, the Supplier must provide temporary workarounds or backup systems to ensure continuity of services.

5. **Software Bug Fixes & Updates**
   The Supplier shall provide patches, updates, or bug fixes for any software supplied under the contract during the warranty period at no extra cost.

6. **Documentation of Repairs**
   All repairs, replacements, and updates must be logged and documented. Reports shall be submitted to the Purchaser on a monthly or as-needed basis.

7. **Warranty Period Coverage**
   The warranty period shall begin upon official acceptance of the delivered solution and remain valid for (12 months), unless otherwise stated in the contract.

8. **Exclusion of User-Induced Damages**

   Repairs or replacements due to misuse, unauthorized modifications, or environmental damage may be excluded, subject to mutual agreement.

9. **Escalation Procedure**

   A clearly defined escalation matrix shall be provided in cases where the Supplier fails to meet response/resolution obligations.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

5.1.1.1 Warranty Defect Repair Service

Coverage Period:

- The warranty shall cover **software** for a minimum of 1 year from the date of **Operational Acceptance.**

Response Time & Problem-Resolution Performance Standards:

- **Critical Issues (e.g., system failure, security breach):** Response time **within 2 hours**, resolution within **24 hours.**

- **Major Issues (e.g., performance degradation, data access issues):** Response time **within 4 hours**, resolution within **48 hours.**

- **Minor Issues (e.g., UI bugs, configuration changes):** Response time **within 8 hours**, resolution within **5 business days.**

Modes of Service:

- **On-Site Support:** For critical hardware failures, a technician will be dispatched to the **Correctional Services facility.**

- **Remote Support:** Software and network-related issues will be resolved **remotely via secure access.**

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 bidding documents).

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

The tenderer shall sign a service level and support agreement to ensure that the commissioned system is adequately supported and it maintains the acceptable levels of uptime. the tenderer shall also ensure the following;

1. Guarantee the support for the system for a period not less that 2 years post commissioning.

2. Provide a maintenance schedule for the system.

3. Provide a draft SLA, annual post warranty support and maintenance document.

4. Test all necessary interfaces which integrate the components of the proposed system.

5. Provide technical support for tuning and reconfigurations as requested from time to time as requested based on the signed SLA.

6. Under the proposed draft SLA, the tenderer shall provide the following;

    a) Escalation matrix.

    b) Emails and phone numbers of atleast 2 technical contact persons.

    c) proof of local presence (if applicable).

    d) online support and onsite support.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Supplier **MUST** provide the following services under the Contract, or as appropriate, under separate contracts as specified in the bidding documents:

a) Post-Implementation Support

● Provision of on-site and/or remote technical assistance for a defined period (24 months or as agreed in the SLA) following system deployment.

- Support for troubleshooting issues, bug fixes, and resolution of defects identified during operational use.
- Dedicated support contact(s) for issue escalation.

b) Helpdesk Services

- A functional helpdesk (email, phone, and ticketing system) available during standard working hours, and optionally 24/7 for critical systems.
- Defined **Service Level Agreements (SLAs)** with response and resolution timelines for various issue categories (critical, high, medium, and low).

c) System Maintenance

- Regular preventive maintenance of software and infrastructure components.
- Patch management and software updates to address security vulnerabilities, performance improvements, or compliance requirements.
- Backup and data integrity checks as per agreed schedules.

d) User Support and Guidance

- Provision of user manuals, FAQs, and troubleshooting guides.
- Ongoing support to end-users including guidance on how to use new features or functionality post-updates.

e) Training and Knowledge Transfer

- Periodic refresher training sessions for system administrators and end-users.
- On-the-job training for ICT staff to build internal capacity for support and troubleshooting.

f) Monitoring and Performance Optimization

- Tools or dashboards to monitor system health, usage statistics, and performance.

- Recommendations and support for tuning system performance and managing resource usage.

g) Incident and Problem Management

- A clear protocol for logging, classifying, tracking, and resolving incidents.
- Root cause analysis and post-resolution reports for major incidents.

h) Security Support

- Technical support for securing the system against cyber threats including intrusion detection, access control enforcement, and data protection.
- Regular updates and patches to mitigate newly discovered vulnerabilities.

i) Reporting and Documentation

- Quarterly reports summarizing support activities, issue resolution metrics, and improvement recommendations.
- Full documentation of all support cases and resolutions provided during the contract period.

j) Optional Extended Support

- Option for the Procuring Entity to procure extended technical support services beyond the initial support period, under mutually agreed terms.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

5.2.1.1 User Support / Hotline

Coverage Period:

- **24/7 Support** for critical system issues.

- **Business Hours Support** (Monday–Friday, 8 AM – 6 PM) for general inquiries and non-critical issues.

Response Time & Problem-Resolution Performance Standards:

- **Critical Issues (e.g., system downtime, security incidents):** Response time **within 1 hour**, resolution within **12 hours.**

- **Major Issues (e.g., performance lags, application errors):** Response time **within 4 hours**, resolution within **24 hours.**

- **Minor Issues (e.g., password resets, general inquiries):** Response time **within 8 hours**, resolution within **3 business days.**

Support Channels:

- **Toll-Free Hotline** for immediate assistance.

- **Email & Ticketing System** for tracking issues and resolution progress.

- **Live Chat Support** for real-time troubleshooting.

5.2.1.2 Technical Assistance

Categories of Technical Staff Required:

- **System Administrators:** Handling server and database issues.

- **Network Engineers:** Troubleshooting network and connectivity problems.

- **Software Support Specialists:** Resolving application bugs and user issues.

- **Cybersecurity Experts:** Monitoring threats and enforcing security policies.

Support Methods:

- **On-site Support** for critical infrastructure failures.

- **Remote Assistance** for software and minor technical issues.

- **Scheduled Maintenance** to prevent system failures.

5.2.1.3 Post-Warranty Maintenance Services

Coverage Period:

● Extends beyond the initial **warranty period (1 year after go-live)** to ensure continuous system operation.

Response Time & Problem-Resolution Standards:

● **Same response times as warranty period** for major issues.

● **Quarterly system check-ups** and preventive maintenance.

Modes of Service:

● **On-Site Repairs:** For hardware failures requiring physical intervention.

