KENYA CIVIL AVIATION AUTHORITY
P.O BOX 30163-00100
NAIROBI
Email:- procurement@kcaa.or.ke

INVITATION TO TENDER (ITT) NO: KCAA/018/2025-2026

TENDER FOR

PROVISION OF OFFICE SUITE SOFTWARE AND RELATED END POINT SECURITY.

DATE OF NOTICE: TUESDAY, 10TH FEBRUARY,2026

CLOSING DATE: THURSDAY, 26TH FEBRUARY,2026 AT 11:00 AM

Note:

1. *All bidders to note that KCAA communicates only in writing to all interested bidders.*
2. *A mandatory pre-bid meeting will be held at KCAA Headquarters, Aviation House on* ***Friday, 20th February 2026 at 10:00 Hours***
3. *All clarification requests from bidders should be sent to email: procurement@kcaa.or.ke on or before* ***Friday, 20th February,2026 by 5pm.***

TABLE OF CONTENTS

PREFACE ..... **iv**

APPENDIX TOTHE PREFACE vi
GUIDELINES FOR PREPARATION OF TENDER DOCUMENTS vi
1. GENERAL vi
2. PART 1 - TENDERING PROCEDURES vi
3. PART 2 – PROCUREMENT ENTITY'S REQUIREMENTS vii
4. PART 3 – CONDITIONS OF CONTRACT ANDCONTRACTFORMS vii

INVITATION TOTENDER ix

PART I –TENDERING PROCEDURE 1

Section I - Instructions to Tenderers 1

A. General **1**
1. Scope of Tender 1
2. Unfair Competitive Advantage 1
3. Fraud and Corruption 1
4. Eligible Tenderers 1
5. Qualification of the Tenderer 3

B. Contents of Tendering Document **3**

6. Sections of Tendering Document 3
PART 1: Tendering Procedures 3
PART 2: Procuring Entity's Requirements 4
PART3: Contract 4
7. Site Visit. 4
8. Pre-Tender Meeting and a pre-arranged pretender visit of the site of the works 4
9. Clarification of Tender Document, Site Visit, Pre-Tender Meeting. 4
10. Amendment of Tendering Documents 5

C. Preparation of Tenders **5**

11. Cost of Tendering 5
12. Language of Tender 5
13. Documents Comprising the Tender 5
14. Form of Tender and Activity Schedule 6
15. Alternative Tenders 6
16. Tender Prices and Discounts 6
17. Currencies of Tender and Payment 6
18. Documents Establishing Conformity of Services 6
19. Documents Establishing the Eligibility and Qualifications of the Tenderer 7
20. Period of Validity of Tenders 8
21. Tender Security 8
22. Format and Signing of Tender 9

D. Submission and Opening of Tenders **9**
23. Sealing and Marking of Tenders 9
24. Deadline for Submission of Tenders 10
25. Late Tenders 10
26. Withdrawal, Substitution and Modification of Tenders 10
27. Tender Opening 10

E.

Evaluation and Comparison of Tenders **11**
28. Confidentiality 11
29. Clarification of Tenders 11
30. Deviations, Reservations, and Omissions 11
31. Determination of Responsiveness 12
32. Correction of Arithmetical Errors 12
33. Conversion to Single Currency 12
34. Margin of Preference and Reservations 34
35. Evaluation of Tenders 34
37. Abnormally Low Tenders and Abnormally High Tenders 34
38. Unbalanced and/or Front-Loaded Tenders 14
39. Qualification of the Tenderer 14
40. Procuring Entity's Right to Accept Any Tender, and to Reject Any or All Tenders 15

F. Award of Contract 15
41. Award Criteria 15
42. Notice of Intention to enter into a Contract 15
43. Standstill Period 15
44. Debriefing by the Procuring Entity 15
45. Letter of Award 15
46. Signing of Contract 16
47. Performance Security 16
48 Publication of Procurement Contract 16
48. Adjudicator 16
49. Procurement Related Complaint 16

SECTION II - TENDER DATASHEET (TDS) **17**

SECTION III - EVALUATION AND QUALIFICATION CRITERIA **21**
1. General Provision 21
2. Preliminary examination for Determination of Responsiveness 21
3. Tender Evaluation (ITT 35) 21
4. Multiple Contracts 21
5. Alternative Tenders (ITT 14.1) 22
6. MARGIN OF PREFERENCE 22
7. Post qualification and Contract ward (ITT 39), more specifically 22

SECTION IV-TENDERING FORMS **24**

1. FORM OFTENDER **24**
i) TENDERER'S ELIGIBILITY- CONFIDENTIAL BUSINESS QUESTIONNAIRE . 27
ii) CERTIFICATE OF INDEPENDENT TENDER DETERMINATION 29
iii) SELF-DECLARATION FORM 30
iv) APPENDIX 1- FRAUD AND CORRUPTION 33

2. TENDERER INFORMATION FORM **35**

OTHER FORMS **36**
3. FORM OF TENDER SECURITY - DEMANDBANKGUARANTEE 36
4. FORM OF TENDER SECURITY(TENDERBOND) 37
5. FORM OFTENDER-SECURING DECLARATION 38

QUALIFICATION FORMS **40**
6. FOREIGN TENDERERS40% RULE 40
7. FORM EQU: EQUIPMENT 41
8. FORM PER -1 42
9. FORM PER-2 44

TENDERERS QUALIFICATION WITHOUT PREQUALIFICATION **46**
10. FORM ELI -1.1 46
11. FORM ELI -1.2 47
12. FORM CON– 2 48
13. FORM FIN– 3.1 50
14. FORM FIN– 3.2 52
15. FORM FIN– 3.3 52
16. FORM FIN– 3.4 53
17. FORM EXP- 4.1 54
18. FORM EXP- 4.2(a) 55
19. FORM EXP- 4.2(b) 56

SCHEDULE FORMS 58
1. Method Statement 61
2. Work Plan 62
3. Others –Time Schedule 63

CONTRACTFORMS **64**
1. NOTIFICATION OF INTENTIONTOAWARD 64
2. NOTIFICATION OF AWARD - FORMOFACCEPTANCE 66
3. FORM OF CONTRACT 67
4. FORM OF TENDER SECURITY (Bank Guarantee) 69
5. FORM OF TENDER SECURITY(TENDERBOND) 70
6. FORM OFTENDER-SECURING DECLARATION 71

PART II – PROCURINGENTITY'S REQUIREMENTS **72**

SECTION VII – ACTIVITY SCHEDULE **73**
1. Objectives 73
2. Day work Schedule 73
3. Provisional Sums 73
4. PERFORMANCE SPECIFICATIONS AND DRAWINGS 74

PART III – CONDITIONS OF CONTRACT AND CONTRACT FORMS **75**

SECTION VIII - GENERAL CONDITIONS OF CONTRACT **76**
A. General Provisions **76**
1. Definitions 76
2. Commencement, Completion, Modification, and Termination of Contract 77
3. Obligations of the Service Provider 79
4. Service Provider's Personnel 82
5. Obligations of the Procuring Entity 82
6. Payments to the Service Provider 82
7. Quality Control 84
8. Settlement of Disputes 84

B. SECTION IX - SPECIAL CONDITIONS OF CONTRACT **88**

C. APPENDICES **91**
Appendix A - Description of the Services 91
Appendix B - Schedule of Payments and Reporting Requirements 91
Appendix C - Breakdown of Contract Price 91
Appendix D - Services and Facilities Provided by the Procuring Entity 91

D. SECTION X –CONTRACT FORMS **92**
FORM NO. 1 - PERFORMANCE SECURITY – (Unconditional Demand Bank Guarantee) 92
FORM No. 2 - PERFORMANCE SECURITY OPTION 2– (Performance Bond) 93
FORM NO. 3 - ADVANCE PAYMENT SECURITY [Demand Bank Guarantee] 95

INVITATION TO TENDER (ITT)
KENYA CIVIL AVIATIONAUTHORITY

CONTRACT NAME AND DESCRIPTION: PROVISION OF OFFICE SUITE SOFTWARE AND RELATED END POINT SECURITY.

1. The Kenya Civil Aviation Authority invites sealed tenders for **Provision of Office suite software and related end point Security.**

2. Tendering will be conducted under open competitive method (National Tender) using a standardized tender document. Tendering is open to all qualified and interested Tenderers.

3. Qualified and interested tenderers may obtain further information and inspect the Tender Documents during office hours **0900 to1500 hours** at the address given below.

4. A complete set of tender documents may be purchased or obtained by interested tenders upon payment of a non-refundable fees of Kshs.1000 in cash or banker's cheque payable to Kenya Civil Aviation Authority. Tenderers may also view and download the bidding document electronically from KCAA website: **www.kcaa.or.ke** or Public Procurement Information Portal **www.tenders.go.ke** at no cost and immediately forward their particulars for records and for the purposes of receiving any further tender clarifications and/or addendums **procurement@kcaa.or.ke.**

5. Tender documents obtained electronically will be free of charge. Tenderers downloading documents from a designated Website shall advise the Procurement Entity that they have downloaded the tender documents, giving full contact addresses of the tenderer through ***procurement@kcaa.or.ke.***

6. Tender documents may be viewed and downloaded for free from the website www.kcaa.or.ke or www.tenders.go.ke. Tenderers who download the tender document must forward their particulars immediately to ***procurement@kcaa.or.ke*** to facilitate any further clarification or addendum. **KCAA will respond to the request for clarifications and send to all the interested bidders who have notified the Authority of their interest in the tender as required.**

7. The tenders must be accompanied by a tender Security *as per the two LOTs below;*
8. ***LOT 1 (Office suite) = Kshs. 500,000.00 (Five Hundred Thousand Only)***
LOT 2 = (End point security) Kshs.1,000,000.00 (One million Only)

9. **A mandatory pre-bid meeting** will be held at KCAA Headquarters, Aviation House on Friday, **20th February 2026 at 10:00 Hours.**

10. All clarifications should be sought from KCAA through email address procurement@kcaa.or.ke on or before **Friday, 20th February,2026 at 5.00pm**.

11. Completed tenders must be delivered to the address below on or before **THURSDAY, 26TH FEBRUARY,2026** at **1100 hours East African time**. Electronic Tenders **will not** be permitted.

12. Tenders will be opened immediately after the deadline date and time specified above or any dead line date and time specified later. Tenders will be publicly opened in the presence of the Tenderers' designated representatives and anyone who chooses to attend at the address below.

13. Late tenders will be rejected.

14. The addresses referred to above are:

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

Kenya Civil Aviation Authority
Procurement Office, Ground floor, Aviation House,
Jomo Kenyatta International Airport:
P.O. Box 30163-00100 Nairobi
Email: ***procurement@kcaa.or.ke***
Tel:- 020827470-5, +254 709725000
P.O Box 30163-00100, Nairobi

B. Address for Submission of Tenders.

Director General
Kenya Civil Aviation Authority
Ground floor, Aviation House, Jomo Kenyatta International Airport:
P.O. Box 30163-00100 Nairobi

C. Address for Opening of Tenders.

Kenya Civil Aviation Authority
Auditorium, Ground floor, Aviation House, Jomo Kenyatta International Airport
Invitation issued by:- William K. Kitum
Designation: - Deputy Director, Supply Chain Management
(For Director General)
Date: - 26th February,2026.

SECTION I -INSTRUCTIONS TO TENDERERS

A. General

1. Scope of Tender

1.1 This tendering document is for the delivery of Non-Consulting Services, as specified in Section V, Procuring Entity's Requirements. The name, identification and number of this tender are specified in the **TDS.**

2. Throughout this tendering document:

The terms:

a) The term "in writing" means communicated in written form (e.g., by mail, e-mail, fax, including if specified **in the TDS**, distributed or received through the electronic-procurement system used by the Procuring Entity) with proof of receipt;

b) if the contexts or esquires, "singular" means "plural" and vice versa; and

c) "Day" means calendar day, unless otherwise specified as "Business Day". A Business Day is any day that is an official working day of the Procuring Entity. It excludes the Procuring Entity's official public holidays.

2.2 The successful Tenderer will be expected to complete the performance of the Services by the Intended Completion Date provided **in the TDS**.

3. Fraud and Corruption

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

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

3.3 **Unfair Competitive Advantage** - Fairness and transparency in the tender process require that the firms or their Affiliates competing for a specific assignment do not derive a competitive advantage from having provided consulting services related to this tender. To that end, the Procuring Entity shall indicate in the **TDS** and make available to all the firms together with this tender document all Information that would in that respect gives such firm any unfair competitive advantage over competing firms.

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

4. Eligible Tenderers

4.1 A Tenderer may be a firm that is a private entity, a state-owned entity or institution subject to ITT 4.6, or any combination of such entities in the form of a Joint Venture (JV) under an existing agreement or with the intent to enter into such an agreement supported by a Form of intent. In the case of a joint venture, all members shall be jointly and severally liable for the execution of the entire Contract in accordance with the Contract terms. The JV shall nominate a Representative who shall have the authority to conduct all business for and on behalf of any and all the members of the JV during the Tendering process and, in the event the JV is awarded the Contract, during contract execution. Members of a joint venture may not also make an individual tender, be a sub contract or in a separate tender or be part of another joint venture for the purposes of the same Tender. The maximum number of JV members shall be specified in the **TDS.**

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

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

a Directly or indirectly controls, is controlled by or is under common control with another Tenderer; or

b Receives or has received any direct or indirect subsidy from another Tenderer; or

c has the same legal representative as another Tenderer; or

d has a relationship with another Tenderer, directly or through common third parties, that puts it in a position to influence the Tender of another Tenderer, or influence the decisions of the Procuring Entity regarding this Tendering process; or

e oranyofitsaffiliatesparticipatedasaconsultantinthepreparationoftheProcuringEntity'sRequirements (including Activities Schedules, Performance Specifications and Drawings) for the Non-Consulting Services that are the subject of the Tender; or

f or any of its affiliates has been hired (or is proposed to be hired) by the Procuring Entity or Procuring Entity 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 TDS ITT 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 Procuring Entity or of the project implementing agency, who:

i. are directly or in directly involved in the preparation of the tendering document or specifications of the contract, and/or the Tender evaluation process of such contract; or

ii. Would be involved in the implementation or supervision of such contract unless the conflicts teeming from such relationship has been resolved in a manner acceptable to the Procuring Entity throughout the procurement process and execution of the Contract.

4.4 A firm that is a Tenderer (either individually or as a JV member) shall not participate in more than one tender, except for permitted alternative Tenders. This includes participation as a subcontractor. Such participation shall result in the disqualification of all Tenders in which the firm is involved. A firm that is not a Tenderer or a JV member may participate as a sub-contractor in more than one Tender.

4.5 A Tenderer may have the nationality of any country, subject to the restrictions pursuant to ITT 4 .9.

4.6 A Tenderer that has been sanctioned by PPRA or are under a temporary suspension or a debarment imposed by any other entity of the Government of Kenya shall be ineligible to be pre-qualified for, initially selected for, tender for, propose for, or be awarded a contract during such period of sanctioning. The list of debarred firms and individuals is available at the PPRA Website www.ppra.go.ke

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

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

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

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

4.11 Pursuant to the eligibility requirements of ITT 4.10, a tender is considered a foreign tenderer, if the tenderer is not registered in Kenya or if the tenderer is registered in Kenya and has less than 51 percent ownership by Kenyan citizens. JVs are considered as foreign tenderers if the individual member firms are not registered in Kenya or if are registered in Kenya and have less than 51 percent ownership by Kenyan citizens. The JV shall not sub contract to foreign firms more than 10 percent of the contract price, excluding provisional sums.

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

4.13 A Tenderer may be considered ineligible if he/she offers goods, works and production processes with characteristics that have been declared by the relevant national environmental protection agency or by other competent authority as harmful to human beings and to the environment shall not be eligible for procurement.

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

5 Qualification of the Tenderer

5.1 All Tenderers shall provide in Section IV, Tendering Forms, a preliminary description of the proposed work method and schedule, including drawings and charts, as necessary.

5.2 In the event that pre-qualification of Tenderers has been undertaken as stated in ITT 18.3, the provisions on qualifications of the Section III, Evaluation and Qualification Criteria shall not apply.

B. Contents of Tendering Document

6 Sections of Tendering Document

6.1 The tendering 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 ITT 10.

PART 1: Tendering Procedures

i) Section I - Instructions to Tenderers (ITT)
ii) Section II - Tender Data Sheet (TDS)
iii) Section III - Evaluation and Qualification Criteria
iv) Section IV - Tendering Forms

PART 2: Procuring Entity's Requirements

v) Section V-Procuring Entity's Requirements

PART 3: Contract

i) Section VI - General Conditions of Contract (GCC)

ii) Section VII - Special Conditions of Contract (SCC)

iii) Section VIII - Contract Forms

6.2 The Invitation to Tender (ITT) notice or the notice to pre-qualify Tenderers, as the case may be, issued by the Procuring Entity is not part of this tendering document.

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

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

7. Site Visit

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

8 Pre-Tender Meeting

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

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

8.3 Minutes of the pre-Tender meeting and the pre-arranged pre tender visit of the site of the service, if applicable, including the text of the questions asked by Tenderers and the responses given, together with any responses prepared after the meeting, will be transmitted promptly to all Tenderers who have acquired the Tender Documents in accordance with ITT6.3. Minutes shall not identify the source of the questions asked.

8.4 The Procuring Entity shall also promptly publish anonymized (*no names*) Minutes of the pre-Tender meeting and the pre-arranged pretender visit of the site of the service at the web page identified **in the TDS**. Any modification to the Tender Documents that may become necessary as a result of the pre-Tender meeting shall be made by the Procuring Entity exclusively through the issue of an Addendum pursuant to ITT10 and not through the minutes of the pre-Tender meeting. Nonattendance at the pre-Tender meeting will not be a cause for disqualification of a Tenderer.

9 Clarification of Tender Documents

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

Procuring Entity shall amend the Tender Documents appropriately following the procedure under ITT 8.4.

10 Amendment of Tender Documents

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

10.2 Any addendum issued shall be part of the tendering document and shall be communicated in writing to all who have obtained the tendering document from the Procuring Entity in accordance with ITT 6.3. The Procuring Entity shall also promptly publish the addendum on the Procuring Entity's web page in accordance with ITT 8.4.

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

C. Preparation of Tenders

11 Cost of Tendering

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

12 Language of Tender

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

13 Documents Comprising the Tender

13.1 The Tender shall comprise the following:

a **Form of Tender** prepared in accordance with ITT 14;

b **Schedules:** priced Activity Schedule completed in accordance with ITT 14 and ITT 16;

c **Tender Security or Tender-Securing Declaration** in accordance with ITT 21.1;

d **Alternative Tender**: if permissible in accordance with ITT 15;

e **Authorization:** written confirmation authorizing the signatory of the Tender to commit the Tenderer, in accordance with ITT 22.3;

f **Qualifications:** documentary evidence in accordance with ITT 19 establishing the Tenderer's qualifications to perform the Contract if its Tender is accepted;

g **Tenderer's Eligibility**: documentary evidence in accordance with ITT 19 establishing the Tenderer's eligibility to Tender;

h **Conformity**: documentary evidence in accordance with ITT 18, that the Services conform to the tendering document; and

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

The Tenderer shall chronologically serialize pages of all tender documents submitted.

13.2 In addition to the requirements under ITT 13.1, Tenders submitted by a JV shall include a copy of the Joint Venture Agreement entered into by all members. Alternatively, a Form of intent to execute a Joint Venture Agreement in the event of a successful Tender shall be signed by all members and submitted with the Tender, together with a copy of the proposed Agreement.

13.3 The Tenderer shall furnish in the Form of Tender information on commissions and gratuities, if any, paid or to be paid to agents or any other party relating to this Tender.

14 Form of Tender and Activity Schedule

14.1 The Form of Tender and priced Activity Schedule shall be prepared using the relevant forms furnished in Section IV, Tendering Forms. The forms must be completed without any alterations to the text, and no substitutes shall be accepted except as provided under ITT 22.3. All blank spaces shall be filled in with the information requested.

14.2 The Tenderer shall furnish in the Form of Tender information on commissions and gratuities, if any, paid or to be paid to agents or any other party relating to this Tender.

15 Alternative Tenders

15.1 Unless otherwise indicated **in the TDS**, alternative Tenders shall not be considered. If alternatives are permitted, only the technical alternatives, if any, of the Best Evaluated Tender shall be considered by the Procuring Entity.

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

15.3 When specified **in the TDS**, Tenderers a reemitted to submit alternative technical solutions for specified parts of the Services, and such parts will be identified **in the TDS**, as will the method for their evaluating, and described in Section VII, Procuring Entity's Requirements.

16. Tender Prices and Discounts

16.1 The prices and discounts (including any price reduction) quoted by the Tenderer in the Form of Tender and in the Activity Schedule (s) shall conform to the requirements specified below.

16.2 All lots (contracts) and items must be listed and priced separately in the Activity Schedule(s).

16.3 The Contract shall be for the Services, as described in Appendix A to the Contract and in the Specifications (or Terms of Reference), based on the priced Activity Schedule, sub mitted by the Tenderer.

16.4 The Tenderer shall quote any discounts and indicate the methodology for their application in the Form of Tender in accordance with ITT 16.1.

16.5 The Tenderer shall fill in rates and prices for all items of the Services described in the in Specifications (or Terms of Reference), and listed in the Activity Schedule in Section VII, Procuring Entity's Requirements. Items for which no rate or price is entered by the Tenderer will not be paid for by the Procuring Entity when executed and shall be deemed covered by the other rates and prices in the Activity Schedule.

16.6 All duties, taxes, and other levies payable by the Service Provider under the Contract, or for any other cause, as of the date 30 days prior to the deadline for submission of Tenders, shall be included in the total Tender price submitted by the Tenderer.

16.7 If provided for **in the TDS**, the rates and prices quoted by the Tenderer shall be subject to adjustment during the performance of the Contract in accordance with and the provisions of Clause 6.6 of the General Conditions of Contract and / or Special Conditions of Contract. The Tenderer shall submit with the Tender all the information required under the Special Conditions of Contract and of the General Conditions of Contract.

16.8 For the purpose of determining the remuneration due for additional Services, a breakdown of the lump-sum price shall be provided by the Tenderer in the form of Appendices D and E to the Contract.

17 Currencies of Tender and Payment

17.1 The currency of the Tender and the currency of payments shall be Kenya Shillings.

18 Documents Establishing Conformity of Services

18.1 To establish the conformity of the Non-Consulting Services to the tendering document, the Tenderer shall furnish as part of its Tender the documentary evidence that Services provided conform to the technical specifications and standards specified in Section VII, Procuring Entity's Requirements.

18.2 Standards for provision of the Non-Consulting Services are intended to be descriptive only and not restrictive. The Tenderer may offer other standards of quality provided that it demonstrates, to the Procuring Entity's satisfaction, that the substitutions ensure substantial equivalence or are superior to those specified in the Section VII, Procuring Entity's Requirements.

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

18.4 The purpose of the information described in ITT 18.3 above, overrides any claims to confidentiality which a tenderer may have. There can be no circumstances in which it would be justified for a tenderer to keep information relating to its ownership and control confidential where it is tendering to undertake public sector work and receive public sector funds. Thus, confidentiality will not be accepted by the Procuring Entity as a justification for a Tenderer's failure to disclose, or failure to provide required information on its ownership and control.

18.4 The Tenderer shall provide further documentary proof, information or authorizations that the Procuring Entity may request in relation to ownership and control which information on any changes to the information which was provided by the tenderer under ITT18.3. The obligations to require this information shall continue for the duration of the procurement process and contract performance and after completion of the contract, if any change to the information previously provided may reveal a conflict of interest in relation to the award or management of the contract.

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

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

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

i) If the procurement process is still on going, the tenderer will be disqualified from the procurement process,

ii) if the contract has been awarded to that tenderer, the contract award will be set aside, pending the outcome of (iii),

iii) The tenderer will be referred to the relevant law enforcement authorities for investigation of whether the tenderer or any other persons have committed any criminal offence.

18.9 If a tenderer submits information pursuant to these requirements that is in complete, inaccurate or out-of-date, or attempts to obstruct the verification process, then the consequences ITT 18.9 will ensue unless the tenderer can show to the reasonable satisfaction of the Procuring Entity that any such act was not material, or was due to genuine err or which was not attributable to the intentional act, negligence or recklessness of the tenderer.

19 Documents Establishing the Eligibility and Qualifications of the Tenderer

19.1 To establish Tenderer's their eligibility in accordance with ITT4, Tenderers shall complete the Form of Tender, included in Section IV, Tendering Forms.

19.2 The documentary evidence of the Tenderer's qualification stopper form the Contract if its Tender is accepted shall establish to the Procuring Entity's satisfaction that the Tenderer meets each of the qualification criterion specified in Section III, Evaluation and Qualification Criteria.

19.3 All Tenderers shall provide in Section IV, Tendering Forms, a preliminary description of the proposed methodology, work plan and schedule.

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

19.5 If pre-qualification has not taken place before Tendering, the qualification criteria for the Tenderers are specified- in Section III, Evaluation and Qualification Criteria.

20 Period of Validity of Tenders

20.1 Tenders shall remain valid for the Tender Validity period specified in the TDS. The Tender Validity period starts from the date fixed for the Tender submission deadline date (as prescribed by the Procuring Entity in accordance with ITT 24.1). A Tender valid for a shorter period shall be rejected by the Procuring Entity as non-responsive.

20.2 In exceptional circumstances, prior to the expiration of the Tender validity period, the Procuring Entity may request Tenderers to extend the period of validity of their Tenders. The request and the responses shall be made in writing. If a Tender Security is requested in accordance with ITT20, it shall also be extended for a corresponding period. A Tenderer may refuse the request without forfeiting its Tender Security. A Tenderer granting the request shall not be required or permitted to modify its Tender.

21 Tender Security

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

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

21.3 If a Tender Security is specified pursuant to ITT 21.1, from a reputable source, and an eligible country and shall be in any of the following forms at the Tenderer's option:

i) cash;

ii) a bank guarantee;

iii) a guarantee by an insurance company registered and licensed by the Insurance Regulatory Authority listed by the Authority; or

iv) a guarantee issued by a financial institution approved and licensed by the Central Bank of Kenya,

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

21.5 If a Tender Security is specified pursuant to ITT 21.1, the Tender Security of unsuccessful Tenderers shall be returned as promptly as possible upon the successful Tenderer's signing the contract and furnishing the Performance Security pursuant to ITT 46. The Procuring Entity shall also promptly return the tender security to the tenderers where the procurement proceedings are terminated, all tenders were determined non-responsive or a bidder declines to extend tender validity period.

21.6 The Tender Security of the successful Tenderer shall be returned as promptly as possible once the successful Tenderer has signed the Contract and furnished the required Performance Security.

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

a. If a Tenderer withdraw sits Tender during the period of Tender validity specified by the Tenderer in the Form of Tender, or any extension there to provide by the Tenderer; or

b. if the successful Tenderer fails to:

c. sign the Contract in accordance with ITT 46; or

d. Furnish a performance security in accordance with ITT 47.

21.8 Where tender securing declaration is executed, the Procuring Entity shall recommend to the PPRA that PPRA debars the Tenderer from participating in public procurement as provided in the law.

21.9 The Tender Security or Tender-Securing Declaration of a JV must be in the name of the JV that submits the Tender. If the JV has not been legally constituted into a legally enforceable JV at the time of Tendering, the Tender security or Tender-Securing Declaration shall be in the names of all future members as named in the Form of intent referred to in ITT 4.1 and ITT 13.2.

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

22 Format and Signing of Tender

22.1 The Tenderer shall prepare one original of the documents comprising the Tender as described in ITT 13, bound with the volume containing the Form of Tender, and clearly marked "Original. "In addition, the Tenderer shall submit copies of the Tender, in the number specified **in the TDS**, and clearly marked as "Copies. "In the event of discrepancy between them, the original shall prevail.

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

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

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

22.5 Any inter-lineation, erasures, or overwriting shall be valid only if they are signed or initialed by the person signing the Tender.

D. Submission and Opening of Tenders

23 Sealing and Marking of Tenders

23.1 Depending on the sizes or quantities or weight of the tender documents, a tenderer may use an envelope, package or container. The Tenderer shall deliver the Tender in a single sealed envelope, or in a single sealed package, or in a single sealed container bearing the name and Reference number of the Tender, addressed to the Procuring Entity and a warning not to open before the time and date for Tender opening date. Within the single envelope, package or container, the Tenderer shall place the following separate, sealed envelopes:

a. in an envelope or package or container marked "ORIGINAL", all documents comprising the Tender, as described in ITT13; and

b. in an envelope or package or container marked "COPIES", all required copies of the Tender; and

c. if alternative Tenders are permitted in accordance with ITT15, and if relevant:

i. in an envelope or package or container marked "ORIGINAL–ALTERNATIVE TENDER", the alternative Tender; and

ii. in the envelope or package or container marked "COPIES- ALTERNATIVE TENDER", all required copies of the alternative Tender.

The inner envelopes or packages or containers shall:

a) Bear the name and address of the Procuring Entity.

b) Bear the name and address of the Tenderer; and

c) Bear the name and Reference number of the Tender.

23.2 If an envelope or package or container is not sealed and marked as required, the *Procuring Entity* will assume no responsibility for the misplacement or premature opening of the Tender. Tenders misplaced or opened prematurely will not be accepted.

24 Deadline for Submission of Tenders

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

24.2 The Procuring Entity may, at its discretion, extend the deadline for the submission of Tenders by amending the tendering document in accordance with ITT9, in which case all rights and obligations of the Procuring Entity and Tenderers previously subject to the deadline shall thereafter be subject to the deadline as extended.

25 Late Tenders

25.1 The Procuring Entity shall not consider any Tender that arrives after the dead line for submission of Tenders, in accordance with ITT 24. Any Tender received by the Procuring Entity after the deadline for submission of Tenders shall be declared late, rejected, and returned un opened to the Tenderer.

26 Withdrawal, Substitution and Modification of Tenders

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

a) Prepared and submitted in accordance with ITT 21 and ITT 22 (except that withdrawal notices do not require copies), and in addition, the respective envelopes shall be clearly marked "WITHDRAWAL," "SUBSTITUTION," or "MODIFICATION;" and
b) Received by the Procuring Entity prior to the deadline prescribed for submission of Tenders, in accordance with ITT 23.

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

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

27 Tender Opening

27.1 Except as in the cases specified in ITT 23 and ITT 25.2, the Procuring Entity shall, at the Tender opening, publicly open and read out all Tenders received by the deadline at the date, time and place specified **in the TDS** in the presence of Tenderers' designated representatives and anyone who choose to attend. Any specific electronic Tender opening procedures required if electronic tendering is permitted in accordance with ITT 23.1 shall be as specified **in the TDS.**

27.2 First, envelopes marked "WITHDRAWAL" shall be opened and read out and the envelope with the corresponding Tender shall not be opened, but returned to the Tenderer. If the withdrawal envelope does not contain a copy of the "power of attorney" confirming the signature as a person duly authorized to sign on behalf of the Tenderer, the corresponding Tender will be opened. No Tender withdrawal shall be permitted unless the corresponding withdrawal notice contains a valid authorization to request the withdrawal and is read out at Tender opening.

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

27.4 Next, envelopes marked "MODIFICATION" shall be opened and read out with the corresponding Tender. No Tender modification shall be permitted unless the corresponding modification notice contains a valid authorization to request the modification and is read out at Tender opening.

27.5 Next, all remaining envelopes shall be opened one at a time, reading out: the name of the Tenderer and whether there is a modification; the total Tender Prices, per lot (contract) if applicable, including any discounts and

alternative Tenders; the presence or absence of a Tender Security or Tender-Securing Declaration, if required; and any other details as the Procuring Entity may consider appropriate.

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

27.7 The Procuring Entity shall neither discuss the merits of any Tender nor reject any Tender (except for late Tenders, in accordance with ITT25.1).

27.8 The Procuring Entity shall prepare are cord of the Tender opening that shall include, as a minimum:

a) The name of the Tenderer and whether there is a withdrawal, substitution, or modification;

b) The Tender Price, per lot (contract) if applicable, including any discounts; and

c) any alternative Tenders;

d) The presence or absence of a Tender Security or Tender-Securing Declaration, if one was required.

e) Number of pages of each tender document submitted

27.9 The Tenderers' representatives who a rep resent shall be requested to sign the record. The omission of a Tenderer's signature on the record shall not invalidate the contents and effect of the record. A copy of the tender opening register shall be distributed to Tenderer upon request.

E. Evaluation and Comparison of Tenders

28 Confidentiality

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

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

28.3 Notwithstanding ITT 28.2, from the time of Tender opening to the time of Contract Award, if any Tenderer wishes to contact the Procuring Entity on any matter related to the Tendering process, it should do so in writing.

29 Clarification of Tenders

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

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

30 Deviations, Reservations, and Omissions

30.1 During the evaluation of Tenders, the following definitions apply:

a) “Deviation” is a departure from the requirements specified in the tendering document;

b) “Reservation” is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the tendering document; and

c) “Omission” is the failure to submit part or all of the information or documentation required in the tendering document.

31 Determination of Responsiveness

31.1 The Procuring Entity's determination of a Tender's responsiveness is to be based on the contents of the Tender itself, as defined in ITT 12.

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

a) If accepted, would:

i. affect in any substantial way the scope, quality, or performance of the Non-Consulting Services specified in the Contract; or

ii. limit in any substantial way, inconsistent with the tendering document, the Procuring Entity's rights or the Tenderer's obligations under the Contract; or

b) if rectified, would unfairly affect the competitive position of other Tenderers presenting substantially responsive Tenders.

31.3 The Procuring Entity shall examine the technical aspects of the Tender submitted in accordance with ITT 18and ITT 19, in particular, to confirm that all requirements of Section VII, Procuring Entity's Requirements have been met without any material deviation or reservation, or omission.

31.4 If a Tender is not substantially responsive to the requirements of tendering document, it shall be rejected by the Procuring Entity and may not subsequently be made responsive by correction of the material deviation, reservation, or omission.

31.5 Provided that a Tender is substantially responsive, the Procuring Entity may waive any non-conformity in the Tender.

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

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

32 Arithmetical Errors

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

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

a) Any error detected if considered a major deviation that affects the substance of the tender, shall lead to disqualification of the tender as non-responsive.

b) Any errors in the submitted tender arising from a miscalculation of unit price, quantity, subtotal and total bid price shall be considered as a major deviation that affects the substance of the tender and shall lead to disqualification of the tender as non-responsive .and

c) If there is a discrepancy between words and figures, the amount in words shall prevail

32.3 Tenderers shall be notified of any error detected in their bid during the notification of a ward.

33 Conversion to Single Currency

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

34 Margin of Preference and Reservations

34.1 Margin of preference on local service providers may be allowed if it is deemed that the services require participation of foreign tenderers. If so allowed, it will be indicated in the **TDS.**

34.2 Where it is intended to reserve the contract to specific groups under Small and Medium Enterprises, or enterprise of women, youth and /or persons living with disability, who are appropriately registered as such by the authority to be specified in the **TDS**, a procuring entity shall ensure that the invitation to tender specifically indicates that only businesses/firms belonging to the specified group are eligible to tender as specified in the **TDS**. Otherwise, if not so stated, the invitation will be open to all tenderers.

35 Evaluation of Tenders

35.1 The Procuring Entity shall use the criteria and methodologies listed in this ITT and Section III, Evaluation and Qualification Criteria. No other evaluation criteria or methodologies shall be permitted. By applying the criteria and methodologies, the Procuring Entity shall determine the Best Evaluated Tender. This is the Tender of the Tenderer that meets the qualification criteria and whose Tender has been determined to be:

a) Substantially responsive to the tendering document; and

b) The lowest evaluated cost.

35.2 In evaluating the Tenders, the Procuring Entity will determine for each Tender the evaluated Tender cost by adjusting the Tender price as follows:

a) Price adjustment due to discounts offered in accordance with ITT 16.4;

b) price adjustment due to quantifiable non material non-conformities in accordance with ITT 31.3;

c) converting the amount resulting from applying (a) and (b) above, if relevant, to a single currency in accordance withITT33; and

d) any additional evaluation factors specified **in the TDS** and Section III, Evaluation and Qualification Criteria.

35.3 The estimated effect of the price adjustment provisions of the Conditions of Contract, applied over the period of execution of the Contract, shall not be considered in Tender evaluation.

35.4 In the case of multiple contracts or lots, Tenderers are allowed to tender for one or more lots and the methodology to determine the lowest evaluated cost of the lot (contract) and for combinations, including any discounts offered in the Form of Tender, is specified in Section III, Evaluation and Qualification Criteria. For one or more lots (contracts). Each lot or contract will be evaluated in accordance with ITT

35.5. The methodology to determine the lowest evaluated tenderer or tenderers based one lot (contract) or based on a combination of lots (contracts), will be specified in Section III, Evaluation and Qualification Criteria. In the case of multiple lots or contracts, tenderer will be will be required to prepare the Eligibility and Qualification Criteria Form for each Lot.