● **Remote Troubleshooting:** For software updates and system optimizations.

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 <u>Post-Operational Acceptance Technical Assistance Activities</u> 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 are specified in the relevant System Inventory Tables for Recurrent Cost Items.

    5.3.1.1 <u>System Analyst</u>: *[for example, specify: **education/certifications, years' experience in, demonstrated successful experience in,** etc.]*

    5.3.1.2 <u>Database Expert</u>: *[for example, specify: **education/certifications, years' experience in, demonstrated successful experience in,** etc.]*

    5.3.1.3 <u>Programming   Expert</u>:   *[for   example,   specify: **education/certifications, years' experience in, demonstrated successful experience in,** etc.].*

    5.3.1.4 …

Note: *The Technical Assistance Team specification may be used to develop bid prices for technical support Recurrent Costs. These may be included in the main Contract or be subject to separate contracts. In either regard, to obtain meaningful and comparable bid prices, the Purchaser will need to specify the roles of the technical support team members in this section and indicate the quantities of the corresponding inputs in the Systems Inventory Tables for Recurrent Cost items.*

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 bidding 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 bidders from organizing the proposed work in the most efficient and effective manner.

To facilitate the bidding 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 bids (and ease the bid 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.

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 bidding documents during the preparation and bidding 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 Bidders 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 Bidder will have to perform under the Contract, including related travel and subsistence costs.

This information will also help Bidders identify which site(s) may warrant a site visit during the period they are preparing their bids. If the System presents complex installation challenges, site layout drawings should be included in the Background and Informational Materials Section.

Table of Contents: Implementation Schedule

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.]*

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

S/No	Event /Milest one	Deliverable	Timelines from contract commence ment dates	Number and Format of reports presentation
1	Inception	1. Full detailed project plan, including work plan, methodology, and Gantt chart/project charter for the team, among other inaugural items before commencing the assignment. 2. Inception report, certificate of acceptance sign off for all the listed documents	1 month	2 hard copies and a digital copy

2	System Technical design	1. Functional requirements document (FRD) and design document 2. System design document (SDD) 3. Documents mapping all tasks and come up with a task flow chart for each module Evidence: Certificate of acceptance and sign-off for user requirements and task flow chart	1 month	2 hard copies and a digital copy
3	Software installation and testing (each module)	1. System installation, implementation, unit testing, and integrated end-to-end system testing on all modules. 2. Tests report for all modules. 3. UAT plan and User Acceptance Testing 4. System vulnerability Assessment and penetration testing (VAPT) Certificate of Acceptance sign-off for full installation, end to end functionality testing report, Approved UAT report. Vulnerability Assessment and Penetration Testing VAPT report.	6.5 months	2 hard copies and a digital copy

4.	Data Migration and Integration with other systems	1. Integration of the system to all the required systems. Should include documentation on integration criteria and API set ups. 2. Migration of existing data to the new system.	1.5 months	
5.	Training of Relevant staff and commissioning of the system	1. Approved training plan. 2. Training ODPC's technical staff, administrators and users on the use of the various modules 3. Provision of training manuals, and operational manuals for the system configuration 4. Training reports and documents. 5. System go live.	2 months	2 hard copies and a digital copy
6.	System Maintenance and support. Post go live	1. Provision of a support matrix. 2. Provision of a licensing structure. 3. Quarterly reports on the system stability and support issues	12 months	

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

S/No	Event / Milestone	Deliverable	Timelines from Contract Commencement (Months)	Number and Format of Reports/Presentation
1	Inception Phase	Inception Report including finalized project plan, team structure, and stakeholder engagement plan	Month 1	2 printed copies + 1 soft copy (PDF + editable format)
2	Requirements Gathering & Analysis (All Systems)	System Requirements Specifications (SRS) for CMS, LDIMS, and LOD	Month 2	2 printed copies per system + soft copies (PDF + Word)
3	System Architecture & Design (All Systems)	Architecture Diagrams, Wireframes, and Technical Design Documents	Month 3	2 printed copies + soft copy (PDF + editable) per system
4	Development of Case Management System (CMS)	Completed CMS prototype with core modules	Months 4–6	Biweekly progress reports (email) + Monthly status report (PDF)
5	User Acceptance Testing (UAT) for CMS	UAT Plan, Test Scripts, and UAT Report signed by end-users	Month 7	1 UAT report (PDF), 1 signed approval document
6	Deployment & Training for CMS	Live CMS system + Training manuals + Staff trained	Month 8	Training Report + Attendance Sheets + Training Materials (PDF)

7	Development of Legislative Drafting Information Mgmt System (LDIMS)	Completed LDIMS prototype with core modules	Months 6–8	Biweekly updates + Monthly summary report
8	UAT for LDIMS	UAT Plan, Test Scripts, and UAT Report signed by users	Month 9	1 UAT report (PDF), 1 signed approval document
9	Deployment & Training for LDIMS	Live LDIMS system + Staff training and materials	Month 10	Training Report + Attendance Sheets + Materials (PDF)
10	Development of Legal Opinion Database (LOD)	Completed Legal Advisory/Opinion System with search, tagging, and metadata classification	Months 9–10	Biweekly updates + Monthly summary report
11	UAT for LOD	UAT Plan, Test Scripts, and UAT Report signed by users	Month 11	1 UAT report (PDF), 1 signed approval document
12	Deployment & Training for LOD	Live Legal Opinion System + Staff training and materials	Month 12	Training Report + Attendance Sheets + Training Materials (PDF)
13	Final System Integration, Go-Live, and Operational Acceptance Testing (All Systems)	Signed Operational Acceptance Test Reports for CMS, LDIMS, LOD	End of Month 12	3 OAT Reports + Go-Live Certificate per system
14	System Support & Maintenance	Ongoing technical support, issue resolution, minor enhancements	Months 13–24	Quarterly system health reports + Support logs + Incident tracking

15	Project Closeout	Final Report including Lessons Learned, User Feedback, and Handover Docs	End of Month 24	Final project report (3 printed + soft copy PDF)

Lot 3: Correctional Services Management Information System for State Department for Correctional Services

5.5 PROJECT MILESTONES

Milestones for the Integrated Correctional Management Information System (ICMIS)