36 Comparison of Tenders

36.1 The Procuring Entity shall compare the evaluated costs of all substantially responsive Tenders established in accordance with ITT 35.2 to determine the Tender that has the lowest evaluated cost.

37 Abnormally Low Tenders and Abnormally High

Tenders Abnormally Low Tenders

37.1 An Abnormally Low Tender is one where the Tender price, in combination with other elements of the Tender, appears so low that it raises material concerns as to the capability of the Tenderer in regards to the Tenderer's ability to perform the Contract for the offered Tender Price.

37.2 In the event of identification of a potentially Abnormally Low Tender, the Procuring Entity shall seek written clarifications from the Tenderer, including detailed price analyses of its Tender price in relation to the subject

matter of the contract, scope, proposed methodology, schedule, allocation of risks and responsibilities and any other requirements of the Tender document.

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

Abnormally High Tenders

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

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

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

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

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

38 Unbalanced and/or Front-Loaded Tenders

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

38.2 After the evaluation of the information and detailed price analyses presented by the Tenderer, the Procuring Entity may as appropriate:

a) Accept the Tender; or

b) require that the total amount of the Performance Security be increased at the expense of the Tenderer to a level not exceeding 10% of the Contract Price; or

c) agree on a payment mode that eliminates the inherent risk of the Procuring Entity paying too much for undelivered works; or

d) Reject the Tender.

39 Qualification of the Tenderer

39.1 The Procuring Entity shall determine to its satisfaction whether the Tenderer that is selected as having submitted the lowest evaluated cost and substantially responsive Tender 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 Tenderer's qualifications submitted by the Tenderer, pursuant to ITT 18. The determination shall not take into consideration the qualifications of other firms such as the Tenderer's subsidiaries, parent entities, affiliates, subcontractors or any other firm(s)different from the Tenderer that submitted the Tender.

39.3 An affirmative determination shall be a prerequisite for award of the Contract to the Tenderer. A negative determination shall result in disqualification of the Tender, in which event the Procuring Entity shall proceed to the Tenderer who offers a substantially responsive Tender with the next lowest evaluated cost to make a similar determination of that Tenderer's qualifications to perform satisfactorily.

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

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

F. Award of Contract

43 Award Criteria

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

42 Notice of Intention to enter in to a Contract

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

a) The name and address of the Tenderer submitting the successful tender;

b) The Contract price of the successful tender;

c) a statement of the reason(s) the tender of the unsuccessful tenderer to whom the letter is addressed was unsuccessful, unless the price information in(c) above already reveals the reason;

d) the expiry date of the Stand still Period; and

e) instructions on how to request a debriefing and/or submit a complaint during the stand still period;

43 Stand still Period

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

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

44 Debriefing by the Procuring Entity

44.1 On receipt of the Procuring Entity's Notification of Intention to Enter into a Contract referred to in ITT 42, an unsuccessful tenderer may make a written request to the Procuring Entity for a debriefing on specific issues or concerns regarding their tender. The Procuring Entity shall provide the debriefing with in five days of receipt of the request.

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

45 Letter of Award

Prior to the expiry of the Tender Validity Period and upon expiry of the Standstill Period specified in ITT 43.1, upon addressing a complaint that has been filed within the Standstill Period, the Procuring Entity shall transmit the Letter of Award to the successful Tenderer. The letter of award shall request the successful tenderer to furnish the Performance Security within 21 days of the date of the letter.

46 Signing of Contract

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

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

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

47 Performance Security

47.1 Within twenty-one (21) days of the receipt of the Form of Acceptance from the Procuring Entity, the successful Tenderer, if required, shall furnish the Performance Security in accordance with the GCC 3.9, using for that purpose the Performance Security Form included in Section X, Contract Forms, or another Form acceptable to the Procuring Entity. If the Performance Security furnished by the successful Tenderer is in the form of a bond, it shall be issued by a bonding or insurance company that has been determined by the successful Tenderer to be acceptable to the Procuring Entity. A foreign institution providing a bond shall have a correspondent financial institution located in Kenya, unless the Procuring Entity has agreed in writing that a correspondent financial institution is not required.

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

48 Publication of Procurement Contract

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

a) Name and address of the Procuring Entity;

b) Name and reference number of the contract being awarded, a summary of its scope and the selection method used;

c) The name of the successful Tenderer, the final total contract price, the contract duration.

d) Dates of signature, commencement and completion of contract;

e) Names of all Tenderers that submitted Tenders, and their Tender prices as read out at Tender opening.

49 Adjudicator

49.1 The Procuring Entity proposes the person named **in the TDS** to be appointed as adjudicator or under the Contract, at an hourly fee specified in **the TDS**, plus reimbursable expenses. If the Tenderer disagrees with this Tender, the Tenderer should so state in the Tender. If, in the Form of Acceptance, the Procuring Entity has not agreed on the appointment of the Adjudicator, the Adjudicator shall be appointed by the Appointing Authority designated in the Special Conditions of Contract at the request of either party.

50 Procurement Related Complaint

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

SECTION II - TENDER DATA SHEET (TDS)

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

Reference to ITC Clause	PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS
A. General	
ITT 1.1	The reference number of the Invitation to Tender (ITT) is: ***KCAA/018/2025-2026*** The Procuring Entity is: **KENYA CIVIL AVIATION AUTHORITY** The name of the ITT is: **Provision of Office suite software and related end point Security.** The number and identification of lots (contracts) comprising this ITT is: **TWO Lots.**
ITT 2.1 (a)	Electronic –Procurement System **SHALL NOT BE USED** The Procuring Entity shall use the following electronic-procurement system to manage this Tendering process: **NOT APPLICABLE**
ITT 2.2	The Intended Completion Date is **ONE YEAR AFTER THE DATE OF CONTRACT SIGNING AND THREE YEAR FOR SERVICE LEVEL AGREEMENT (SLA)**
ITT 3.3	Information that any unfair competitive advantage over competing firms is as follow: **NONE**
ITT 3.4	The firms that provided consulting services; **N/A**
ITT 4.1	Maximum number of members in the Joint Venture (JV) shall be: **NONE**
B. Contents of the Tendering Document	
ITT 8.1	**The pre-tender conference will NOT be held. NOT APPLICABLE**
ITT 8.2	Any questions/clarification requests in writing, shall reach the Procuring Entity not later than **FRIDAY, 20TH FEBRUARY,2026 AT 5.00PM**
ITT 8.4	Minutes of the pre-tender meeting and the pre-arranged pretender visit of the site of the works will be published at the website : **NOT APPLICABLE**
ITT 9.1	The Procuring Entity shall publish its response at the website: **www.kcaa.or.ke**
C. Preparation of Tenders	
ITT 13.1 (j)	The Tenderer shall submit the following additional documents in its Tender: **AS LISTED IN THE EVALUATION CRITERIA**
ITT 14.1	Alternative Tenders **SHALL NOT BE** considered.
ITT 14.2	Alternative times for completion shall not permitted. If permitted , the range of acceptable completion time is: **NOT APPLICABLE**
ITT 14.3	Alternative technical solutions shall be permitted for the following parts of the Plant and Installation Services: **NONE.**
ITT 16.7	The prices quoted by the Tenderer **SHALL NOT** be subject to adjustment during the performance of the Contract.
ITT 20.1	**The Tender security shall be as follows for EACH LOT.** **LOT 1 (Office suite) = Kshs. 500,000.00 (Five Hundred Thousand Only)** **LOT 2 = (End point security) Kshs.1,000,000.00 (One million Shillings Only)** validity period shall be **121 days.**
ITT 21.8	The Procuring Entity shall declare the Tenderer ineligible to be awarded a contract by the Procuring Entity for a period of: **ONE YEAR.**

Reference to ITC Clause	PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS
ITT 22.1	In addition to the original of the Tender, the number of copies is: **ONE ORIGINAL AND ONE COPY BOTH IN PAPER FORMAT, SEQUENTIALLY SERIALIZED AND ONE IN A FLASH DISK.**
ITT 22.3	The written confirmation of authorization to sign on behalf of the Tenderer shall consist of: **POWER OF ATTORNEY SIGNED BY THE DONOR AND DULY WITNESSED BY AN ADVOCATE OR COUNSEL.**
D. Submission and Opening of Tenders	
ITT 24.1	For **Tender submission purposes** only, the Procuring Entity's address is: **Attention: Director General** **Kenya Civil Aviation Authority** Ground floor, Aviation House, Jomo Kenyatta International Airport: P.O. Box 30163-00100 **NAIROBI** **The deadline for Tender submission is:** **Date: THURSDAY, 26TH FEBRUARY,2026.** **Time: 11:00 am,** **Tenderers SHALL NOT** have the option of submitting their Tenders electronically
ITT 27.1	The Tender opening shall take place at: **Ground floor, Aviation House, Jomo Kenyatta International Airport, Nairobi** **Date: THURSDAY, 26TH FEBRUARY,2026.** **Time: 11:00 AM**
ITT 27.6	The Form of Tender and Price Schedules shall be initialed by **at least three (3)** representatives of the Procuring Entity conducting Tender opening as follows: i. ***The name of the Tenderer and whether there is a withdrawal, substitution, or modification;*** ii. ***The Tender Price, per lot if applicable, including any discounts;*** ii. ***Any alternative Tenders; and*** v. ***The presence or absence of a Tender Security or a Tender-Securing Declaration.*** v. ***Number of pages for each tender***
E. Evaluation, and Comparison of Tenders	
ITT 31.7	For comparison purposes only, to reflect the price of a missing or non-conforming item or component in the manner specified as follows: The adjustment shall be based on the highest price of the item or component as quoted in other substantially responsive Tenders. If the price of the item or component cannot be derived from the price of other substantially responsive Tenders, the Procuring Entity shall use its best estimate.
ITT 33.1	The currency that shall be used for Tender evaluation and comparison purposes only to convert at the selling exchange rate all Tender prices expressed in various currencies into a single currency is: **KENYA SHILLINGS** The source of exchange rate shall be: **The Central bank or Kenya (mean rate)** The date for the exchange rate shall be: **The deadline date for Submission of the Tenders**. For comparison of Tenders, the Tender Price, corrected pursuant to ITT 31, shall first be broken down into the respective components payable in various currencies by using the selling exchange rates specified by the Tenderer in accordance with ITT 33. In the second step, the Procuring Entity will convert the amounts in various currencies in which the Tender Price is payable (excluding Provisional Sums but including Day work where priced competitively) to the single currency identified above at the selling rates established for similar transactions by the authority specified and, on the date stipulated above.

Reference to ITC Clause	PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS
ITT 34.1	A margin of preference **SHALL NOT** be allowed.
ITT 34.2	The invitation to tender is extended to the following group that qualify for Reservations: **NOT APPLICABLE**
ITT 35.2	Additional evaluation factors shall be: **AS INDICATED IN THE EVALUATION CRITERIA**
ITT 49	The Adjudicator proposed by the Procuring Entity is: **TO BE CONFIRMED** The hourly fee for this proposed Adjudicator shall be: **AS WILL BE AGREED UPON** The biographical data of the proposed Adjudicator is as follows: **TO BE CONFIRMED**
ITT 49	The procedures for making a Procurement-related Complaint are detailed in the "Notice of Intention to Award the Contract" herein and are also available from the PPRA website info@ppra.go.ke or complaints@ppra.go.ke. **For the attention**: ***Director General*** **Title/position**: ***Director General*** **Procuring Entity**: ***Kenya Civil Aviation Authority*** **Email address***: **procurement@kcaa.or.ke*** In summary, a Procurement-related Complaint may challenge any of the following: **1.** the terms of the Tendering Documents; and the Procuring Entity's decision to award the contract.

SECTION III – EVALUATION AND QUALIFICATION CRITERIA

1) PRELIMINARY OF EVALUATION RESPONSIVENESS

The Procuring Entity will start by examining the tender to ensure it meets all respects of the eligibility criteria and other mandatory requirements in the ITT, and that the tender is complete in all aspects in meeting the requirements provided for in the preliminary evaluation criteria outlined below.

EVALUATION CRITERIA

Kenya Civil Aviation Authority will consider the following three categories of criteria to evaluate the tenders.

a) Preliminary tender requirements
b) Technical capability assessment
c) Financial Evaluation.
d) The Authority may carry out due diligence where applicable

a) PRELIMINARY MANDATORY REQUIREMENTS FOR LOT 1 & LOT 2:

The submission of the following mandatory items will be required in the determination of the completeness of the bid and responsiveness of bidders. Bids that do not contain all the information required will be declared non responsive and shall not be evaluated further.

No	Mandatory requirements/documents
1.	**Ineligibility** - Bidders and their associated firms who have existing ongoing contracts with KCAA which have delayed beyond the original scheduled completion period in the contract without proper justification or who according to KCAA records, have failed in performance of previous contracts or have had their previous contracts terminated for non-performance are not eligible to participate.
2.	The tender is signed by the person holding a valid power of attorney, without material deviation, reservation or omission. Attach a copy of Power of Attorney signed by the donor and duly witnessed by an advocate or counsel.
3.	Tenderer's eligibility – duly filled, signed and stamped confidential business questionnaire
4.	Tenderer is a legally registered entity. Attach copy of registration and CR12 certificate
5.	Duly filled, signed and stamped form of tender and tender is valid for 121 days.
6.	Duly filled, signed and stamped price schedules completed in accordance with ITT 14 and ITT 19
7.	Attach a valid tax compliance certificate issued by Kenya Revenue Authority.
8.	Duly filled Certificate of Independent Tender Determination.
9.	The bidder shall provide **two hard copies sequentially paginated marked Original** and copy and MUST provide a **softcopy of the bidding document in a readable flash disk**
10.	Provide a demand bank guarantee for the tender security as follows; (valid for 121 days) ***LOT 1 (Office suite) = Kshs. 500,000.00 (Five Hundred Thousand Only)*** ***LOT 2 = (End point security) Kshs.1,000,000.00 (One million Only)***
11.	Tenderer is not debarred by PPRA or any other Authority. Submit a duly filled and signed Form SD1
12.	Self-declaration that the person/tenderer will not engage in any corrupt or fraudulent practice. Submit a duly filled and signed Form SD2
13.	Project commitment/implementation plan – Bidders MUST attach sample project plan/work program clearly indicating the expected completion date of the project (provide details).
14.	Tenderer has no conflict of interest.
15.	Submit a statement in the bidder's letter head that the company is not insolvent, receivership, bankrupt or in the process of being wound up.
16.	**Warranty -** The bidder MUST provide warranty certificate for three years for EACH solution as applicable.

No	Mandatory requirements/documents
17.	**Bidders experience** – The bidder MUST have successfully deployed at least three (3) similar sites for **Office suite software and related end point Security which must meet the following requirements: -.** **a) LOT 1 (Office Suite) =** i. Experience in similar Microsoft products deployment assignments with three (3) corporate clients (Provide evidence of copies of Sign Off certificate/LSO/LPO/Contract documents) and the names, addresses and contact details of the corporate clients. Each of the contracts should be of value Kshs 25 million and above per. ii. Experience in implementation and deployment of SharePoint intranet in at least One (1) corporate client (Provide evidence of the contract i.e. provide copies of Sign Off certificate/LSO/LPO/Contract documents) and the names, addresses and contact details of the corporate clients. **b) LOT 2 (End Point Security):-** The bidder MUST have successfully deployed at least three (3) similar sites comprised of endpoint, email or Network Security. For each of the sites, attach the following: - i. Name of site/client ii. Copies of LSO/contracts iii. Respective completion certificates or recommendation letters. iv. Contact person's name and email address. v. Each of the contracts must be of value Kshs. 10 million and above.
18.	**Work plan and Methodology –** Provide a detailed technical implementation strategy of the project with the following aspects: - a) Detailed approach, methodology and work plan that the requirements and provision of licenses. The implementation plan should also clearly indicate the 3-year maintenance and support period. b) Details of staff to be involved in the maintenance. These should be the staff with the relevant certifications and experience. c) Step by step tasks from delivery of the office suite and end point security licenses and maintenance and support. d) Documentation of the project. e) Risk management
19.	**Brochure** - Include detailed brochures and datasheets of the bidder's proposed hardware and solutions
20.	**Manufacturer's Authorizations -** The bidder MUST provide the manufacturer's authorizations for the following Security solutions: - i. Office suite ii End-Point Security iii. Email Security iv. Cybersecurity Threat Defense v. Network Access Control (NAC) System
21.	**SLA to be provided –** The bidder shall include a proposed SLA to be adopted after system commissioning. The SLA should include the following key deliverables: - i. Period – 3 years ii. Services to be provided within the SLA iii. Response times iv. Escalations v. Penalties Further details for the required SLA are available in the detailed technical specifications document
22.	The bidders shall submit the latest three years audited financial statements – 2024,2023 &2022.

NOTE:- Bidders may quote for both LOTS or One LOT.

b) MANDATORY TECHNICAL REQUIREMENTS ON LOT 1: OFFICE SUITE:

All Vendors MUST **respond in writing against** each technical requirement **clearly showing technical compliance for each specification against their** brochure with references**. Marking compliant/non-compliant (√) or (X) will be considered** INVALID **and** WILL NOT BE EVALUATED

No.	Documents to be submitted	Bidders' response
1.	Bidders must have Microsoft Manufacturer's Authorization as a Microsoft Licensing Solution Provider (LSP) or Cloud Solutions Provider (CSP) - provide evidence	
2.	Provide evidence that the bidder has at least Four (4) Kenyan based Microsoft Technical Certified professionals to manage KCAA Microsoft environment from a Managed Services perspective. Include Microsoft Certification for each resource. *The bidder must undertake in writing to ensure that the proposed project team is maintained throughout the onboarding phase and commissioning of the new licenses.*	
3.	Bidder must submit Draft Service Level Agreement for support	
4.	Licenses must be genuine and verifiable via KCAA's Microsoft 365 Admin Center.	
5.	Licenses must be assignable seamlessly through the existing KCAA Microsoft 365 tenant.	
6.	Supplier to provide transition window and onboarding assistance where required	
7.	Renewal confirmation from Microsoft and access to Admin Center reporting.	
8.	Training and Knowledge Transfer: The bidder should describe how they shall meet the requirements for training and knowledge transfer. The requirements are as follows: - i. The exercise shall take a period of five (5) days. ii. This bidder shall propose a detailed schedule for the five (5) days including knowledge transfer and training. iii. The training shall entail user and license management, security, compliance, configuration, and ongoing administration of Microsoft 365 services to ensure smooth, secure, and efficient operation of the environment. iv. Six (6) KCAA ICT staff shall be trained. This shall be undertaken at a serene environment out of town. v. All the applicable costs for this activity shall be borne by the vendor. vi. These include but not limited to conferencing, subsistence allowance and other applicable costs.	

c) MANDATORY REQUIREMENTS FOR - SLA SERVICES - LOT 1 (OFFICE SUITE).