No.	Milestone	Activity	Duration from Contract Commencement date (Months)	Deliverables
1	Project Initiation	· Kick-off meeting with stakeholders · Submission and approval of the Project Inception Report ● Establish and operationalize Project management office	1	· Project Charter and Initiation report · Sign-off / Acceptance certificate · Operational Project management office

2	System Design Completion	• Develop and approve the System Design Document • Conduct design review sessions with stakeholders .	3	· Approved system design · User acceptance report and certificate
3	System Development	• Complete development of core modules • Conduct internal testing and iterations • Establish a secure correctional database • Encryption	5	· A working ICMIS and a secure database · User acceptance report and certificate
4	User Access Control and Security Implementation	• Implement user authentication mechanisms • Conduct security audits	6	
5	System Integration	• Integrate with other systems • Test data flows and system interoperability	7	· APIs · Sign-off / Acceptance certificate

6	User Acceptance Testing (UAT)	• Conduct UAT sessions with stakeholders Document feedback and implement necessary adjustments	8	· Final approved UAT document · Sign-off / Acceptance certificate
7	Training, Change management and Capacity Building	• Conduct training sessions for administrators and end-users • Provide user manuals and video tutorials • Conduct change management	9	· Training reports and attendance registers · Hard copy user manuals and video tutorials · Sign-off / Acceptance certificate
8	Deployment and Rollout	• Execute rollout across all correctional facilities and probation offices • Monitor and address any deployment issues	10	· Consolidated Report · Sign-off / Acceptance certificate
9	Post-Implementation Support and Monitoring	• Provide ongoing technical support • Monitor system performance and usage	11	· Monitoring and Evaluation Report

| 10 | Final Project Closure | ● Submit the Final Project Report

● Conduct project closure meeting

● Document lessons learned and recommendations for future improvements | 12 | · Certificate of completion |

| | | ● Submit periodic compliance and audit reports | | |

(Note: the "Submit periodic compliance and audit reports" row appears above row 10 in the image.)

Price schedule

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

S/ No	Event /Milestone	Duration	Percentage
1.	Approved Inception report	1 month	10%

2.	System Technical design documentation.	1 month	
3.	Software installation, testing and Integration with other systems, and certificate of acceptance sign off (each module).	6.5 months	40%
4.	Data Migration and Integration with other systems	1.5 months	
5.	Training of Relevant staff and commissioning of the system.	2 months	30%
6.	System Maintenance and support. Post Go live.	12 months	20%

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (Bidder to specify in the Preliminary Project Plan)	Installation (weeks from Effective Date)
0	Project Plan	- -	- -		- -
1	Subsystem 1	1	___		- -
:	etc.				
x	Operational Acceptance of the System as an integrated whole	- -	all sites		- -
y	Recurrent Cost Items – Warranty Period	y	- -		

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

No.	Milestone	Duration (Months)	Percentage of Contract Amount
1.	Project Initiation & Design Phase	0–3 months	25%
2.	Development and Implementation Phase	4–9 months	40%
3.	System Deployment & Operational Acceptance	10–12 months	25%
4.	Post-Deployment Support Period	13–15 months	10%

Lot 3: Correctional Services Management Information System for State Department for Correctional Services

PAYMENT SCHEDULE

The proposed payment schedule based on satisfactory performance

No.	Milestone	Duration (Months)	Percentage Of The Contract Amount
1.	Project Initiation, project plan and Inception report	1	20%
2.	System Design Completion	3	
3.	System Development	5	30%
4.	User Access Control and Security Implementation	6	
5.	System Integration	7	
6.	User Acceptance Testing (UAT)	8	20%
7.	Deployment and Rollout	9	
8.	Training, Change management and Capacity Building	10	
9.	Post-Implementation Support and Monitoring	11	30%

10.	Final Project Closure	12	

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.

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)
	Headquarters			
R1	Region 1			
R1.1	Region 1 Head Office			
R1.2	ABC Branch Office			

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

Site Code	Site	City / Town / Region	Primary Street Address	Drawing Reference No. (if any)
ODPC	Headquarters	Nairobi	Hospital road, Upper Hill, Britam Towers, 12th Floor.	NA

R1	Region 1			
R1.1	Region 1 Head Office			
R1.2	ABC Branch Office			
R1.3	DEF Branch Office			

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

Site Code	Site	City / Town / Region	Primary Street Address	Drawing Reference No. (if any)
OAG&D OJ	Headquarters	Nairobi	Sheria House, Harambee Avenue, Nairobi	NA

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).**]*

Month	20xy	20xy+1	20xy+2	....			
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

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). The second version of the table permits the Purchaser to obtain price information about items that are needed during the Warranty Period.

Table of Contents: System Inventory Tables

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.

SYSTEM INVENTORY TABLE (RECURRENT COST ITEMS) *[INSERT: IDENTIFYING NUMBER]* –

Line item number: *[specify: **relevant line item number from the Implementation Schedule (e.g., y.1)**]*

Component No.	Component	Relevant Technical Specifications No.	Y1	Y2	Y3
1.	Warranty Defect Repair		all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price
2.	Software/Firmware Licenses and Updates:		all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price	all items, all sites, included in the Supply and Install Price
3.	Technical Services				
3.1	Sr. Systems Analyst		80 days	40 days	20 days
3.2	Sr. Programmer		20 days	40 days	60 days
3.3	Sr. Network Specialist, …. etc.		- -	20 days	20 days
	…				

Note: - - indicates not applicable. " indicates repetition of table entry above.

Background and Informational Materials

Notes on Background and Informational Materials

This section of the bidding document provides a place to gather materials that the Purchaser believes will help Bidders prepare more precisely targeted technical bids and more precise bid prices.

These materials MUST NOT introduce requirements for the Information System. Rather they should assist Bidders to interpret the Technical Requirements and the General and Specific Conditions of Contract. For example, these Background and Informational Materials may describe existing information systems that the Information System to be supplied and installed under the Contract must integrate with. However, the specific requirement that the Supplier must integrate the Information System with other systems needs to be stated in the Technical Requirements. Similarly, these Background and Informational Materials may describe the legal and regulatory norms (including for example statutory report formats) that are relevant to the Information System. The Technical Requirements Section would need to spell out that the Supplier must ensure the Information System complies with the relevant legal and regulatory norms.