NO	Requirement/tasks	Bidder's Response
General Support services		
1.	The maintenance and support period shall be three years (3) years.	
2.	Provision of 24/7 support on Microsoft 365 and its related products and systems	
3.	Provision of Onsite resources on schedule and on demand to resolve technical issues that may arise from time-to-time.	
4.	Maintenance of Office 365 Applications installed and used by KCAA staff	
5.	Support and enhancement of Microsoft Windows Active Directory Environment and on-premises Microsoft Entra ID	
6.	SharePoint Online development and support	
7.	Provision of escalation point for all Microsoft related problems that pertain to Office 365 Subscription Services	
Proactive Support		**Bidder's Response**
1.	Scheduled Infrastructure health checks on key systems for Microsoft 365	
2.	Proactive diagnosis and prevent system problems in scope.	
3.	Carrying out day-to-day escalation duties for tasks in scope.	
4.	Sitting in project deliberations meetings where required.	
5.	Advice the KCAA technical team on best practices and procedures they can adopt to enable them increase Uptime and reduce incidents.	
6.	Provide reports for management consumption when required.	
7.	Generating quarterly reports for KCAA regarding service level performance	
8.	**Reviews** - There will be quarterly reviews of the system support carried out jointly by KCAA and the successful vendor.	
9.	The health reviews and optimization and maintenance of KCAA Microsoft 365 Infrastructure.	
10.	Review of the Active Directory policies	
11.	Office 365 Policies and Best Practices	
12.	Ensure compliance with recommended security score on KCAA Microsoft 365 platform as per Policies and best Practices	

B) MANDATORY TECHNICAL REQUIREMENTS ON LOT 2: END POINT SECURITY INFRASTRUCTURE:

Part A: Mandatory Technical Documentation Requirements – LOT 2

Note: All bidders must provide the following mandatory technical documentation to be considered responsive to proceed to the next evaluation stage. The bidder MUST provide detailed explanations of how they shall fully meet the required technical documentation. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Technical Documentation Required		
No.	**Item/Specification**	**Requirement**	**Bidder's Response**
1.	Manufacturer's Authorizations	The bidder MUST provide the manufacturer's authorizations for the following Security solutions: - i. End-Point Security ii. Email Security iii. Cybersecurity Threat Defense Services iv. Cyber Risk Exposure Management (CREM) v. Network Access Control (NAC) System	
2.	Proof of Physical Location of the Business	The bidder shall provide proof of occupation of the business premises. The proof should be signed lease(s), ownership documentation, or any other applicable and acceptable documentation.	
3.	Staff Competence in Endpoint, Server and Email Security	The bidder MUST have at least three (3) Engineers trained in the deployment of physical servers, virtualization, endpoint, Server, and email security. For each of the engineers: - i. Attach certified CVs ii. Attach copies of certificates showing knowledge of Application Security, VMware, Cloud Security, and Servers. iii. The bidder MUST have 2 vendor certifications of the proposed solution. iv. Attach documentation for sites implemented by the respective Engineers. *The engineers proposed here MUST be involved in the project's implementation if awarded.*	
4.	Staff Competence in Network Security	The bidder MUST have at least two (2) Engineers who are trained and experienced in deploying the Network Access Control System. For each of the Engineers: - i. Attach certified CVs. ii. Attach copies of certificates showing knowledge of Network Security and Access Control iii. The bidder MUST have 2 vendor certifications of the proposed solution. iv. Attach documentation for sites implemented by the respective Engineers. *The engineers proposed here MUST be involved in the project's implementation if awarded.*	

	Technical Documentation Required		
No.	**Item/Specification**	**Requirement**	**Bidder's Response**
5.	Brochure	Include detailed brochures and datasheets of the bidder's proposed solutions	
6.	Sample Service Level Agreement (SLA)	The bidder shall include a proposed SLA to be adopted after system commissioning. The SLA should include the following key deliverables: - i. Period – 3 years ii. Services to be provided within the SLA iii. Response times iv. Escalations v. Penalties Further details for the required SLA are available in the detailed technical specifications document	
7.	Soft copy of the Bidding Document	The vendor MUST provide a soft copy of the bidding document on a Flash Disk.	
8.	Pre-bid Meeting	A pre-bid meeting form duly signed by a KCAA staff member	
9.	Warranty	a. The bidder MUST indicate detailed maintenance and support plan for the system within the warranty periods. b. Further, provide documentation indicating that the warranty for the hardware covers the East African region. c. The bidder MUST indicate the total expected life of the equipment to be supplied	
10.	Vendor Accreditation	a. The vendor must be a leader in the last 3 OMDIA vulnerability Disclosure Index. Attach the OMDIA reports. b. The bidder must be a leader in the latest Magic Quadrant for Extended Detection and Response (XDR). Attach the report's reference. c. Must be named a Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms d. Must be a leader in The Forrester Wave™: Attack Surface Management Solutions	
11.	Collaboration with Law enforcement	The proposed vendor must work with Law-enforcement globally and in Africa. Share public information on such cases including but not limited to fraud bursting or dismantling cybercriminal syndicates	

Note: All bidders must meet the following mandatory technical specifications to be considered responsive in order to proceed to the next stage of evaluation. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirement. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	ANTIVIRUS+XDR			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Product and Quantity	1000 endpoint security licenses shall be deployed in all endpoints at KCAA HQ and all stations	M	
2.	Anti-Malware Capability	Provide advanced automated threat detection and response against a variety of advanced malware threats, including fileless attacks, crypto mining, and ransomware		
3.	Deployment Options	Provide flexible cloud (SaaS) or on-premises deployment options	M	
4.	Unified Agent	The solution should offer both EDR and an endpoint protection platform (Anti-malware, Web Reputation, Device Control, Integrated DLP, Machine learning, Behavior Analysis, Endpoint Cloud Sandbox submission, Virtual Patching for endpoint via HIPs, and Application Control, Endpoint FW) in a single agent	M	
		Provide both Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) features in a single agent	M	
	Intrusion Prevention System	Shall reduce risk exposure due to missing patches	M	
5.		The proposed solution can provide virtual patching functionality without additional agent footprint or 3rd party integration	M	
		The solution shall provide the customer with a performance and security priority option that meets their security requirements and environment.	M	
		Shall be able to block against known & unknown vulnerability exploits	M	
		Solution shall shield endpoints from network exploitable vulnerabilities targeting endpoint OS	M	
		Must have a host-based intrusion prevention system (HIPS) to virtually patch known and unknown vulnerabilities before a patch is available or deployable.	M	
6.	Central Management	Solution must provide central management functions for logs, threat intelligence, status of	M	

	ANTIVIRUS+XDR			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
		managed products/devices, and application deployment.		
		Solution must provide central management functions of threat intelligence, which can be shared with managed products/devices	M	
		Single pane of glass for all security controls and products in the suite	M	
		The solution should be managed through a web console	M	
		Solution must provide central management functions of logs collected from managed products/devices	M	
		Solution must provide granular log search filters for users to define their own search criteria	M	
7.	Damage clean-up service	Solution must be able to remove (reset) malware changes in the Windows registry, remove dropped file(s), and terminate running malicious processes.	M	
		Able to perform different scan Actions based on various malware types (Trojan/ Worm, Joke, Hoax, Virus, etc.)	M	
		Solution shall have a behavior monitoring capability to detect malicious program behavior that is common to exploit attacks	M	
		Able to detect and remove Spyware and Adware even after it is installed and running on the computer.	M	
		It should provide continuous malware protection and perform updates regardless of whether the client is connected to the management server.	M	
		Shall provide continuous malware protection regardless of whether the endpoint is connected to the Internet.	M	
8.	Web Reputation Services	Solution must be able to block access to malicious websites and URLs with an accurate and comprehensive rating algorithm	M	
		Must be able to support the approved (whitelist) and blocked (blacklist) URLs list	M	
		Must be able to block connection attempts to command and control (C&C) servers	M	
		Must be able to support approved (whitelist) and blocked (blacklist) IP lists	M	
9.	Device Control	Able to display a notification message on the client computer when a violation happens	M	
		Able to log Device Control violation	M	

	ANTIVIRUS+XDR			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
		Allow adding of trusted devices	M	
		Must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write, and Deny Access.	M	
10.	System Lockdown	The proposed solution can provide application control functionality without additional agent footprint or 3rd party integration	M	
		Able to manually (by the administrator or security officer) or automatically (via sandbox report) block the tagged suspicious applications.	M	
		Must be able to correlate data from millions of application events to identify threats and maintain an up-to-date database of validated applications	M	
11.	Root Cause Analysis	The solution should identify affected endpoints through on-demand investigations and fully customizable monitoring. Integration with the endpoint cloud Sandbox provides a comprehensive set of threat details that can help administrators and information security experts respond effectively to attacks.	M	
		Must have a visualized root cause analysis (RCA) report	M	
		The solution should provide threat investigation capabilities.	M	
		The solution should be able to terminate a running process (or file) or isolate an endpoint as a response action to an ongoing attack investigation	M	
		The solution should provide a customized endpoint investigation. The solution should support IOC and YARA rules, which allow the creation, sharing, and re-use of existing threat information.	M	
	AI Capability	Must have embedded Cybertron AI framework that uses large language models (LLMs), curated datasets, and AI agents to analyze telemetry from native sensors and third-party sources, predicting threats before they materialize and delivering customer-specific recommendations	M	
All Requirements are Mandatory (P/F)			**P/F**	

Note: All bidders must meet the following mandatory technical specifications to be considered responsive in order to proceed to the next stage of evaluation. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirement. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	EMAIL SECURITY			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Product and Quantity	Email security licenses shall be deployed to 1000 mailboxes.	M	
2.	General Solution Requirements	Provide a SaaS platform with a simple, seamless integration to the M365 platform	M	
		The Solution Should Protect Office 365 email and other cloud file-sharing and collaboration services	M	
		The solution should discover unknown malware using multiple patternless techniques, including machine learning and sandbox analysis.	M	
		The solution must detect ransomware and other malware hidden in Office file formats or PDF documents	M	
3.	Business Email Compromise	The solution must identify business email compromise (BEC) attacks using artificial intelligence (AI), including expert systems and machine learning, to analyze email headers, content, and authorship, while applying more stringent protections for high-profile users.	M	
		The solution must prevent executive spoofing scams by using Writing Style DNA to detect impersonations of high-profile users (such as the CEO, VP, or GM). It analyzes the writing style of a suspicious email and compares it to an AI model of that user's writing.	M	
4.	Sandboxing	The Solution Should provide built-in sandbox malware analysis with multiple operating systems and extensive anti-evasion technology	M	
5.	Retro Scan	The solution must protect internal email and allow manual scans to uncover attacks already in progress.	M	
6.	Computer Vision	The solution must prevent credential phishing by blocking URLs that masquerade as legitimate logon websites.	M	
7.	Data Loss Prevention	The solution should give visibility into sensitive data use with cloud file-sharing services	M	
	Embedded NIC	The solution should provide Data Loss Prevention (DLP) and advanced malware protection for Box, Dropbox, Google Drive, SharePoint, OneDrive, and Teams.	M	

	EMAIL SECURITY			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
		The solution should discover compliance data in existing stored files and emails by scanning databases.	M	
		The solution must have pre-built compliance templates, user/group policies, and support for Microsoft® Rights Management services.	M	
8.	Systems Management	The solution must provide direct cloud-to-cloud integration for high performance and scalability, without relying on email redirection or web proxies.	M	
9.	Email-Based AI	Must have AI-powered credential phishing and brand impersonation detection using computer vision to analyze login page images and visual patterns, identifying visually deceptive websites in real time	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

Note: All bidders must meet the mandatory technical specifications for the storage array. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	SERVER SECURITY			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Product and Quantity	Server Security licenses shall be deployed to 100 Servers (VMs and Physical Servers included)	M	
2.	General Requirements	The solution must provide a single platform for complete server protection over physical, virtual & cloud	M	
		Complete protection from a single integrated platform: addresses all of the 'Gartner top ten server security priorities'.	M	
		Provides layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.	M	
		The solution must be able to support cloud server and physical server protection	M	
		The proposed solution provides self-defending servers, with multiple integrated modules below providing a line of defense at the server	M	
		The Anti-Malware, Firewall, and Deep Packet Inspection can be deployed using a single agent or virtual appliance on the ESXi host for virtual desktops protection.	M	
		The proposed solution must be able to provide antimalware and virtual patching capabilities in a single agent	M	
		The dashboard must be configured by the administrator to display the information that is required only	M	
		The proposed solution must have a web-based management system for administrators to access using web browsers	M	
		Providing "Alerts" on the main menu to view administrator notifications concerning system or security events.	M	
3.	Anti-Malware & Machine Learning	Must be able to provide file reputation with variant protection that looks for obfuscated, polymorphic by using fragments of previously seen ad detection algorithms	M	
		The proposed solution must be able to provide Web Reputation filtering to protect against malicious websites for virtual desktops	M	
		Must be capable of doing predictive machine learning as below, complementing behavior analysis	M	
		i) Pre-execution	M	
		ii) Run-time execution	M	
4.	Intrusion Prevention	Must be able to provide HIPS/HIDS feature that immediately protects against vulnerabilities like Shellshock, Heartbleed, or WannaCry	M	
		Must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations	M	

	SERVER SECURITY			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
		Must be ABLE to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities	M	
		Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred	M	
		Must be able to provide protection against known and zero-day attacks (Please explain)	M	
5.	Intrusion Prevention	Must assists compliance (PCI DSS) to protect web applications and the data they process	M	
		Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot	M	
6.	Intrusion Detection	Provide virtual patching which shield vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs within minutes	M	
		Must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours	M	
7.	Application Control	The proposed solution must be able to lock down software and unwanted application execution to continuously monitor for software changes on protected servers	M	
8.	Supported Platform	Shall Support Platform, including: Microsoft Windows Server, Virtual (Vmware, Citrix, Microsoft HyperV), Linux(RedHat, SUSE, Centos, Cloud Linux, Debian, Oracle, Amazon Linux)	M	
9.	Security Compliance	Provides out-of-the-box compliance support for: PCI DSS 2.0, NIST, HIPAA, SOX, ISO 2700x, SAS70	M	
10.	3rd Party Validation	The proposed solution MUST be positioned as a leader in vulnerability research by the latest Omdia reports	M	
		Leader in Threat Intelligence for Strength of Vulnerability Research	M	
		The proposed solution MUST be in the latest Gartner MQ leadership position for more than 5 years	M	
	Artificial Intelligence capability	Must have AI-based behavioral analysis and anomaly detection that baselines normal endpoint and network activity, then detects deviations such as unusual process behavior, privilege changes, or data exfiltration patterns	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

PART E: MANDATORY TECHNICAL REQUIREMENTS FOR CYBER RISK EXPOSURE MANAGEMENT – LOT 2

Note: All bidders must meet the mandatory technical specifications for Cyber Risk Exposure Management(CREM). The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Cyber Risk Exposure Management (CREM)			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Quantity	Lot	M	
2.	General requirements	Solution should be able to continuously identify, categorize and document all the assets within the organization's digital ecosystem. Assets should be listed and categorized but not limited to the following asset categories: • Internet-facing Assets • Internal device Assets • Account Assets Application Assets.	M	
3.	Visibility	Solution should provide contextual visibility into all assets by: •Criticality based on asset attribute and activity. •Graphical presentation of the relationship of assets Historical risk assessment result.	M	
4.	Management	The solution should be able to manage all discovered assets from a single unified management console.	M	
5.	Integration	The solution should be able to integrate with a cybersecurity platform that manages the organization's Endpoint, Email, Cloud, Network, OT Security, XDR, and zero-trust solutions in a single console.	M	
6.	Attack Prediction	The solution should provide attack-path functionality to identify and predict potential attacks from external to internal critical assets. The solution should include built-in support for security playbooks for automated remediation.	M	
7.	External Attack Surface Management	Solution should be able to assess the security posture of the Internet and other external-facing assets in the organization	M	
8.	Risk Assessment	The solution should provide an organization-wide risk score based on continuous risk assessment across the organization.	M	

	Cyber Risk Exposure Management (CREM)			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
9.	Exposure Index	The solution should provide an exposure index score that summarizes the likelihood of an exploit or threat occurring in the environment, and a security configuration index score that summarizes deployed and missing security controls within the environment.	M	
10.	External Attack Surface Management	The solution should provide risk assessment for each domain and IP address asset and assign a risk score that can be monitored over time. Display risk indicators, including risk type, events, and risk level, for each discovered risk.	M	
11.	Device Assets	Provide risk assessment for each device asset and assign a risk score that can be monitored over time. Display risk indicators, including risk type, events, and risk level, for each discovered risk.	M	
12.	Accounts/ Identity Assets	Should be able to provide the account's latest risk score, user type, role, location, job title, and when the account was first and last seen, and enumerate exposed APIs connected to discovered service accounts.	M	
13.	Application Assets	Identify both Cloud and Local Applications, and provide the risk level	M	
14.	Vulnerability Management	Provides vulnerability management metrics for both internal and Internet-facing assets over time and can compare the organization's score to the global average. Metric: Mean Time to Patch	M	
15.	Remediation & Mitigation	Automate and orchestrate response actions to mitigate risks and respond to threats using advanced AI and ML technologies.	M	
16.	Reports & Dashboards	Provides insights into the organization's security posture using an executive-level dashboard. Must be able to show the company's overall risk score, individual asset risks, a view of ongoing attacks, and its contributing risk factors.	M	
17.	Zero Trust capability	Must have risk control rules to manage user accounts and devices based on risk scores and behavioral indicators, with the ability to block access dynamically under preset conditions	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

PART F: MANDATORY TECHNICAL REQUIREMENTS FOR CYBERSECURITY THREAT DEFENSE – LOT 2:

Note: All bidders must meet the mandatory technical specifications for Cybersecurity Threat Defense. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	CYBERSECURITY THREAT DEFENSE			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Quantity	Lot	M	
2.	Telemetry sources	The solution must collect and correlate data across email, endpoint, servers, cloud workloads, and networks, enabling visibility and analysis that is difficult or impossible to achieve otherwise.	M	
3.	Technique	The solution must apply effective AI and expert analytics to the activity data collected from native sensors in the environment to produce fewer, higher-fidelity alerts.	M	
4.	Prioritized Alerts	The solution is a single platform that provides:	M	
		Prioritized alerts based on one expert alert schema to interpret data in a standard and meaningful way	M	
		A consolidated view to uncover events and the attack path across security layers	M	
		Guided investigations to understand the impact and identify the path to resolution	M	
5.	Threat Detection	The solution must detect and respond to threats across multiple layers and gain greater context for better understanding.	M	
		The solution must identify activity that may not seem suspicious on its own suddenly becomes a high-priority alert, allowing the company to contain its impact faster	M	
6.	Threat Intelligence	The solution must detect more with built-in security analytics combined with global threat intelligence.		
		The solution's XDR analytics must automatically tie together a series of lower-confidence activities into a higher-confidence event, surfacing fewer prioritized alerts for action		
		The solution must correlate threat and detection data from the company environment with Global Threat Intelligence Network for richer, more meaningful alerts		
		The solution must provide context with mapping to the MITRE ATT&CK framework for faster detection and higher fidelity alerts		
7.	Security Analyst's Workbench	The solution must be one platform to respond faster with less resources.		
		The solution must contain threats more easily, assess the impact, and action the response across email, servers, cloud workloads, and networks		
		The solution must be one source of prioritized alerts, based on one expert alert schema to interpret data in a standard and meaningful way		
		The solution must be one place for investigations to quickly visualize the entire chain of events across security layers or drill down into an execution profile or network traffic analysis		
		The solution must be one location to respond using containment actions for email, cloud/server workloads, and networks		

	CYBERSECURITY THREAT DEFENSE			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
		The solution must provide prioritized view of threats across the company by correlating threats across the organization and adding expert threat intelligence, AI, and big data analytics, security personnel will get fewer, more meaningful, and richer alerts - prioritized by severity.		
		The solution must provide more effective analysis with native integration into email, servers, cloud environments, and networks, XDR sensors benefit from a deep understanding of data sources. This results in more effective analytics, compared to having thirdparty integration through application programming interfaces (APIs).		
		The solution must provide clearer contextual view of threats by viewing more contextual alerts across more threat vectors, events that seem benign on their own suddenly become meaningful indicators of compromise.		
		The solution must allow the company to connect more dots into a single view, enables more insightful investigations, and gives you the ability to detect threats earlier.		
		The solution must reduce time to detect and stop threats by collapsing the time it takes to detect, contain, and respond to threats, minimizing the severity and scope of impact		
		The solution must provide increased effectiveness and efficiency of threat investigation by automatically correlating threat data from multiple sources, XDR speeds up and removes manual steps involved in investigations and enables security analysts to quickly find the story of an attack.		
8.	Alerts	The solution must provide one place for investigation to achieve an attack-centric view of an entire chain of events across security layers		
		The solution must provide the ability to run a root cause analysis, look at the execution profile of an attack (including associated MITRE ATT&CK TTPs), and identify the scope of impact across assets		
9.	Customer Service Platform	Vendor Should provide the Customer Service Platform which gives the complete visibility of the infrastructure including but not limited to Health of the product, Advisories, Threat Intelligence, IOCs, Raw Logs.		
10.	Threat Advisories	The vendor should have their inhouse threat intelligence platform which can integrate threat intelligence feeds from different sources and should also support STIX, TAXII integration.		
		The vendor should provide the notification and IOCs based advisories including but not limited to Global, regional and Industrial Specific Threat Advisories.		
		Vendor should provide proactive automatic IOC sweeping across infrastructure.		
11	Threat Hunting	The vendor should provide IOC and hypothesis-based threat hunting at least twice a month.		
All Requirements are Mandatory (Pass/Fail)			**P/F**	

Part G: Network Access Control (NAC) – LOT 2:

Note: All bidders must meet the mandatory technical specifications for the storage array. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
1.	Software	Supply of 2000 license to implement NAC with three-year warranty	M	
2.	Project Services Implementation	• Conducting Business Requirement Mapping • Preparation of architecture design, documentation and project plan for implementation. • Installation & Configuration of the supplied software associated Software and System Integration. • Development of appropriate security incidence response procedures in alignment with related policies. • Training on the NAC solution administration to Four ICT Staff • Handing over of final configuration document.	M	
3.	Policy lifecycle management	Enforces policies for all operating scenarios without requiring separate products or additional modules		
4.	Profiling and visibility	Recognizes and profiles users and their devices before malicious code can cause damage		
5.	Guest networking access	Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal.		
6.	Security posture check	Evaluates security-policy compliance by user type, device type, and operating system.		
7.	Incidence response	Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention.		
8.	Bidirectional integration	Integrate with other security and network solutions		
		Must be supplied as virtual appliances/Software (on-prem/cloud)		
		Must support agentless scanning of network for detection and classification of devices		
		Must create an inventory of all devices on the network		
		Must support event reporting to SIEM with detailed contextual data to reduce investigation time		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		Must assess risk of every endpoint on the network		
		Must support subscription-based licensing model		
		Must automate onboarding process for large number of endpoints, users and guests		
		Must enforce dynamic network access control and enable network segmentation		
		Must reduce containment time from days to seconds		
		Must support multiple canned reports for network reporting, compliance, and analysis		
		Must form a security integration with the proposed firewalls for automated quarantine of infected hosts		
		Must support legacy network access devices that do not support RADIUS		
		The solution must support major hypervisors including VMWare and Hyper-V		
		Must be able to scale to 15,000 concurrent users per VM		
		Must be licensed with at least 1000 concurrent user/device licenses		
		Must support at least 12GB RAM		
		Must support at least 1TB of attached storage		
		The proposed VM appliances must be deployed in high availability for high availability		
		The proposed VM appliances must be deployed centrally in the datacenter without any requirement of having different appliances across branch sites		
9.	***Visibility:***	Must support Network Discovery		
		Must support both agentless and persist agent deployments		
		Must support User and Device Domain Authorization		
		Must support User and Device Captive Portals		
		Must support Rogue Endpoint Identification		
		Must support Device Profiling and Classification		
		Must support MDM Integration		
10.	***Automation / Control***	Must support Network Access Policies		
		Must support BYOD Onboarding		
		Must support Advanced Guest Management		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		Must support IoT Onboarding with Sponsor Authorization		
		Must support Endpoint Compliance		
		Must support automated Rogue Device Detection & Restriction		
		Must support Web & Firewall Single Sign On		
		Must support Firewall Segmentation		
11.	***Incident Response***	Must support Event Correlation		
		Must support Extensible Actions & Audit Trail		
		Must support Alert Criticality & Routing		
		Must support Guided Triage Workflows		
12.	***Integrations***	Must support Inbound Security Events		
		Must support REST API		
13.	***Reporting***	Must support live reporting		
		Must support historical analysis		
14.	**System Features:**	Must support Role-Based-Access-Control.		
		The solution must support secure management protocols (e.g. HTTPS, SSH)		
		The solution must support advanced auditing capabilities		
		Processes running on the device or operating system		
		The solution must provide e-mail alerting for administrative alerts		
		The solution must support configuration backup/restore		
		The solution must support common external authentication mechanisms for administrators (e.g.LDAP, AD, RADIUS, etc.)		
15.	**Policy Requirements:**	The solution must be able to classify assets on the network based on categories (e.g. Windows, Linux Mobile, etc.)		
		The solution must collect detailed asset information (E.g. MAC address, Logged on user, OS, NIC vendor, Switch Port, etc.)		
		The solution must be able to prevent network access from unauthorized and/or non-compliant devices (e.g.: BYOD device, device without Antivirus running)		
		The solution must provide captive portal abilities for guest device self-registration		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		The solution must provide captive portal abilities for BYOD devices via corporate logon credentials (e.g. AD, LDAP)		
		The solution must be able to detect/prevent ARP spoofing		
		The solution must be able to detect/prevent device dual-homing (e.g. wired + wireless access)		
		The solution must be able to detect/prevent malicious hosts		
		The solution must be able to detect Windows Update compliance		
		The solution must be able to detect Antivirus Update compliance		
		The solution must be able to detect endpoint firewall compliance		
		The solution must be able to detect/prevent external storage media & peripherals (e.g. USB flash drives webcams, etc.)		
		The solution must be able to detect custom attributes of devices (e.g. script output, WMI, registry, file attributes, running processes, etc.)		
		The solution must be able to quarantine devices based on policy (e.g. Switch port block, virtual firewall)		
		The solution must support administrative reversal of policy actions (e.g. unquarantined device)		
		The solution must support manual administrative actions (e.g. quarantine device, re-evaluate policies,		
16.	***Mandatory Integration Requirements:***	The solution must integrate with common router/switch vendors (e.g. Cisco, Brocade)		
		The solution must integrate with common AV/EDR vendors (e.g. Sophos, Crowdstrike, Carbon Black Symantec)		
		The solution must integrate with common firewall vendors (e.g. Palo Alto, Fortinet, Check Point)		
		The solution must integrate with common Anti- malware vendors (e.g. FireEye)		
		The solution must integrate with common Wi-Fi vendors (e.g. Ruckus, Cisco, UniFi, Aruba)		
		The solution must integrate with common mobile device management (MDM) vendors (e.g. Airwatch, Mobile Iron, Citrix)		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		The solution must integrate with common vulnerability assessment vendors (e.g. Qualys Rapid7)		
17.	***Mandatory Reporting Requirements:***	The solution must include pre-built report templates (e.g.: device policy compliance)		
		The solution must support custom reports		
		The solution must support scheduled reports		
18.	**Vendor Requirements**	The vendor must be PECB MS Certified (ISMS)		
		The vendor lead engineer must be certified by the OEM as a system administrator or implementor		
		The vendor must provide proof of having engaged in similar NAC projects		
19.	**Technical Training**	The bidder should describe how they shall meet the requirements for NAC technical training. The requirements are as follows: - a. The exercise shall take a period of Five (5) days. b. Six (6) KCAA ICT staff shall be trained. This shall be undertaken at a fully accredited Vendor training centre with all the requisite labs, simulators and facilities. c. All the applicable costs for this activity shall be borne by the vendor. These include but not limited to economy air tickets, VISA fees, subsistence allowance and other applicable costs.	M	
20.	**Operational Testing and Knowledge transfer**	The bidder should describe how they shall meet the requirements for operational testing and knowledge.	M	
21.	**Go-LIVE and Commissioning**	The bidder should describe how they shall meet the requirements for go-live and commissioning.	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

Part H: Project Implementation Services – LOT 2:

Note: All bidders must meet the mandatory technical specifications for the Renewal of Cybersecurity Infrastructure . The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Upgrades and Other Services			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
1.	Project Management	a. Mandatory letter to KCAA providing assurance that the project will be completed in three (3) months after contract award. b. A Comprehensive Project Implementation Plan MUST be attached. c. Details of the Project Manager. i. Attach CV. ii. Copies of PMP or Prince 2 certifications. iii. The project manager MUST have implemented at least three (3) successful projects. d. The bidder to provide sample documents of the proposed project implementation documents. These are; Project Charter, Sample Project Initiation Document and Sign-Offs.	M	
2.	Integration with existing environment	a. The bidder MUST integrate the existing environment with the proposed environment. b. The bidder is expected to provide a technical proposal of how to undertake this integration.	M	
3.	Technical Certified Training	The bidder should describe how they shall meet the requirements for technical training. The requirements are as follows: - a. The exercise shall take a period of ten (10) working days. b. The training shall entail the following key areas; Cybersecurity Policies, Solutions, Design and Implementation. c. Six (6) KCAA ICT staff shall be trained. This shall be undertaken at a fully accredited OEM training centre with all the requisite labs, simulators and facilities. d. All the applicable costs for this activity shall be borne by the vendor. These include but not limited to economy air tickets,	M	

	Upgrades and Other Services			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		VISA fees, subsistence allowance and other applicable costs.		
4.	Operational Testing and Knowledge transfer.	The bidder should describe how they shall meet the requirements for operational testing and knowledge transfer. The requirements are as follows: - a. The exercise shall take a period of five (5) days. b. This bidder shall propose a detailed schedule for the five (5) days including knowledge transfer and training. c. The quality assurance, testing and training should entail; Inspection of installations works, centralized useability and management, robust monitoring and reporting. d. Eight (8) KCAA ICT staff shall be trained. This shall be undertaken at a serene environment out of town. e. All the applicable costs for this activity shall be borne by the vendor. f. These include but not limited to conferencing, subsistence allowance and other applicable costs.	M	
5.	Go-LIVE and Commissioning	The bidder should describe how they shall meet the requirements for go-live and commissioning. The requirements are as follows: - a. The exercise shall take a period of one (1) day immediately after operational testing and knowledge transfer.	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

Note: All bidders must meet the mandatory technical specifications for SLA. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	SLA			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
1.	Maintenance and Support Term	The maintenance and support period is three (3) years backed by OEM	M	
2.	Items to be maintained and supported	The Security Infrastructure and all its components.	M	
3.	Preventive Maintenance	Health checks for all components (hardware, firmware and software) and preventive maintenance to be undertaken once every quarter for the three (3) year period. Status reports to be provided to KCAA indicating the status of each maintenance item.	M	
4.	Corrective Maintenance	a. To be undertaken immediately if a maintenance component fails. Items to be replaced under the OEM. b. Where downtime is required, this shall be arranged with the KCAA systems administration team for approval prior to the required downtime.	M	
5.	Outage Severity Levels and Required Response Times	a. **Severity One/Red:** KCAA is unable to do their business as a result of complete or partial system failure. This has a major impact on the KCAA's business operations. Response: The vendor should respond within one (1) hour. A resolution or a workaround should be provided within two (2) hours. b. **Severity Two/Orange:** The problem has high visibility and impacts on the way KCAA does business. The ARMS service is disrupted but not halted. The system performance may be degraded, or functions limited. Response: The vendor should respond within three (3) hours. A resolution or a workaround should be provided within twelve (12) hours. c. **Severity Three/Green:** A single component or several components are affected with or without a work around. The problem may affect KCAA's efficiency but is limited in visibility and does not prevent work from being completed. Response: The vendor should respond within twelve (12) hours. A resolution or a workaround should be provided within seventy-two (72) hours.	M	
6.	Fault Logging Procedure and Reporting	a. The vendor to provide a support service desk email and a telephone number manned 24/7 for logging faults and a fault should be allocated a reference number for ease of tracking. b. Response to faults logs shall be undertaken as per the response times based on severity levels.	M	

	SLA			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		c. Once a red or orange level fault is resolved, a report should be provided entailing the following: - i. The root cause analysis ii. The measures taken to resolve it iii. The measures taken to ensure it does not recur		
7.	Escalations	The vendor shall provide two escalation levels after a fault is reported and left unattended. Phone numbers and email addresses of the escalation levels shall be required. The levels are as follows: - a. Level 0 – Normal helpdesk reporting after a fault. b. Level 1 – Technical manager or service provision manager after the response times for resolution are not met. c. Level 2 – The CEO after the required response times are not met after escalating to level 2.	M	
8.	Maintenance and Support Services	a. Ensuring uptime of all security systems. b. Maintenance and support should include security appliance and related accessories. c. Consultation for guidance on complex procedures and processes in configuration and integration of the Solution. d. Assistance in configuration of the Solution in case of failure of any part of the System. e. Configuration of the Solution to optimize performance. f. Support and assistance on matters concerning security upgrades and any Service Pack installations. g. Bugs and Errors resolution as far as the security software is concerned. h. Receive, classify, log and track all reported issues and provide case updates until the issues is conclusively resolved. i. Provide urgent security alerts on the version deployed by the client. j. Troubleshooting and provide workarounds assistance where existing system cannot perform some of the tasks. k. Installation and configuration advice to KCAA ICT technical staff. l. Answering questions and providing a reasonable level of guidance to KCAA about the Security Solutions. m. Provide trained Technical Support personnel to handle inquiries and problems. n. Provide documentation updates and major system releases information. o. Provide pro-active maintenance release announcements sent to customer directly. p. Participate in failover and failback tests for the KCAA remote disaster recovery site.	M	

	SLA			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
9.	Infrastructure Upgrades	Occasionally the Authority will make plans for replacement of the infrastructure. The vendor will be required to: - a. Make recommendations for security infrastructure b. Undertaking infrastructure upgrades as requested by KCAA.	M	
10.	SLA Payments	Payments pertaining the three-year SLA shall be paid semi-annually in arrears after invoicing and provision of SLA (maintenance and support) reports applicable for the payment period. The detailed and signed reports shall be provided by the bidder.	M	
11.	Sample SLA	The vendor shall provide a sample SLA that meets all the above provisions for adoption in the contract.	M	
12.	SLA penalties	Core services are provided 24 hours a day by the Authority. The Authority expects the infrastructure to be available 99.95% of the time per annum. The vendor will be penalized in cases of protracted downtime. This will be calculated by factoring in the number of hours constituting to 99.95% per year, the applicable amount per hour and the number of hours the system has been unavailable within a particular payment period.	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

FINANCIAL EVALUATION:

The winning bidder will be the lowest evaluated responsive bidder having been substantially responsive to the bidding document among those who will have passed the mandatory preliminary evaluation and mandatory technical evaluation as outlined above in the mandatory and technical mandatory requirements except where other conditions are not met as specified in the tender document.

NOTE: The award of tender will be based on EACH LOT on the lowest evaluated responsive bidder.

SECTION IV - TENDERING FORMS

The bidder shall be required to fill the following forms attached.