Table of Contents: Background and Informational Materials

Background and Informational Materials

Note: *The following is only a sample outline. Entries should be modified, extended, and/or deleted, as appropriate for the particular System to be supplied and installed. DO NOT introduce requirements for the System in this section.*

A. BACKGROUND

0.1   The Purchaser

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

The Office of the Data Protection Commissioner (ODPC) is established under the Data Protection Act, 2019(The Act). The Mandate of the Office mandate is to regulate the processing of personal data; ensure that the processing of personal data is guided by the principles set out in Section 25 of The Act; protect privacy of individuals; establish the legal and institutional mechanisms to protect personal data , and provide data subjects with rights and remedies to protect processing of their personal data from processing that is not in accordance with the Act.

Lot 2: Case Management System, Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

The Office of the Attorney Generaland Deprtment of Justice (OAG&DOJ) of Kenya is a constitutional office established under the **Constitution of Kenya, 2010**, specifically in **Article 156**. The Attorney General serves as the principal legal advisor to the government of Kenya, representing the state in legal matters and providing legal opinions to government institutions. The OAG&DOJ is tasked with overseeing public prosecutions and offering legal advice to the President, Cabinet, and other state organs. Additionally, the OAG plays a key role in formulating and reviewing legislative frameworks, ensuring legal compliance, and supporting the justice system. The office operates under the **Office of the Attorney General Act, 2012**, which provides further structure and mandates for the office's operations and functions.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

1.1 Background

The State Department for Correctional Services is domiciled in the Ministry of Interior and National Administration. It comprises two technical Services: Kenya Prisons

Service (KPS) and Probation and Aftercare Service (PACS). Its mandate is to promote a just and secure society through efficient and effective management of offenders and administration of justice.

The Kenya Prisons Service (KPS) and the Probation and Aftercare Service (PAS) are seeking to modernize their operations through the implementation of an Integrated Correctional Management System (ICMS). This system will serve as a centralized platform for managing inmate records, probation cases, staff administration, financial operations, and reporting. To ensure the confidentiality, availability, and reliability of sensitive data, the ICMS will incorporate encryption technologies aligned with international standards and best practices.

The State Department currently provides correctional services to over 120,000 offenders in custodial and non-custodial sentences. Kenya Prisons Service has 136 prisons spread across the country, 8 regional offices, 1 staff college and 1 prison headquarters which offer safe and humane containment to 64,000 inmates with a staff capacity of 35,000.

Similarly, Probation and Aftercare Service has 47 county probation offices, 8 Regional offices, 9 Probation Institutions and 148 stations spread across the country which offers non-custodial offender management to over 63,000 offenders with a staff capacity of 1,670.

The State Department for Correctional Services is committed to improving the efficiency and effectiveness of the country's correctional services by transforming the Kenya Prisons Services (KPS) and Probation and After Care Services (PACS) to modern correctional facilities. To this end, The State Department for Correctional Services seeks to implement an Integrated Correctional Management Information System (ICMIS) which entails the Inmates Management System for Kenya Prisons Services (KPS) and the Case Management System for the Probation and Aftercare Service to enhance offender management, streamline operations, and ensure compliance with legal and regulatory standards.

0.2 The Purchaser's Business Objectives for the Information System

Lot 1: Data Management Information System for Office of the Data Protection Commissioner.

In the wake of rapid digital transformation initiatives and technological changes, the office has automated its processes in order to provide critical data protection services to its clients. As part of the office capacity development through digitization, ODPC has invested on optimal

and secure Information and Communication Technologies (ICT) infrastructure that includes Servers, data centers, Fiber Connectivity, Storage & Network equipment as well as adequate end user computing equipment.

Currently, the registration portal is a module within the internal IDMIS system that has limited capacity and inadequate support to expand its capability to match client demands and effective delivery of the office mandate.

In addition, the complaints management processes and reporting of data breaches is currently a hybrid of online and manual processes and therefore there is a need for end to end automation of the processes

In line with the e-Government Strategy, Government Systems & Applications Standard (ICTA.6.003:2023), ODPC strategic plan 2022/23 to 2024/25, ODPC's ICT policy, the Office is required to implement platforms that are seamless and efficient in provision of services to the clients and the general public in adherence to the service charter and the act.

It is on this basis that ODPC seeks to acquire an end-to-end, robust, secure, and a seamless Integrated Data Management Information System (IDMIS).

Lot 2: Case Management System,Legislative Drafting Information Management System & Legal Opinion System for the Office of the Attorney General

1. **Automate and Streamline Case Management (CMS)**: Enable efficient tracking and management of legal cases, ensuring timely updates, tracking of deadlines, and reducing manual case handling. The CMS will improve productivity, reduce case backlogs, and ensure real-time case status visibility.

2. **Enhance Legislative Drafting and Collaboration (LDIMS)**: Facilitate efficient drafting, reviewing, and collaboration on legislative documents by providing a centralized platform for document storage, version control, and workflow management. The LDIMS will support the seamless integration of inputs from various stakeholders, ensuring efficient lawmaking processes.

3. **Centralize Legal Opinions and Advisory Services (Legal Advisory Database)**: Establish a comprehensive and searchable database for legal opinions, advisory notes, and precedents, ensuring easy access to critical legal information, improving consistency in legal advice, and enhancing the quality of legal services provided to government bodies and institutions. **Improve Data Access, Security, and Compliance**: Implement a secure, scalable platform that ensures the confidentiality, integrity, and availability of sensitive legal data. The system will comply with Kenyan data protection laws and best practices for information security, enabling authorized users to access critical data while protecting sensitive information.

4. **Enhance Reporting and Analytics**: Provide advanced reporting and analytical capabilities to support informed decision-making within the OAG&DOJ. The system will enable the generation of detailed reports on case progress, legislative drafts, legal advisory outcomes, and key performance metrics, improving oversight and performance monitoring.

5. **Foster Collaboration and Communication**: Improve communication and collaboration among OAG&DOJ staff, external counsel, and stakeholders by providing an integrated platform for real-time information sharing, document exchange, and task management.