1. Duly filled, signed and stamped Form of Tender
2. Submit dully filled and signed confidential questionnaire
3. Submit a duly filled and signed Certificate of Independent Tender Determination.
4. Submit a duly filled and signed Self Declaration of the Tenderer (Form SD1 & SDA2)
5. Declaration and commitment to the code of ethics.
6. Tender information form
7. Price schedules

1. FORM OF TENDER

INSTRUCTIONS TO TENDERERS

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

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

iii) Tenderer must complete and sign CERTIFICATE OF INDEPENDENT TENDER DETERMINATION and the SELF DECLARATION OF THE TENDERER attached to this Form of Tender.

iv) TheFormofTendershallincludethefollowingFormsdulycompletedandsignedbytheTenderer.

a) Tenderer's Eligibility-Confidential Business Questionnaire

b) Certificate of Independent Tender Determination

c) Self-Declaration of the Tenderer

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

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

Alternative No.:_____[*insert identification No if this is a Tender f or an alternative*] To:_____**[*insert complete name of Procuring Entity*]**

a) **No reservations:** We have examined and have no reservations to the tendering document, including Addenda issued in accordance with ITT9;

b) **Eligibility**: We meet the eligibility requirements and have no conflict of interest in accordance with ITT4;

c) **Tender-Securing Declaration:** We have not been suspended nor declared ineligible by the Procuring Entity based on execution of a Tender-Securing Declaration or Proposal-Securing Declaration in Kenya in accordance with ITT21;

d) **Conformity:** We offer to provide the Non-Consulting Services inconformity with the tendering document of the following:[*insert a brief description of the Non-Consulting Services*];

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

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

Or

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

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

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

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

g) **Tender Validity Period:** Our Tender shall be valid for the period specified in TDS 19.1 (as amended if applicable) from the date fixed for the Tender submission deadline (specified in TDS 23.1(as amended if applicable),and it shall remain binding upon us and may be accepted at any time before the expiration of that period;

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

i) **One Tender Per Tenderer:** We are not submitting any other Tender(s) as an individual Tenderer, and we are not participating in any other Tender(s) a s a Joint Venture member or as a subcontractor, and meet the requirements of ITT4.3, other than alternative Tenders submitted in accordance with ITT14;

j) **Suspension and Debarment**: We, along with any of our subcontractors, suppliers, consultants, manufacturers,orserviceprovidersforanypartofthecontract,arenotsubjectto,and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the PPRA. Further, we are not ineligible under Kenya's official regulations or pursuant to a decision of the United Nations Security Council;

k) **State-owned enterprise or institution**: [*select the appropriate option and delete the other*] [*We are not a state-owned enterprise or institution*] / [*We are a state-owned enterprise or institution but meet the requirements of ITT 4.6*];

g) **Commissions, gratuities and fees**: We have paid, or will pay the following commissions, gratuities, or fees with respect to the Tendering process or execution of the Contract: *[insert complete name of each Recipient, its full address, r gratuity].*

Name of Recipient	Address	Reason	Amount

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

*a) [Delete if not appropriate, or amend to suit]*We confirm that we understand the provisions relating to Standstill Period as described in this tendering document and the Procurement Regulations.

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

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

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

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

q) **Code of Ethical Conduct:** We undertake to adhere by the Code of Ethics for Persons Participating in Public Procurement and Asset Disposal, copy available from_____(*specify website*) during the procurement process and the execution of any resulting contract.

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

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

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

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

iv) Declaration and commitment to the Code of Ethics for Persons Participating in Public Procurement and Asset Disposal.

Further, we confirm that we have read and understood the full content and scope of fraud and corruption as informed in **"Appendix 1- Fraud and Corruption**" attached to the Form of Tender.

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

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

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

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

Date signed..... [*insert date of signing*] **day of** .....[*insert month*], [*insert year*]

2. TENDERER'S ELIGIBILITY - CONFIDENTIAL BUSINESS QUESTIONNAIRE

Instruction to Tenderer

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

a) Tenderer's details

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

General and Specific Details

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

Name in full_____Age_____

Nationality_____Country of Origin_____

Citizenship _____

Partnership, provide the following details.

	Names of Partners	Nationality	Citizenship	% Shares owned
1				
2				
3				

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

i) Private or public Company _____

ii) State the nominal and issued capital of the Company-

Nominal Kenya Shillings (Equivalent) …….....…....

Issued Kenya Shillings (Equivalent) …….....…

iii) Give details of Directors as follows.

	Names of Director	Nationality	Citizenship	% Shares owned
1				
2				
3				

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

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

If yes, provide details as follows.

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

ii) Conflict of interest disclosure

	Type of Conflict	Disclosure YES OR NO	If YES provide details of the relationship with Tenderer
1	Tenderer is directly or indirectly controlled by or is under common control with another tenderer.		
2	Tenderer receives or has received any direct or indirect subsidy from another tenderer.		
3	Tenderer has the same legal representative as another tenderer		

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

f) Certification

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

Full Name_____

Title or Designation_____

_____ _____

(Signature) *(Date)*

3. CERTIFICATE OF INDEPENDENT TENDER DETERMINATION

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

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

1. I have read and I understand the contents of this Certificate;
2. I understand that the Tender will be disqualified if this Certificate is found not to be true and complete in every respect;
3. I am the authorized representative of the Tenderer with authority to sign this Certificate, and to submit the Tender on behalf of the Tenderer;
4. For the purposes of this Certificate and the Tender, I understand that the word "competitor" shall include any individual or organization, other than the Tenderer, whether or not affiliated with the Tenderer, who:
   a) Has been requested to submit a Tender in response to this request for tenders;
   b) could potentially submit a tender in response to this request for tenders, based on their qualifications, abilities or experience;
5. The Tenderer discloses that [check one of the following, a s applicable]:
   a) The Tenderer has arrived at the Tender independently from, and without consultation, communication, agreement or arrangement with, any competitor;
   b) the Tenderer has entered into consultations, communications, agreements or arrangements with one or more competitors regarding this request for tenders, and the Tenderer discloses, in the attached document(s), complete details thereof, including the names of the competitors and the nature of, and reasons for, such consultations, communications, agreements or arrangements;
6. In particular, without limiting the generality of paragraphs(5)(a) or (5)(b) above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:
   a) prices;
   b) methods, factors or formulas used to calculate prices;
   c) the intention or decision to submit, or not to submit, a tender; or
   d) the submission of a tender which does not meet the specifications of the request for Tenders; except as specifically disclosed pursuant to paragraph (5) (b) above;
7. In addition, there has been no consultation, communication, agreement or arrangement with any competitor regarding the quality, quantity, specifications or delivery particulars of the works or services to which this request for tenders relates, except as specifically authorized by the procuring authority or as specifically disclosed pursuant to paragraph (5)(b) above;
8. The terms of the Tender have not been, and will not be, knowingly disclosed by the Tenderer, directly or indirectly, to any competitor, prior to the date and time of the official tender opening, or of the awarding of the Contract, which ever comes first, unless otherwise required by law or as specifically disclosed pursuant to paragraph (5) (b) above.

Name_____

Title_____

Date

_____

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

4. SELF-DECLARATION FORMS

FORM SD1

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

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

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

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

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

…….	…….	……
(Title)	(Signature)	(Date)

Bidder Official Stamp

FORM SD2

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

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

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

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

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

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

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

…… ……..……. .....

(Title) (Signature) (Date)

Bidder's Official Stamp

5. DECLARATION AND COMMITMENT TO THE CODE OF ETHICS

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

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

Name of Authorized signatory.....

Sign…….....….....

Position…….....

Office address……. Telephone…….....

E-mail…….....

Name of the Firm/Company…….....

Date…….....

(Company Seal/ Rubber Stamp where applicable)

Witness

Name…….....

Sign…….....

Date…….....

ii) APPENDIX1-FRAUDANDCORRUPTION

(Appendix 1 shall not be modified)

1. Purpose

1.1 The Government of Kenya's Anti-Corruption and Economic Crime laws and their sanction's policies and procedures, Public Procurement and Asset Disposal Act *(no. 33 of 2015)* and its Regulation, and any other Kenya's Acts or Regulations related to Fraud and Corruption, and similar offences, shall apply with respect to Public Procurement Processes and Contracts that are governed by the laws of Kenya.

2. Requirements

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

2.2 Kenya's public procurement and asset disposal act *(no. 33 of 2015)* under Section 66 describes rules to be followed and actions to be taken in dealing with Corrupt, Coercive, Obstructive, Collusive or Fraudulent practices, and Conflicts of Interest in procurement including consequences for offences committed. A few of the provisions noted be low highlight Kenya's policy of no tolerance for such practices and behavior:

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

2) A person referred to under sub section (1) who contravenes the provisions of that sub-section commits an offence;

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

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

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

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

3. An employee or agent of the procuring entity or a member of the Board or committee of the procuring entity who has a conflict of interest with respect to a procurement: -

a) Shall not take part in the procurement proceedings;

b) shall not, after a procurement contract has been entered into, take part in any decision relating to the procurement or contract; and

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

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

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

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

a) Defines broadly, for the purposes of the above provisions, the terms 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 investigation by Public Procurement Regulatory Authority (PPRA) or any other appropriate authority appointed by Government of Kenya into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or

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

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

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

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

d) Pursuant to the Kenya's above stated Acts and Regulations, may sanction or recommend to appropriate authority(ies) for sanctioning and debarment of a firm or individual, as applicable under the Act sand Regulations;

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

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

---

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

[2] *Inspections in this context usually are investigative (i.e., forensic) in nature. They involve fact-finding activities undertaken by the*

Investigating Authority or persons appointed by the Procuring Entity to address specific matters related to investigations/ audits, such as evaluating the veracity of an allegation of possible Fraud and Corruption, through the appropriate mechanisms. Such activity includes but is not limited to: accessing and examining a firm's or individual's financial records and information, and making copies 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 there of as relevant; interviewing staff and other relevant individuals; performing physical inspections and site visits; and obtaining third party verification of information.

6. TENDERER INFORMATION FORM

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

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

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

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

1. Tenderer's Name: .....*[insert Tenderer's legal name]*

2. In case of JV, legal name of each member: .....*[insert legal name of each member in JV]*

3. Tenderer's actual or intended country of registration: .....*[insert actual or intended country of registration]*

4. Tenderer's year of registration: .....*[insert Tenderer's year of registration]*

5. Tenderer's Address in country of registration: .....*[insert Tenderer's legal address in country of registration]*

6. Tenderer's Authorized Representative Information

   Name: .....*[insert Authorized Representative's name]*

   Address.....*[insert Authorized Representative's Address]*

   Telephone:.....*[insert Authorized Representative's telephone/fax numbers]*

   Email Address:.....*[insert Authorized Representative's email address]*

7. Attached are copies of original documents of..... *[check the box(es) of the attached original documents]*

   ☐ Articles of Incorporation (or equivalent documents of constitution or association), and/or documents of registration of the legal entity named above, in accordance with ITT 4.4.

   ☐ In case of JV, Form of intent to form JV or JV agreement, in accordance with ITT

   4.1. In case of state-owned enterprise or institution, in accordance with ITT4.6 documents

   establishing:

   i) Legal and financial autonomy
   ii) Operation under commercial law
   iii) Establishing that the Tenderer is not under the supervision of the agency of the Procuring Entity

   ☐ A current tax clearance certificate or tax exemption certificate in case of Kenyan tenderers issued by the Kenya Revenue Authority in accordance with ITT 4.14.

8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

7. PRICE SCHEDULE FOR LOT 1: THE PROVISION OF OFFICE SUITE SOFTWARE

TENDER NUMBER: - KCAA/018/2025-2026

NAME OF TENDER: - PROVISION OF OFFICE SUITE SOFTWARE

	NETWORK ACCESS CONTROL			
No	**Item Description**	**Quantity**	**Unit cost - Kshs.**	**Total Cost - Kshs.**
1.	Microsoft E5	10		
2.	Microsoft E3	300		
3.	Business Premium	300		
4.	Microsoft 365 Business Basic	300		
5.	Exchange Online Plan1	200		
6.	Copilot Access	20		
7.	Service Level Agreement	3 Years		
8.	Knowledge Transfer for 6 ICT staff	6		
Include capacity building Levy of 0.03% of the total contract sum				
Include Value Added Tax				
TOTAL PRICE IN KENYA SHILLINGS INCLUSIVE OF ALL APPLICABLE LEVIES AND TAXES TO BE TRANSFERRED TO THE FORM OF TENDER FOR LOT 1.				

PLEASE NOTE AND COMPLY WITH THE FOLLOWING:

i. All bidders to indicate the LOT being quoted for.
ii. Each LOT must have all the items quoted for it to considered responsive
iii. The contract will be awarded on each LOT to the lowest evaluated responsive bidders.
iv. In case of discrepancy between unit price and total, the unit price shall prevail.
v. Bidders must indicate prices in Kenya Shillings

Authorized Official:

Name **Signature, date and official stamp**

B) PRICE SCHEDULE FOR LOT 2: PROVISION OF ICT END POINT SECURITY INFRASTRUCTURE.

TENDER NUMBER: - KCAA/018/2025-2026.

NAME OF TENDER: - END POINT SECURITY:

	USER, EMAIL, SERVER SECURITY AND CYBER THREAT DEFENCE			
No	**Item Description**	**Quantity**	**Unit cost - Kshs.**	**Total Cost - Kshs.**
1.	Supply, installation and implementation of Endpoint Security (Endpoint Security Essentials)	1000		
2.	Supply, installation and implementation of Server Security(Endpoint Security Pro)	100		
3.	Supply, installation and implementation of Email Security(Email and Collaboration Security Essentials)	1000		
4.	Cybersecurity Threat Defense Services - SOC Essentials	Lot		
5.	Cyber Risk Exposure Management (CREM)(Cyber Risk Exposure Management Essentials (devices))	1100		
6.	Supply, Installation, and Implementation Network access Control System (NAC)	2000		
7.	Training – technical certified training and operational training.	Lot		
8.	Implementation and Professional Services	Lot		
9.	Service Level Agreement (SLA)	3 Years		
Include capacity building Levy of 0.03% of the total contract sum				
Include Value Added Tax				
TOTAL PRICE IN KENYA SHILLINGS INCLUSIVE OF ALL APPLICABLE LEVIES AND TAXES TO BE TRANSFERRED TO THE FORM OF TENDER FOR LOT 2.				

PLEASE NOTE AND COMPLY WITH THE FOLLOWING:

i. All bidders to indicate the LOT being quoted for.
ii. Each LOT must have all the items quoted for it to considered responsive
iii. The contract will be awarded on each LOT to the lowest evaluated responsive bidders.
iv. In case of discrepancy between unit price and total, the unit price shall prevail.
v. Bidders must indicate prices in Kenya Shillings

Authorized Official:

Name **Signature, date and official stamp**

8. NOTIFICATION OF INTENTION TO AWARD

[*This Notification of Intention to Award shall be sent to each Tenderer that submitted a Tender.*] [*Send this Notification to the Tenderer's Authorized Representative named in the Tenderer Information Form*]

For the attention of Tenderer's Authorized Representative

Name: .....*[insert Authorized Representative's name]*

Address: .....*[insert Authorized Representative's Address]*

Telephone numbers: .....*[insert Authorized Representative's telephone/fax numbers]*

Email Address:..... *[insert Authorized Representative's email address]*

[IMPORTANT: insert the date that this Notification is transmitted to Tenderers. The Notification must be sent to all Tenderers simultaneously. This means on the same date and as close to the same time as possible.]

DATE OF TRANSMISSION:..... This Notification is sent by: [*email/fax*] on [*date*] (local time)

Procuring Entity: .....*[insert the name of the Procuring Entity]*

Contract title:..... *[insert the name of the contract]*

ITT No: .....*[insert ITT reference number from Procurement Plan]*

This Notification of Intention to Award (Notification) notifies you of our decision to award the above contract. The transmission of this Notification begins the Standstill Period. During the Standstill Period you may:

a) Request a debriefing in relation to the evaluation of your Tender, and/or

b) Submit a Procurement-related Complaint in relation to the decision to award the contract.

I). The successful Tenderer

Name:	[*insert nameof successful Tenderer*]
Address:	[*insert addressof the successful Tenderer*]
Contract price:	[*insert contract priceof the successful Tender*]

ii). **Other Tenderers** ***[INSTRUCTIONS: insert names of all Tenderers that submitted a Tender. If the Tender's price was evaluated include the evaluated price as well as the Tender price as read out.]***

	Tender price	**Evaluated Tender price (if applicable)**
[*insert name*]	[*insert Tender price*]	[*insert evaluated price*]
[*insert name*]	[*insert Tender price*]	[*insert evaluated price*]
[*insert name*]	[*insert Tender price*]	[*insert evaluated price*]
[*insert name*]	[*insert Tender price*]	[*insert evaluated price*]

iii). How to request a debriefing

DEADLINE: The deadline to request a debriefing expires at midnight on [*insert date*] (local time).

You may request a debriefing in relation to the results of the evaluation of your Tender. If you decide to request a debriefing your written request must be made within three (3)Business Days of receipt of this Notification of Intention to Award.

Provide the contract name, reference number, name of the Tenderer, contact details; and address the request for debriefing as follows:

Attention: .....[*insert full name of person, if applicable*]

Title/position: .....[*insert title/position*]

Agency: .....[*insert name of Procuring Entity*]

Email address:..... [*insert email address*]

If your request for a debriefing is received within the3Business 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.

iv. How to make a complaint

Period: Procurement-related Complaint challenging the decision to award shall be submitted by [*insert date and time*].

Provide the contract name, reference number, name of the Tenderer, contact details; and address the Procurement-related Complaint as follows:

Attention:.....[*insert full name of person, if applicable*]

Title/position:..... [*insert title/position*]

Agency: .....[*insert name of Procuring Entity*]

Email address:..... [*insert email address*]

At this point in the procurement process, you may submit a Procurement-related Complaint challenging the decision to award the contract. You do not need to have requested, or received, a debriefing before making this complaint. Your complaint must be submitted within the Stand still Period and received by us before the Stand still Period ends. In summary, there are four essential requirements:

1. You must be an 'interested party'. In this case, that means a Tenderer who submitted a Tender in this tendering process, 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 period stated above.
4. You must include, in your complaint, all of the information required to support the complaint.
5. The application must be accompanied by the fees set out in the Procurement Regulations, which shall not be refundable (information available from the Public Procurement Authority at info@ppra.go.ke or complaints@ppra.go.ke

v). 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 as stated in Section 4 above.
If you have any questions regarding this Notification please do not hesitate to contact us.

On behalf of the Procuring Entity:

Signature:_____

Name:_____

Title/position:_____

Telephone:_____

Email: _____

9. NOTIFICATION OF AWARD -FORM OF ACCEPTANCE

[Form head paper of the Procuring Entity]

.....*[date]*

To:.....*[name and address of the Service Provider]*

This is to notify you that your Tender dated*[date]*forexecutionofthe*[nameoftheContractandidentificationnumber, as given in the Special Conditions of Contract]* for the Contract Price of the equivalent of *[amount in numbers and words] [name of currency]*, as corrected and modified in accordance with the Instructions to Tenderers is hereby accepted by us (Procuring Entity).

You are requested to furnish the Performance Security within 28days in accordance with the Conditions of Contract, using, for that purpose, one of the Performance Security Forms included in Section X, Contract Forms, of the tender document.

Please return the attached Contract dully signed

AuthorizedSignature:.....

Name and Title of Signatory:.....

Name of Agency:.....