6. **Ensure Operational Efficiency and Cost Reduction**: Reduce operational costs by eliminating manual processes, reducing paper-based workflows, and improving resource allocation. The system will enhance efficiency in legal case management, legislative drafting, and the provision of legal advice.

7. **Scalable, Flexible, and Sustainable Solution**: Provide a robust, flexible system that can scale with the OAG&DOJ's future needs, adapt to changing legal processes, and support ongoing digital transformation in the legal sector.

Lot 3: Correctional Services Management Information System for State Department for Correctional Services.

4.0 OBJECTIVE / BENEFITS

4.1 General Objective

The overall objective is aimed at the acquisition and implementation of an Integrated Correctional Management Information System (ICMIS) which entails the Inmates Management system for Kenya Prisons Services (KPS) and the Case Management system for the Probation and Aftercare Service and knowledge transfer to staff during and after digitalization.

4.2 Specific Objectives

1. To provide an automated centralized database to manage offender's data securely.
2. To efficiently control and manage the offender's affairs, which helps in instant planning and decision-making for the department and other stakeholders.
3. Regulate court production and manage daily activities for custodial and non-custodial offenders.
4. Prompt information flow and quick decision-making reliable mechanism for data protection and backup.
5. To ensure capacity building and technological innovation for both officers using the system and the technical team to provide support to the system.
6. Data Security: To ensure the confidentiality, integrity, and availability of data through the deployment of encryption technologies for data at rest, in transit, and in use.
7. Supply all necessary hardware and software components for the ICMIS, including servers, storage devices, and encryption tools.
8. Install and configure the ICMIS and encryption system in accordance with the design specifications.
9. Compliance: To align the ICMIS with international standards and best practices in data security, encryption, and information management

B. INFORMATIONAL MATERIALS

0.3   The Legal, Regulatory, and Normative Context for the Information System

0.3.1   *[provide: an overview of the laws, regulations and other formal norm which will shape the Information System.]*

0.3.2   *[provide: samples of existing standardized reports, data entry forms, data formats, data coding schemes, etc. which the Information System will need to implement.]*

0.4   Existing Information Systems / Information Technologies Relevant to the Information System

0.4.1   *[provide: an overview of the existing information systems and information technologies which will establish the technological context for the implementation of the Information System.]*

0.4.2   *[provide: an overview of the ongoing or planned information systems initiatives that will shape context for the implementation of   the Information System.]*

0.5   Available Training Facilities to Support the Implementation of the Information System.

0.5.1   *[provide: an overview of the Purchaser's existing training facilities that would be available to support the implementation of the Information System.]*

0.6   Site Drawings and Site Survey Information Relevant to the Information System

0.6.1   *[provide: information of the sites at which the Information System would be implemented.]*

PART 3 – CONDITIONS OF CONTRACT AND CONTRACT FORMS

SECTION VIII - GENERAL CONDITIONS OF CONTRACT

Table of Clauses

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 bidding 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 bidding documents.

(vii) **"Implementation Schedule"** means the Implementation Schedule in Section VII of the bidding documents.

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

(ix) **"Procurement Regulations"** refers to the edition **specified in the SCC** of the World Bank "Procurement Regulations for IPF Borrowers".

(x) **"bidding documents"** refers to the collection of documents issued by the Purchaser to instruct and inform potential suppliers of the processes for bidding, selection of the winning bid, and Contract formation, as well as the contractual conditions governing the relationship between the Purchaser and the Supplier. The General and Special Conditions of Contract, the Technical Requirements, and all other documents included in the bidding documents reflect the Procurement Regulations that the Purchaser is obligated to follow during procurement and administration of this Contract.

(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, Subcontractors' 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 bid to **perform** the **Contract** has 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 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 bid. 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.

(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 (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 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 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 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 these bidding documents (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.

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 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 Electronic Data Interchange (EDI), with the following provisions.

4.1.1 Any notice sent by facsimile, electronic mail, or EDI shall be confirmed within two (2) days after dispatch 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.

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 bidding 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 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 bid, 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).

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

(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 bid 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

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 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.

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:

(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

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

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

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.

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.

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 bidding documents 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 bidding documents, 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 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 bid 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 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 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 bid), 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 bid 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 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.

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.

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.

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 therefore, 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 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.

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 bid, 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.

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; 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 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 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.

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 bid 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 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 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 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 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 bid 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 bid.

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 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 Bid) 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.

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 bidding documents, 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 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 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 bid, 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

(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:

(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 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 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, 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.

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 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

(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.

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 Bid; 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 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 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 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 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 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

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.

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 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.

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 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 bidding documents.

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.

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 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 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.

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

(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 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;

(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

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

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,

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

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.l   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

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

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.

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.

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;[10] (ii) to be a nominated[11] 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[12] 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.

---

[10]   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.

[11]   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.

[12]   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.

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 _____, _____

SECTION IX - SPECIAL CONDITIONS OF CONTRACT

Table of Clauses

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: **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 is: *[insert: **name and/or the official title of Project Manager**]*. GCC
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 **12 months** starting with the completion of the Warranty Period.

Notices (GCC Clause 4)

GCC 4.3	Address of the Project Manager: *[as appropriate, insert: **personal delivery, postal, facsimile, email, and/or EDI addresses.**]*
	Fallback address of the Purchaser: *[as appropriate, insert: **personal delivery, postal, facsimile, email, and/or EDI addresses.**]*
	[Note: If the Purchaser wishes to use Electronic Data Interchange (EDI) to communicate with the Supplier, it should specify the standards and protocols (for example ANSI X12 or ISO EDIFACT). The details may then be revised at Contract finalization. If so, add the following text.]
	For Electronic Data Interchange (EDI) the Purchaser and Supplier will use the following standards, protocols, addresses, and procedures: *[insert: **standards, protocols, addresses;** also describe: **any relevant procedures**]*

B. SUBJECT MATTER OF CONTRACT

Scope of the System (GCC Clause 7)

GCC 7.3	The Supplier's obligations under the Contract will include the following recurrent cost items, as identified in the Recurrent Cost tables in the Supplier's Bid:
	*[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 Bid. 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 Bid**, 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.]