Attachment: Contract

10. FORM OF CONTRACT

[Form head paper of the Procuring

Entity] **LUMP SUM**

REMUNERATION

This CONTRACT(herein after called the "Contract") is made the *[day]* day of the month of*[month]*,*[year]*, between, on the one hand,*[name of Procuring Entity]*(herein after called the "Procuring Entity") and, on the other hand, *[name of Service Provider]*(hereinafter called the" Service Provider").

[***Note****: In the text below text in brackets is optional; all notes should be deleted in final text. If the Service Provider consist of more than one entity, the above should be partially amended to read as follows:*"…(herein after called the "Procuring Entity") and, on the other hand, a joint venture consisting of the following entities, each of which will be jointly and severally liable to the Procuring Entity for all the Service Provider's obligations under this Contract, namely, *[name of Service Provider]*and*[name of Service Provider]*(herein after called the "Service Provider").]

WHEREAS

i) The Procuring Entity has requested the Service Provider to provide certain Services as defined in the General Conditions of Contract attached to this Contract (herein after called the "Services");

ii) the Service Provider, having represented to the Procuring Entity that they have the required professional skills, and personnel and technical resources, have agreed to provide the Services on the terms and conditions set forth in this Contract at a contract price of……;

NOW THEREFORE the parties hereto hereby agree as follows:

1. The following documents shall be deemed to form and be read and construed as part of this Agreement, and the priority of the documents shall be as follows:
   a) The Form of Acceptance;
   b) The Service Provider's Tender
   c) The Special Conditions of Contract;
   d) The General Conditions of Contract;
   e) The Specifications;
   f) The Priced Activity Schedule; and
   g) The following Appendices: [***Note****: If any of these Appendices are not used, the words "Not Used" should be inserted below next to the title of the Appendix and on the sheet attached hereto carrying the title of that Appendix*.]

   Appendix A: Description of the Services
   Appendix B: Schedule of Payments
   Appendix C: Subcontractors
   Appendix D: Breakdown of Contract Price
   Appendix E: Services and Facilities Provided by the Procuring Entity

2. The mutual rights and obligations of the Procuring Entity and the Service Provider shall be as set forth in the Contract, in particular:
   a) The Service Provider shall carry out the Services in accordance with the provisions of the Contract; and
   b) The Procuring Entity shall make payments to the Service Provider in accordance with the provisions of the Contract.

   INWITNESSWHERE OF, the Parties here to have caused this Contract to be signed in their respective names as of the day and year first above written.

   For and on behalf of_____*[name of Procuring Entity]*

   _____*[Authorized Representative]*

For and on behalf of *[name of Service Provider]*

_____*[Authorized Representative]*

[***Note*** *:If the Service Provider consists of more than one entity, all these entities should appear as signatories, e.g., in the following manner*:]

For and on behalf of each of the Members of the Service Provider

.....*[name of member]*

.....*[Authorized Representative]*

..... *[name of member]*

.....*[Authorized Representative]*

PART II – PROCURING ENTITY'S REQUIREMENTS

SECTION VII - ACTIVITY SCHEDULE

TECHNICAL SPECIFICATIONS FOR OFFICE SUITE SOFTWARE – UNDER LOT 1:

RENEWAL OF OFFICE 365

INTRODUCTION

The Kenya Civil Aviation Authority (KCAA) intends to engage the services of a qualified vendor to renew its Microsoft 365 subscription for a period of three (3) years to ensure uninterrupted access to communication, productivity, collaboration, security, and cloud-based services critical for daily operations.

This renewal will ensure staff continue to leverage advanced collaboration tools, enterprise security features and modern AI-driven productivity solutions provided under Microsoft 365.

(a) Mandatory Technical requirements

No.	Documents to be submitted	Bidders' response
1.	Local based Microsoft Authorized Licensing Solution Provider (LSP) or Cloud Solutions Provider (CSP) - Provide evidence	
2.	Bidders must have Microsoft Manufacturer's Authorization as a Microsoft Licensing Solution Provider (LSP) or Cloud Solutions Provider (CSP) - provide evidence	
3.	Provide evidence that the bidder has at least Four (4) Kenyan based Microsoft Technical Certified professionals to manage KCAA Microsoft environment from a Managed Services perspective. Include Microsoft Certification for each resource. *The bidder must undertake in writing to ensure that the proposed project team is maintained throughout the onboarding phase and commissioning of the new licenses.*	
4.	Experience in similar Microsoft products deployment assignments with three (3) corporate clients (Provide evidence of similar work done i.e. provide copies of Sign Off certificate/LSO/LPO/Contract documents): Attach the names, addresses and contact details of the corporate clients.	
5.	Bidder must submit Draft Service Level Agreement for support	
6.	Licenses must be genuine and verifiable via KCAA's Microsoft 365 Admin Center.	
7.	Licenses must be assignable seamlessly through the existing KCAA Microsoft 365 tenant.	
8.	Supplier to provide transition window and onboarding assistance where required	
9.	Renewal confirmation from Microsoft and access to Admin Center reporting.	

SLA SERVICES

NO	Requirement/tasks	Bidder's Response
General Support services		
1.	The maintenance and support period shall be three years (3) years.	
2.	Provision of 24/7 support on Microsoft 365 and its related products and systems	
3.	Provision of Onsite resources on schedule and on demand to resolve technical issues that may arise from time-to-time.	
4.	Maintenance of Office 365 Applications installed and used by KCAA staff	
5.	Support and enhancement of Microsoft Windows Active Directory Environment and on-premises Microsoft Entra ID	
6.	SharePoint Online development and support	
7.	Provision of escalation point for all Microsoft related problems that pertains to Office 365 Subscription Services	
Proactive Support		
1.	Scheduled Infrastructure health checks on key systems for Microsoft 365	
2.	Proactive diagnosis and prevent system problems in scope.	
3.	Carrying out day-to-day escalation duties for tasks in scope.	
4.	Sitting in project deliberations meetings where required.	
5.	Advice the KCAA technical team on best practices and procedures they can adopt to enable them increase Uptime and reduce incidents.	
6.	Provide reports for management consumption when required.	
7.	Generating quarterly reports for KCAA regarding service level performance	
8.	**Reviews** - There will be quarterly reviews of the system support carried out jointly by KCAA and the successful vendor.	
9.	The health reviews and optimization and maintenance of KCAA Microsoft 365 Infrastructure	
10.	Review of the Active Directory policies	
11.	Office 365 Policies and Best Practices	
12.	Ensure compliance with recommended security score on KCAA Microsoft 365 platform as per Policies and best Practices	

LOT 2: RENEWAL OF ICT SECURITY INFRASTRUCTURE

Technical Specifications for the Renewal of ICT Security Infrastructure

Cyber risks have become strategic imperatives due to their high negative impact on organizations globally. KCAA is focusing on building operational resilience beyond preventive security controls. Part of this strategy includes the acquisition and implementation of the following solutions:

i. End-Point Security
ii. Email Security
iii. Cybersecurity Threat Defense
iv. Cyber Risk Exposure Management (CREM)
v. Network Access Control (NAC) System
vi. Technical training for KCAA Staff
vii. OEM and SLA support and maintenance for the security systems.

These solutions will provide integrated end-to-end cover of the IT infrastructure and related services. The systems will autonomously monitor access to the core network, enforce policies, prevent network security breaches and network intrusion prevention and coordinate responses to network access threats detected across the network in a bid to ensure resilient operations

PART A: MANDATORY TECHNICAL DOCUMENTATION REQUIREMENTS

Note: All bidders must provide the following mandatory technical documentation to be considered responsive to proceed to the next evaluation stage. The bidder MUST provide detailed explanations of how they shall fully meet the required technical documentation. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Technical Documentation Required		
No.	**Item/Specification**	**Requirement**	**Bidder's Response**
1.	Manufacturer's Authorizations	The bidder MUST provide the manufacturer's authorizations for the following Security solutions: - i. End-Point Security ii. Email Security iii. Cybersecurity Threat Defense iv. Network Access Control (NAC) System	
2.	Proof of Physical Location of the Business	The bidder shall provide proof of occupation of the business premises. The proof should be signed lease(s) or ownership documentation or any other applicable and acceptable documentation.	
3.	Staff Competence in Endpoint, Server and Email Security	The bidder MUST have at least three (3) Engineers trained in the deployment of physical servers, virtualization, endpoint, Server, and email security. For each of the engineers: - i. Attach certified CVs ii. Attach copies of certificates showing knowledge of	

	Technical Documentation Required		
No.	**Item/Specification**	**Requirement**	**Bidder's Response**
		Application Security, VMware, Cloud Security, and Servers. iii. The bidder MUST have 2 vendor certifications of the proposed solution. iv. Attach documentation for sites implemented by the respective Engineers. *The engineers proposed here MUST be involved in the implementation of the project if awarded.*	
4.	Staff Competence in Network Security	The bidder MUST have at least two (2) Engineers trained and experienced in the deployment of the Network Access Control System. For each of the Engineers: - i. Attach certified CVs. ii. Attach copies of certificates showing knowledge of Network Security and Access Control iii. The bidder MUST have 2 vendor certifications of the proposed solution. iv. Attach documentation for sites implemented by the respective Engineers. *The engineers proposed here MUST be involved in the implementation of the project if awarded.*	
5.	Bidders experience in similar sites	The bidder MUST have successfully deployed at least three (3) similar sites comprised of End-point, Email and Network Security. For each of the sites, attach the following: - i. Name of site/client ii. Copies of LSO/contracts iii. Respective completion certificates or recommendation letters iv. Contact person's name and email address	
6.	Brochure	Include detailed brochures and datasheets of the bidder's proposed hardware and solutions	
7.	Sample Service Level Agreement (SLA)	The bidder shall include a proposed SLA to be adopted after system commissioning. The SLA should include the following key deliverables: - i. Period – 3 years	

	Technical Documentation Required		
No.	**Item/Specification**	**Requirement**	**Bidder's Response**
		ii. Services to be provided within the SLA iii. Response times iv. Escalations v. Penalties Further details for the required SLA are available in the detailed technical specifications document	
8.	Soft copy of the Bidding Document	The vendor MUST provide a Softcopy of the bidding document in a Flash Disk.	
9.	Pre-bid Meeting	A pre-bid meeting form duly signed by a KCAA staff	
10.	Warranty	a. The bidder MUST indicate a detailed maintenance and support plan for the system within the warranty periods. b. Further, provide documentation indicating that the warranty for the hardware covers the East African region. c. The bidder MUST indicate the total expected life of the equipment to be supplied	
11.	Vendor Accreditation	a. The vendor must be a leader in the last 3 OMDIA vulnerability Disclosure Index. Attach the OMDIA reports. b. The bidder must be a leader on the latest magic quadrant for extended detection and response(XDR). Attach the reports reference. c. Must be on the latest Gartner Magic Quadrant for Endpoint Protection Platforms. Attach the latest Gartner reports.	

Note: All bidders must meet the following mandatory technical specifications to be considered responsive in order to proceed to the next stage of evaluation. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirement. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	ANTIVIRUS+XDR			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Product and Quantity	1000 endpoint security licenses shall be deployed in all endpoints at KCAA HQ and all stations	M	
2.	Anti-Malware Capability	Provide advanced automated threat detection and response against a variety of advanced malware threats, including fileless attack, cryptomining and ransomware		
3.	Deployment Options	Provide flexible cloud (SaaS) or on-premises deployment options	M	
4.	Unified Agent	The solution should offer both EDR and endpoint protection platform (Anti-malware, Web Reputation, Device Control, Integrated DLP, Machine learning, Behaviour Analysis, Endpoint Cloud Sandbox submission, Virtual Patching for endpoint via HIPs and Application Control, Endpoint FW) in single agent	M	
		Provide both Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) features in a single agent	M	
5.	Integration	Able to integrate with customer's SIEM solution	M	
		Allow third-party programs to integrate with the solution through an Application Programming Interface (API)	M	
	Intrusion Prevention System	Shall reduce risk exposure due to missing patches	M	
6.		The proposed solution is able to provide virtual patching functionality without additional agent footprint or 3rd party integration	M	
		Solution shall provide the customer with performance and security priority option that suits their security requirement and environment.	M	
		Shall be able to block against known & unknown vulnerability exploits	M	
		Solution shall shield endpoints from network exploitable vulnerabilities targetting endpoint OS	M	
		Must have a host-based intrusion prevention system (HIPS) to virtually patch known and unknown vulnerabilities before a patch is available or deployable.	M	

	ANTIVIRUS+XDR			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
7.	Central Management	Solution must provide central management functions in terms of logs, threat intelligence, status of managed products / devices, and deployment of applications.	M	
		Solution must provide central management functions of threat intelligence which can be shared with managed products / devices	M	
		Single pane of glass for all security controls and products in the suite	M	
		The solution should be managed through a web console	M	
		Solution must provide central management functions of logs collected from managed products / devices	M	
		Solution must provide granular log search filters for users to define their own search criteria	M	
8.	Damage clean up service	Solution must be able to remove (reset) malware changes in the windows registry, remove dropped file(s) and terminates running malicious processes.	M	
		Able to perform different scan Actions based on varios malware types (Trojan/ Worm, Joke, Hoax, Virus, etc.)	M	
		Solution shall have behavior monitoring capability to detect malicious program behavior that is common to exploit attacks	M	
		Able to detect and remove Spyware and Adware even after it is installed and running on the computer.	M	
		Shall provide continuous malware protection and able to perform updates regardless of whether the client is connected to the management server.	M	
		Shall provide continuous malware protection regardless of whether the endpoint is connected to the Internet.	M	
9.	Web Reputation Services	Solution must be able to block access to malicious websites and URLs with accurate and comprehensive rating algorithm	M	
		Must be able to support approved (whitelist) and blocked (blacklist) URLs list	M	
		Must be able to block connection attempts to command and control (C&C) servers	M	
		Must be able to support approved (whitelist) and blocked (blacklist) IP list	M	

	ANTIVIRUS+XDR			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
10.	Device Control	Able to display notification message on client computer when violation happens	M	
		Able to log Device Control violation	M	
		Allow adding of trusted devices	M	
		Must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access.	M	
11.	System Lockdown	The proposed solution is able to provide application control functionality without additional agent footprint or 3rd party integration	M	
		Able to manually (by the administrator or security officer) or automatically (via sandbox report) block the tagged suspicious applications.	M	
		Must be able to correlate data from millions of application events to identify threats and maintain an up-to-date database of validated applications	M	
12.	Root Cause Analysis	The solution should identify affected endpoints through on-demand investigations and monitoring that are fully customizable to the user's needs. Integration with endpoint cloud Sandbox provides a comprehensive set of threat details that can help administrators and information security experts respond effectively to attacks.	M	
		Must have a visualized root cause analysis (RCA) report	M	
		The solution should provide threat investigation capabilities.	M	
		The solution should be able to terminate a running process (or file) or isolate an endpoint as response action to an ongoing attack investigation	M	
		The solution should provide customized endpoint investigation. The solution should support IOC and YARA rules which allow the creation, sharing and re-use of existing threat information.	M	
All Requirements are Mandatory (P/F)			**P/F**	

Note: All bidders must meet the following mandatory technical specifications to be considered responsive in order to proceed to the next stage of evaluation. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirement. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	EMAIL SECURITY			
No	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Product and Quantity	Email security licenses shall be deployed to 1000 mailboxes.	M	
2.	General Solution Requirements	Provide a SaaS platform with a simple seamless integration to O365 platform	M	
		The Solution Should Protect Office 365 email and other cloud file-sharing and collaboration services	M	
		The solution should discover unknown malware using multiple patternless techniques, including machine learning and sandbox analysis.	M	
		The solution must detect ransomware and other malware hidden in Office file formats or PDF documents	M	
3.	Business Email Compromise	The solution must Identify business email compromise (BEC) attacks by using artificial intelligence (AI), including expert system and machine learning, to examine email header, content, and authorship, while applying more stringent protection for high-profile users.	M	
		The solution must prevent executive spoofing scams using Writing Style DNA to detect impersonations of high-profile users (such as the CEO, VP, GM) by analyzing the writing style of a suspicious email and comparing it to an AI model of that user's writing.	M	
4.	Sandboxing	The Solution Should provide built-in sandbox malware analysis with multiple operating systems and extensive anti-evasion technology	M	
5.	Retro Scan	The solution must protect internal email and allow manual scan to uncover attacks already in progress.	M	

	EMAIL SECURITY			
No	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
6.	Computer Vision	The solution must prevent credential phishing by blocking URLs which disguise as a legitimate logon website.	M	
7.	Data Loss Prevention Embedded NIC	The solution should give visibility into sensitive data use with cloud file-sharing services	M	
		The solution should provide Data Loss Prevention (DLP) and advanced malware protection for Box, Dropbox, Google Drive, SharePoint, OneDrive, and Teams.	M	
		The solution should discover compliance data in existing stored files and email by scanning databases.	M	
		The solution must have pre-built compliance templates, user/group policies, and support for Microsoft® Rights Management services.	M	
8.	Systems Management	The solution must provide direct cloud-to-cloud integration for high performance and scalability and not to rely on redirecting email or web proxies.	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

Part D: Mandatory Technical Requirements for Server Security

Note: All bidders must meet the mandatory technical specifications for the storage array. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	SERVER SECURITY			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Product and Quantity	Server Security licenses shall be deployed to 100 Servers (VM's and Physical Servers included)	M	
2.	General Requirements	The solution must provide single platform for complete server protection over physical, virtual & cloud	M	
		Complete protection from a single integrated platform: addresses all of the 'Gartner top ten server security priorities'.	M	
		Provides layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.	M	
		The solution must be able to support cloud server and physical server protection	M	
		The proposed solution provides self-defending servers; with multiple integrated modules below providing a line of defense at the server	M	
		The Anti-Malware, Firewall and Deep Packet Inspection can be deployed using a single agent or virtual appliance on the ESXi host for virtual desktops protection.	M	
		The proposed solution must be able to provide antimalware and virtual patching capability in a single agent	M	
		The dashboard must be configurable by the administrator to display the information which is required only	M	
		The proposed solution must have a web-based management system for administrators to access using web browsers	M	
		Providing "Alerts" on the main menu to view administrator notifications concerning system or security events.	M	
3.	AntiMalware & Machine Learning	Must be able to provide file reputation with variant protection that look for obfuscated, polymorphic by using fragments of previous seen ad detection algorithm	M	
		The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites for virtual desktops	M	
		Must be capable to do predictive machine learning as below that complementing behaviour analysis	M	
		i) Pre-execution	M	
		ii) Run-time execution	M	

	SERVER SECURITY			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
4.	Intrusion Prevention	Must be able to provide HIPS/HIDS feature that immediately protects against vulnerabilities like Shellshock, Heartbleed , or WannaCry	M	
		Must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations	M	
		Must be ABLE to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities	M	
		Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred	M	
		Must be able to provide protection against known and zero-day attacks (Please explain)	M	
5.	Intrusion Prevention	Must assists compliance (PCI DSS) to protect web applications and the data they process	M	
		Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot	M	
6.	Intrusion Detection	Provide virtual patching which shield vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs within minutes	M	
		Must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours	M	
7.	Application Control	The proposed solution must be able to lock down software and unwanted application execution to continuously monitors for software changes on protected servers	M	
8.	Supported Platform	Shall Support Platform including: Microsoft Windows Server, Virtual (Vmware, Citrix, Microsoft HyperV), Linux(RedHat, SUSE, Centos, Cloud Linux, Debian, Oracle, Amazon Linux)	M	
9.	Security Compliance	Provides out-of-the-box compliance support for: PCI DSS 2.0, NIST, HIPAA, SOX, ISO 2700x, SAS70	M	
10.	3rd Party Validation	The proposed solution MUST be positioned as a leader in vulnerability research by the latest Omdia reports	M	
		Leader in Threat Intelligence for Strength of Vulnerability Research	M	
		The proposed solution MUST be in the latest Gartner MQ leadership position for more than 5 years	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

Note: All bidders must meet the mandatory technical specifications for Cyber Risk Exposure Management(CREM). The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Cyber Risk Exposure Management (CREM)			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
1.	Quantity	Lot	M	
2.	General requirements	Solution should be able to continuously identify, categorize and document all the assets within the organization's digital ecosystem. Assets should be listed and categorized but not limited to the following asset categories: • Internet-facing Assets • Internal device Assets • Account Assets Application Assets.	M	
3.	Visibility	Solution should provide contextual visibility into all assets by: •Criticality based on asset attribute and activity. •Graphical presentation on relationship of assets Historical risk assessment result.	M	
4.	Management	Solution should be able to manage all discovered assets from a single unified management console.		
5.	Integration	Solution should be capable of integrating with a cybersecurity platform that is capable of managing the organization's Endpoint, Email, Cloud, Network, OT Security, XDR and Zero Trust solution in a single console.		
6.	Attack Prediction	Solution should be capable of providing an attack path functionality that can identify and predict potential attacks from external to internal critical assets. Solution should have built-in support for security playbooks that can be used for automated remediation.		
7.	External Attack Surface Management	Solution should be able to assess the security posture of Internet and other external facing assets in the organization		
8.	Risk Assessment	Solution should provide an organization wide risk score based on continuous assessment of risks in the organization.		