Time for Commencement and Operational Acceptance (GCC Clause 8)

GCC 8.1	The Supplier shall commence work on the System within: **21** days from the Effective Date of the Contract.

Supplier's Responsibilities (GCC Clause 9)

GCC 9.1	[*State:* "health and safety manual is/is not required*" and delete the option that is not applicable.*]
GCC 9.8	The following sustainable procurement contractual provisions apply: **None**
GCC 9.18	The Supplier **not 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.

[Note: The advance payment may be higher than 10% in cases where Supplier's mobilization costs (i.e., costs between Contract effectiveness and the first scheduled Contract payment) are likely to be much larger than the advance payment, resulting in substantial negative cash flow for the Supplier. This happens primarily in projects where the Supplier must acquire expensive highly-specialized equipment to customize and configure a solution system prior to the first scheduled payment milestone. In these cases, the entire schedule of payments below obviously needs to be adjusted accordingly.]*

(b)   Information Technologies, Materials, and other Goods, with the exception of Custom Software and Custom Materials:

sixty percent (60%) of the total or pro-rata Contract Price for this category against Delivery

ten percent (10%) of the same price against Installation

ten percent (10%) of the same price against Operational Acceptance.

(c)   Custom Software and Custom Materials:

sixty percent (60%) of the total or pro-rata Contract Price for this category against Installation

twenty percent (20%) of the same price against Operational Acceptance.

[Note: Large custom software development or system integration contracts (e.g., those taking longer than six months from Contract Effectiveness to Operational Acceptance of the Application Software subsystem) are usually paid in increments against Purchaser's acceptance of major intermediate deliverables defined in the implementation schedule as key milestones (e.g. a sequence of major system design documents, such as: software requirements specifications, software design document, development of a prototype for a major subsystem, delivery of a pilot implementation of the software for a subsystem or the entire system, etc). In those cases, the above payment terms should be modified accordingly and refer to the milestones in the Implementation Schedule. The payment terms should allow the Supplier an adequate cash flow vis-à-vis the steps need to achieve an operational Information System.]*

(d)   Services other than Training:

eighty percent (80%) of the pro-rata Contract Price for services performed will be paid monthly in arrears, on submission and Purchaser's approval of invoices:

[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) Training
	thirty percent (30%) of the total Contract Price for training services at the start of the full training program
	fifty percent (50%) of the pro-rata Contract Price for training services performed will be paid monthly in arrears, on submission and approval of appropriate invoices.
	(f) Complete System Integration
	ten percent (10%) of the entire Contract Price, exclusive of all Recurrent Costs, as final payment against Operational Acceptance of the System as an integrated whole.
	(g) Recurrent Costs
	one hundred percent (100%) of the price of the services actually delivered will be paid quarterly in arrears, on submission and Purchaser's approval of invoices.
	[Note: If a separate Operational Acceptance for the System as an integrated whole is not required, increase by 10% points the final payment percentages of all other goods and services above.]
GCC 12.3	The Purchaser shall pay to the Supplier interest on the delayed payments at a rate of: **2%** per annum.
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**

Securities (GCC Clause 13)

GCC 13.3.1	The Performance Security shall be denominated in **Kenya Shillings** for an amount equal to **8** percent of the Contract Price, excluding any Recurrent Costs.
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* *[Note: Special software escrow arrangements are generally needed in relation to Contracts for the supply of Software, particularly Application Software, where there is concern about the ability of the Supplier to provide ongoing support throughout the life of the System. The protection provided by an escrow arrangement, however, should be weighed against the costs of administering it. The actual language of the escrow contract will vary depending on the laws of the country in which the escrow deposit is to be made (which may be the Purchaser's Country or another country with a suitable legal regime) and the escrow agent selected (escrow agents generally have their own standard form contracts). Provisions may cover:* *(i) the Supplier's obligations to deliver the Source Code to the escrow agent and make replacement deposits to ensure that the Source Code is up to date;* *(ii) the Supplier's warranties that the Source Code is at all times capable of being used to generate the latest version of the executable code to the relevant Software in use by the Purchaser and suitable to enable the Purchaser to support and develop the Software;*

	(iii) the escrow agent's obligations to keep the Source Code secure and confidential;
	(iv) the escrow agent's obligations in relation to verification of the Source Code (to ensure that it is Source Code and that it is capable of generating the executable code);
	(v) the obligations of the Supplier and the Purchaser in relation to payment of the escrow agent's fee;
	(vi) the escrow agent's right and obligation to release the Source Code to the Purchaser in certain specified "release events" (e.g., bankruptcy or insolvency of the Supplier or the Supplier's failure to make deposits or to support the Software);
	(vii) limitations and exclusions of the escrow agent's liability;
	(viii) the circumstances in which the escrow arrangement will terminate, and what will happen to the deposited Source Code on termination; and
	(ix) confidentiality undertakings to be given by the Purchaser on release of the Source Code.]*

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)***
	[Note: In the interest of soliciting lower Bid prices, Purchasers may wish to consider defining limitations in the use of the software. For example:
	(a) restrictions on the number of records in particular categories that may be held by the System;
	(b) restrictions on the numbers of transactions in particular categories that may be processed by the System in any day, week, month, or other specified period;
	(c) restrictions on the number of persons who may be authorized to use the System at any time;
	(d) restrictions on the number of persons who may access the System simultaneously at any time; or
	(e) restrictions on the number of workstations that may be connected to the System at any time.]*
	*[**Note**: From the point of view of the Purchaser, if restrictions of any of these kinds (or any similar kind) are to be imposed and there is a real likelihood that the limits may be reached, it would be better to specify*

	additional license fees that are payable when the limits are reached rather than imposing an absolute prohibition on exceeding the limits.]
GCC 16.1 (b) (vi)	***There are no Special Conditions of Contract applicable to GCC Clause 16.1 (b) (vi)*** *[**Note**: The Purchaser may also wish to specify, for example, that such entities shall be not direct competitors of the Supplier.]*
GCC 16.1 (b) (vii)	***There are no Special Conditions of Contract applicable to GCC Clause 16.1 (b) (vii)*** *[**Note**: The Purchaser may, for example, wish to specify the members of the Purchaser's business group that are not direct competitors of the Supplier and that the Purchaser must obtain and provide the Supplier written evidence from such parties that such parties will abide by the terms of the Contract as if they were party to the Contract.]*
GCC 16.2	***There are no Special Conditions of Contract applicable to GCC Clause 16.2*** *[**Note**: If on-site audits are acceptable, the Purchaser may specify conditions on the duration and number of audits per year; the hours or days during which audits may be conducted; the categories of software subject to audit; the procedures for access to Purchaser's hardware or software; the number and affiliation of individual auditors; the timing and terms of advance notice; the indemnity by Supplier for losses, liabilities, and costs incurred by the Purchaser as a direct result of the audit; etc].*

Confidential Information (GCC Clause 17)

GCC 17.1	**There are no Special Conditions of Contract applicable to GCC Clause 17.1** *[**Note**: The Purchaser may wish to give members of its business group or related agencies, for example, access to certain specific types of technical and / or financial information it obtains or develops with respect to the Supplier and its Information Technologies. The SCC covering such an exemption should define the individuals covered and generally provide that the Purchaser will ensure that such parties are aware of and will abide by the Purchaser's obligations under GCC Clause 17 as if such party were a party to the Contract in place of the Purchaser.* *if necessary and appropriate, specify: **persons, topics, and conditions for which the confidentiality clause does not apply.]***

E. SUPPLY, INSTALLATION, TESTING, COMMISSIONING, AND ACCEPTANCE OF THE SYSTEM

Representatives (GCC Clause 18)

GCC 18.1	***There are no Special Conditions of Contract applicable to GCC Clause 18*** *[**Note:** If appropriate specify additional powers or limitations.]* The Purchaser's Project Manager shall have the following additional powers and / or limitations to his or her authority to represent the Purchaser in matters relating to the Contract *[state **necessary and appropriate clauses**].*
GCC 18.2.2	***There are no Special Conditions of Contract applicable to GCC Clause 18.2.2*** *[**Note:** If appropriate specify additional powers or limitations.]* The Supplier's Representative shall have the following additional powers and / or limitations to his or her authority to represent the Supplier in matters relating to the Contract *[state **necessary and appropriate clauses**].* *[**Note:** Any additional powers or limitations of the Supplier's Representative will, of necessity, be subject to discussions at Contract finalization and the SCC amended accordingly.]*

Project Plan (GCC Clause 19)

GCC 19.1	Chapters in the Project Plan shall address the following subject**:** (a) **Project Organization and Management Sub-Plan, including management authorities, responsibilities, and contacts, as well as task, time and resource-bound schedules (in GANTT format);** (b) **Implementation Sub-Plan;** (c) **Training Sub-Plan;** (d) **Testing and Quality Assurance Sub-Plan;** (e) **Warranty Defect Repair and Technical Support Service Sub-Plan**

	Further details regarding the required contents of each of the above chapters are contained in the Technical Requirements, *[insert: cross references]*.
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**

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 Bidder at the time of bid 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*

<table>
<tr>
<td></td>
<td>new versions might be more cost-effective. For 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."]</td>
</tr>
</table>

Inspections and Tests (GCC Clause 25)

<table>
<tr>
<td>GCC 25</td>
<td>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.]</td>
</tr>
</table>

Commissioning and Operational Acceptance (GCC Clause 27)

<table>
<tr>
<td>GCC 27.2.1</td>
<td>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</td>
</tr>
</table>

	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	***There are no Special Conditions of Contract applicable to GCC Clause 28.2.***
	*[**Note:** Typical percentages are, respectively, one half of one percent (0.5%) per week and ten percent (10%) of the total. In some instances, the Purchaser may wish to consider specifying liquidated damages on a daily basis. If so, specify this in the SCC].*
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 Bidders. This most likely will lead to higher bid 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 Bidder's perceptions of financial risk and help lower bid 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.*
	*[**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 bid 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.]*

G. RISK DISTRIBUTION

Insurances (GCC Clause 37)

GCC 37.1 (c)	The Supplier shall obtain Third-Party Liability Insurance in the amount of *[insert: **monetary value]** with deductible limits of no more than *[insert: **monetary value]**. The insured Parties shall be *[list **insured parties**]*. The Insurance shall cover the period from *[insert: **beginning date, relative to the Effective Date of the Contract**]* until *[insert: **expiration date, relative to the Effective Date of the Contract or its completion**]*.
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 Employer'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].]*

H. CHANGE IN CONTRACT ELEMENTS

Changes to the System (GCC Clause 39)

GCC 39.4	**Value Engineering** The Purchaser **will not** consider a Value Engineering Proposal. When the Purchaser will consider a Value Engineering Proposal and if the value engineering proposal is approved by the Purchaser the amount to be paid to the Supplier shall be *[insert **appropriate percentage**, up to 50%]* percent of the reduction in the Contract Price.

I. SETTLEMENT OF DISPUTES

Settlement of Disputes (GCC Clause 43)

GCC 43.1.4	The Appointing Authority for the Adjudicator is: **Not Applicable**
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.

SECTION X - CONTRACT FORMS

Notes to the Purchaser on preparing the Contract Forms

Performance Security: Pursuant to GCC Clause 13.3, the successful Bidder 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 Bidder 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 bidding document to potential Bidders.

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 bidding 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 bidding document.

Notes to Bidders on working with the Sample Contractual Forms

The following forms are to be completed and submitted by the successful Bidder 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 Bidder's Bid Price Schedules are attached to the Agreement. These contain corrections and adjustments to the Supplier's bid prices to correct errors, adjust the Contract Price to reflect – if applicable - any extensions to bid validity beyond the last day of original bid validity plus 56 days, etc.

- • Performance Security: Pursuant to GCC Clause 13.3, the successful Bidder is required to provide the Performance Security in the form contained in this

section of these bidding documents and in the amount specified in accordance with the SCC.

• Advance Payment Security: Pursuant to GCC Clause 13.2, the successful Bidder 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 these bidding documents or another form acceptable to the Purchaser. If a Bidder 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 bid 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 bidding documents for the information of Bidders.

Table of Contract Forms

NOTIFICATION OF INTENTION TO AWARD

[This Notification of Intention to Award shall be sent to each Bidder that submitted a Bid.]

[Send this Notification to the Bidder's Authorized Representative named in the Bidder Information Form]

For the attention of Bidder'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 addres***s*]*

[IMPORTANT: insert the date that this Notification is transmitted to all participating Bidders. The Notification must be sent to all Bidders 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 RFB is issued**]*

Loan No. /Credit No. / Grant No.: *[insert **reference number for loan/credit/grant**]*

RFB No: *[insert RFB **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 Bid, and/or

    b) submit a Procurement-related Complaint in relation to the decision to award the contract.

1. The successful Bidder

Name:	[*insert name of successful Bidder*]
Address:	[*insert address of the successful Bidder*]
Contract price:	[*insert contract price of the successful Bidder*]
Total combined score:	[*insert the total combined score of the successful Bidder*]

2. Other Bidders *[INSTRUCTIONS: insert names of all Bidders that submitted a Bid. If the Bid's price was evaluated include the evaluated price as well as the Bid price as read out.]*

Name of Bidder	Technical Score (If applicable)	Bid price	Evaluated Bid Cost	Combined Score (if applicable)
[*insert name*]	[*insert Technical score*]	[*insert Bid price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Bid price*]	[*insert evaluated cost*]	[*insert combined score*]
[*insert name*]	[*insert Technical score*]	[*insert Bid price*]	[*insert evaluated cost*]	[*insert combined score*]

3. Reason/s why your Bid was unsuccessful *[Delete if the combined score already reveals the reason]*

[INSTRUCTIONS; State the reason/s why <u>this</u> Bidder's Bid was unsuccessful. Do NOT include: (a) a point by point comparison with another Bidder's Bid or (b) information that is marked confidential by the Bidder in its Bid.]

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 Bid. 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 Bidder, contact details; and address the request for debriefing as follows:

Attention: [*insert full name of person, if applicable*]

Title/position: [*insert title/position*]

Agency: [*insert name of 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 Bidder, 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.

In summary, there are four essential requirements:

1.   You must be an 'interested party'. In this case, that means a Bidder who submitted a Bid 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]***

BENEFICIAL OWNERSHIP DISCLOSURE FORM

INSTRUCTIONS TO BIDDERS: DELETE THIS BOX ONCE YOU HAVE COMPLETED THE FORM

This Beneficial Ownership Disclosure Form ("Form") is to be completed by the successful Bidder. In case of joint venture, the Bidder 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 Bidder is any natural person who ultimately owns or controls the Bidder 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 Bidder*

RFB No.: *[insert number of RFB process]*
Request for Bid 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 Bidder (Yes / No)

[include full name (last, middle, first), nationality, country of residence]			

OR

(ii) *We declare that there is no Beneficial Owner meeting one or more of the following conditions:*

- directly or indirectly holding 25% or more of the shares
- directly or indirectly holding 25% or more of the voting rights
- directly or indirectly having the right to appoint a majority of the board of directors or equivalent governing body of the Bidder

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 Bidder 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 Bidder]"

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

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

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

Signature of the person named above: _____

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

---

* In the case of the Bid submitted by a Joint Venture specify the name of the Joint Venture as Bidder. In the event that the Bidder is a joint venture, each reference to "Bidder" in the Beneficial Ownership Disclosure Form (including this Introduction thereto) shall be read to refer to the joint venture member.
** Person signing the Bid shall have the power of attorney given by the Bidder. The power of attorney shall be attached with the Bid Schedules.

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 RFB is issued**]*

Loan No. /Credit No. / Grant No.: *[insert **reference number for loan/credit/grant**]*

RFB No: *[insert RFB **reference number from Procurement Plan**]*

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

To: *[insert **Name of Bidder**]*

This is to notify you that your Bid 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 Bidders 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 BDS ITB 47.1 within eight (8) Business days using the Beneficial Ownership Disclosure Form, included in Section X, - Contract Forms, of the Bidding Document.

Authorized Signature: _____

Name and Title of Signatory: *[insert **Name and Title**]*

Name of Agency: *[insert **Purchaser Name**]*

Attachment: Contract Agreement

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.	1.1	Contract Documents (Reference GCC Clause 1.1 (a) (ii))
Contract Documents		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 bid and original Price Schedules

(f)   Code of Conduct for Supplier's Personnel

(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;

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.   4.1   The Appendixes listed below shall be deemed to form an integral part of this Contract Agreement.

Appendixes

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

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"

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.**]*

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.

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 bid 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

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.

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

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**]*

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 Bid. These Revised Price Schedules reflect any corrections or adjustments to the Supplier's bid price, pursuant to the ITB Clauses 30.3 and 38.2.

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).

2. PERFORMANCE AND ADVANCE PAYMENT SECURITY FORMS

2.1   Performance Security Form (Bank Guarantee)

(Bank Guarantee)

[The bank, as requested by the successful Bidder, 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)**[13] **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,[14] and any demand for payment under it must be received by us at this office on or before that date.

---

[13]   *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.*

[14]   *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.*

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.]*

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***])*[151] 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 credited to the Applicant on its account number *[insert* **number***]* at *[insert* **name and address of Applicant's bank***]*.

---

[151]   *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.*

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.]*

3. INSTALLATION AND ACCEPTANCE CERTIFICATES

3. Installation and Acceptance Certificates

3.1   Installation Certificate

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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]*

3.2   Operational Acceptance Certificate

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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]*

4. CHANGE ORDER PROCEDURES AND FORMS

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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

4.1 Request for Change Proposal Form

(Purchaser's Letterhead)

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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.

(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]*

4.2   Change Estimate Proposal Form

(Supplier's Letterhead)

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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]*

4.3   Estimate Acceptance Form

(Purchaser's Letterhead)

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

Loan/Credit Number: *[insert:* **loan or credit number from RFB** *]*

RFB: *[insert:* **title and number of RFB** *]*

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]*

4.4   Change Proposal Form

(Supplier's Letterhead)

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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**]*

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]*

4.5   Change Order Form

(Purchaser's Letterhead)

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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]*

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]*

4.6   Application for Change Proposal Form
(Supplier's Letterhead)

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

Loan/Credit Number: *[insert: **loan or credit number from RFB**]*

RFB: *[insert: **title and number of RFB**]*

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:

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]*