	Cyber Risk Exposure Management (CREM)			
No.	**Item**	**Specifications Required**	**Score**	**Bidder's Response**
9.	Exposure Index	Solution should provide an exposure index score that summarizes the likelihood of an exploit or threat to occur in the environment and provide a security configuration index score that summarizes deployed and missing security controls within the environment.		
10.	External Attack Surface Management	The solution shall provide risk assessment for each domain and IP address asset and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events and risk level for each discovered risk.		
11.	Device Assets	Provide risk assessment for each device asset and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events and risk level for each discovered risk.		
12.	Accounts/ Identity Assets	Should be able to provide the account's latest risk score, user type, role, location, job title and when the account was first and last seen and enumerate exposed APIs connected to discovered service accounts.		
13.	Application Assets	Identify both Cloud and Local Applications and provide the risk level		
14.	Vulnerability Management	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Mean Time to Patch		
15.	Remediation & Mitigation	Automate and orchestrate response actions to mitigate risks and respond to threats using advanced AI and ML technologies.		
16.	Reports & Dashboards	Provides insights into the organization's security posture using an Executive level dashboard. Must be able show the company's overall risk score, individual asset risks, a view of ongoing attacks and its contributing risk factors.		
All Requirements are Mandatory (Pass/Fail)			**P/F**	

PART F: NETWORK ACCESS CONTROL (NAC)

Note: All bidders must meet the mandatory technical specifications for the storage array. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
1.	Software	Supply of license to implement NAC with three-year warranty	M	
2.	Project Services Implementation	• Conducting Business Requirement Mapping • Preparation of architecture design, documentation and project plan for implementation. • Installation & Configuration of the supplied software associated Software and System Integration. • Development of appropriate security incidence response procedures in alignment with related policies. • Training on the NAC solution administration to Four ICT Staff • Handing over of final configuration document.	M	
3.	Policy lifecycle management	Enforces policies for all operating scenarios without requiring separate products or additional modules		
4.	Profiling and visibility	Recognizes and profiles users and their devices before malicious code can cause damage		
5.	Guest networking access	Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal.		
6.	Security posture check	Evaluates security-policy compliance by user type, device type, and operating system.		
7.	Incidence response	Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention.		
8.	Bidirectional integration	Integrate with other security and network solutions		
		Must be supplied as virtual appliances/Software (on-prem/cloud)		
		Must support agentless scanning of network for detection and classification of devices		
		Must create an inventory of all devices on the network		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		Must support event reporting to SIEM with detailed contextual data to reduce investigation time		
		Must assess risk of every endpoint on the network		
		Must support subscription-based licensing model		
		Must automate onboarding process for large number of endpoints, users and guests		
		Must enforce dynamic network access control and enable network segmentation		
		Must reduce containment time from days to seconds		
		Must support multiple canned reports for network reporting, compliance, and analysis		
		Must form a security integration with the proposed firewalls for automated quarantine of infected hosts		
		Must support legacy network access devices that do not support RADIUS		
		The solution must support major hypervisors including VMWare and Hyper-V		
		Must be able to scale to 15,000 concurrent users per VM		
		Must be licensed with at least 1000 concurrent user/device licenses		
		Must support at least 12GB RAM		
		Must support at least 1TB of attached storage.		
		The proposed VM appliances must be deployed in high availability for high availability.		
		The proposed VM appliances must be deployed centrally in the datacenter without any requirement of having different appliances across branch sites.		
9.	***Visibility:***	Must support Network Discovery		
		Must support both agentless and persistent agent deployments		
		Must support User and Device Domain Authorization		
		Must support User and Device Captive Portals		
		Must support Rogue Endpoint Identification		
		Must support Device Profiling and Classification		
		Must support MDM Integration		
10.		Must support Network Access Policies		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
	Automation / Control	Must support BYOD Onboarding		
		Must support Advanced Guest Management		
		Must support IoT Onboarding with Sponsor Authorization		
		Must support Endpoint Compliance		
		Must support automated Rogue Device Detection & Restriction		
		Must support Web & Firewall Single Sign On		
		Must support Firewall Segmentation		
11.	***Incident Response***	Must support Event Correlation		
		Must support Extensible Actions & Audit Trail		
		Must support Alert Criticality & Routing		
		Must support Guided Triage Workflows		
12.	***Integrations***	Must support Inbound Security Events		
		Must support REST API		
13.	***Reporting***	Must support live reporting		
		Must support historical analysis		
14.	**System Features:**	Must support Role-Based-Access-Control.		
		The solution must support secure management protocols (e.g. HTTPS, SSH)		
		The solution must support advanced auditing capabilities		
		Processes running on the device or operating system		
		The solution must provide e-mail alerting for administrative alerts		
		The solution must support configuration backup/restore		
		The solution must support common external authentication mechanisms for administrators (e.g. LDAP, AD, RADIUS, etc.)		
15.	**Policy Requirements:**	The solution must be able to classify assets on the network based on categories (e.g. Windows, Linux Mobile, etc.)		
		The solution must collect detailed asset information (E.g. MAC address, Logged on user, OS, NIC vendor, Switch Port, etc.)		
		The solution must be able to prevent network access from unauthorized and/or non-compliant devices (e.g.: BYOD device, device without Antivirus running)		
		The solution must provide captive portal abilities for guest device self-registration		
		The solution must provide captive portal abilities for BYOD devices via corporate logon credentials (e.g. AD, LDAP)		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		The solution must be able to detect/prevent ARP spoofing		
		The solution must be able to detect/prevent device dual-homing (e.g. wired + wireless access)		
		The solution must be able to detect/prevent malicious hosts		
		The solution must be able to detect Windows Update compliance		
		The solution must be able to detect Antivirus Update compliance		
		The solution must be able to detect endpoint firewall compliance		
		The solution must be able to detect/prevent external storage media & peripherals (e.g. USB flash drives webcams, etc.)		
		The solution must be able to detect custom attributes of devices (e.g. script output, WMI, registry, file attributes, running processes, etc.)		
		The solution must be able to quarantine devices based on policy (e.g. Switch port block, virtual firewall)		
		The solution must support administrative reversal of policy actions (e.g. unquarantined device)		
		The solution must support manual administrative actions (e.g. quarantine device, re-evaluate policies,		
16.	***Mandatory Integration Requirements:***	The solution must integrate with common router/switch vendors (e.g. Cisco, Brocade)		
		The solution must integrate with common AV/EDR vendors (e.g. Sophos, Crowdstrike, Carbon Black Symantec)		
		The solution must integrate with common firewall vendors (e.g. Palo Alto, Fortinet, Check Point)		
		The solution must integrate with common Anti- malware vendors (e.g. FireEye)		
		The solution must integrate with common Wi-Fi vendors (e.g. Ruckus, Cisco, UniFi, Aruba)		
		The solution must integrate with common mobile device management (MDM) vendors (e.g. Airwatch, Mobile Iron, Citrix)		

	Network Access Control (NAC)			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		The solution must integrate with common vulnerability assessment vendors (e.g. Qualys Rapid7)		
17.	***Mandatory Reporting Requirements:***	The solution must include pre-built report templates (e.g.: device policy compliance)		
		The solution must support custom reports		
		The solution must support scheduled reports		
18.	**Vendor Requirements**	The vendor must be PECB MS Certified (ISMS)		
		The vendor lead engineer must be certified by the OEM as a system administrator or implementor		
		The vendor must provide proof of having engaged in similar NAC projects		
19.	**Technical Training**	The bidder should describe how they shall meet the requirements for NAC technical training. The requirements are as follows: a. The exercise shall take a period of Five (5) days. b. Six (6) KCAA ICT staff shall be trained. This shall be undertaken at a fully accredited Vendor training centre with all the requisite labs, simulators and facilities. c. All the applicable costs for this activity shall be borne by the vendor. These include but not limited to economy air tickets, VISA fees, subsistence allowance and other applicable costs.	M	
20.	**Operational Testing and Knowledge transfer**	The bidder should describe how they shall meet the requirements for operational testing and knowledge.	M	
21.	**Go-LIVE and Commissioning**	The bidder should describe how they shall meet the requirements for go-live and commissioning.	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

PART G: PROJECT IMPLEMENTATION SERVICES

Note: All bidders must meet the mandatory technical specifications for the Renewal of Cybersecurity Infrastructure. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	Upgrades and Other Services			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
1.	Project Management	a. Mandatory letter to KCAA providing assurance that the project will be completed in three (3) months after contract award. b. A Comprehensive Project Implementation Plan MUST be attached. c. Details of the Project Manager. i. Attach CV. ii. Copies of PMP or Prince 2 certifications. iii. The project manager MUST have implemented at least three (3) successful projects. d. The bidder to provide sample documents of the proposed project implementation documents. These are; Project Charter, Sample Project Initiation Document and Sign-Offs.	M	
2.	Integration with existing environment	a. The bidder MUST integrate the existing environment with the proposed environment. b. The bidder is expected to provide a technical proposal of how to undertake this integration.	M	
3.	Technical Certified Training	The bidder should describe how they shall meet the requirements for technical training. The requirements are as follows: - a. The exercise shall take a period of ten (10) working days. b. The training shall entail the following key areas; Cybersecurity Policies, Solutions, Design and Implementation. c. Six (6) KCAA ICT staff shall be trained. This shall be undertaken at a fully accredited OEM training centre with all the requisite labs, simulators and facilities. d. All the applicable costs for this activity shall be borne by the vendor. These include but not limited to	M	

	Upgrades and Other Services			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		economy air tickets, VISA fees, subsistence allowance and other applicable costs.		
4.	Operational Testing and Knowledge transfer	The bidder should describe how they shall meet the requirements for operational testing and knowledge transfer. The requirements are as follows: a. The exercise shall take a period of five (5) days. b. This bidder shall propose a detailed schedule for the five (5) days including knowledge transfer and training. c. The quality assurance, testing and training should entail; Inspection of installations works, centralized useability and management, robust monitoring and reporting. d. Eight (8) KCAA ICT staff shall be trained. This shall be undertaken at a serene environment out of town. e. All the applicable costs for this activity shall be borne by the vendor. f. These include but not limited to conferencing, subsistence allowance and other applicable costs.	M	
5.	Go-LIVE and Commissioning	The bidder should describe how they shall meet the requirements for go-live and commissioning. The requirements are as follows: - a. The exercise shall take a period of one (1) day immediately after operational testing and knowledge transfer.	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

Note: All bidders must meet the mandatory technical specifications for SLA. The bidder MUST provide detailed explanations of how they shall fully meet the required technical requirements. Bidders should NOT write complied or just tick (√) against a requirement, a full detailed explanation is required.

	SLA			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
1.	Maintenance and Support Term	The maintenance and support period is three (3) years backed by OEM	M	
2.	Items to be maintained and supported	The Security Infrastructure and all its components.	M	
3.	Preventive Maintenance	Health checks for all components (hardware, firmware and software) and preventive maintenance to be undertaken once every quarter for the three (3) year period. Status reports to be provided to KCAA indicating the status of each maintenance item.	M	
4.	Corrective Maintenance	a. To be undertaken immediately if a maintenance component fails. Items to be replaced under the OEM. b. Where downtime is required, this shall be arranged with the KCAA systems administration team for approval prior to the required downtime.	M	
5.	Outage Severity Levels and Required Response Times	a. **Severity One/Red:** KCAA is unable to do their business as a result of complete or partial system failure. This has a major impact on the KCAA's business operations. Response: The vendor should respond within one (1) hour. A resolution or a workaround should be provided within two (2) hours. b. **Severity Two/Orange:** The problem has high visibility and impacts on the way KCAA does business. The ARMS service is disrupted but not halted. The system performance may be degraded, or functions limited. Response: The vendor should respond within three (3) hours. A resolution or a workaround should be provided within twelve (12) hours. c. **Severity Three/Green:** A single component or several components are affected with or without a work around. The problem may affect KCAA's efficiency but is limited in visibility and does not prevent work from being completed. Response: The vendor should respond within twelve (12) hours. A resolution or a workaround should be provided within seventy-two (72) hours.	M	
6.	Fault Logging Procedure and Reporting	a. The vendor to provide a support service desk email and a telephone number manned 24/7 for logging faults and a fault should be allocated a reference number for ease of tracking.	M	

	SLA			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		b. Response to faults logs shall be undertaken as per the response times based on severity levels. c. Once a red or orange level fault is resolved, a report should be provided entailing the following: - i. The root cause analysis ii. The measures taken to resolve it iii. The measures taken to ensure it does not recur		
7.	Escalations	The vendor shall provide two escalation levels after a fault is reported and left unattended. Phone numbers and email addresses of the escalation levels shall be required. The levels are as follows: a. Level 0 – Normal helpdesk reporting after a fault. b. Level 1 – Technical manager or service provision manager after the response times for resolution are not met. c. Level 2 – The CEO after the required response times are not met after escalating to level 2.	M	
8.	Maintenance and Support Services	a. Ensuring uptime of all security systems. b. Maintenance and support should include security appliance and related accessories. c. Consultation for guidance on complex procedures and processes in configuration and integration of the Solution. d. Assistance in configuration of the Solution in case of failure of any part of the System. e. Configuration of the Solution to optimize performance. f. Support and assistance on matters concerning security upgrades and any Service Pack installations. g. Bugs and Errors resolution as far as the security software is concerned. h. Receive, classify, log and track all reported issues and provide case updates until the issues is conclusively resolved. i. Provide urgent security alerts on the version deployed by the client. j. Troubleshooting and provide workarounds assistance where existing system cannot perform some of the tasks. k. Installation and configuration advice to KCAA ICT technical staff. l. Answering questions and providing a reasonable level of guidance to KCAA about the Security Solutions. m. Provide trained Technical Support personnel to handle inquiries and problems.	M	

	SLA			
No.	**Item(s)**	**Requirement**	**Score**	**Bidder's Response**
		n. Provide documentation updates and major system releases information. o. Provide pro-active maintenance release announcements sent to customer directly. p. Participate in failover and failback tests for the KCAA remote disaster recovery site.		
9.	Infrastructure Upgrades	Occasionally the Authority will make plans for replacement of the infrastructure. The vendor will be required to: - a. Make recommendations for security infrastructure b. Undertaking infrastructure upgrades as requested by KCAA.	M	
10.	SLA Payments	Payments pertaining the three-year SLA shall be paid semi-annually in arrears after invoicing and provision of SLA (maintenance and support) reports applicable for the payment period. The detailed and signed reports shall be provided by the bidder.	M	
11.	Sample SLA	The vendor shall provide a sample SLA that meets all the above provisions for adoption in the contract.	M	
12.	SLA penalties	Core services are provided 24 hours a day by the Authority. The Authority expects the infrastructure to be available 99.95% of the time per annum. The vendor will be penalized in cases of protracted downtime. This will be calculated by factoring in the number of hours constituting to 99.95% per year, the applicable amount per hour and the number of hours the system has been unavailable within a particular payment period.	M	
All Requirements are Mandatory (Pass/Fail)			**P/F**	

PART III – CONDITIONS OF CONTRACT AND CONTRACT FORMS

SECTION VIII - GENERAL CONDITIONS OF CONTRACT

A. General

Provisions Definitions

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

a) The Adjudicator is the person appointed jointly by the Procuring Entity and the Service Provider to resolve disputes in the first instance, as provided for in Sub-Clause8.2 hereunder.
b) "Activity Schedule" is the priced and completed list of items of Services to be performed by the Service Provider forming part of his Tender;
c) "Completion Date" means the date of completion of the Services by the Service Provider as certified by the Procuring Entity
d) "Contract" means the Contract signed by the Parties, to which these General Conditions of Contract (GCC) are attached, together with all the documents listed in Clause 1 of such signed Contract;
e) "Contract Price" means the price to be paid for the performance of the Services, in accordance with Clause 6;
f) "Day works" means varied work inputs subject to payment on a time basis for the Service Provider's employees and equipment, in addition to payments for associated materials and administration.
g) "Procuring Entity" means the Procuring Entity or party who employs the Service Provider
h) "Foreign Currency" means any currency other than the currency of Kenya;
i) "GCC" means these General Conditions of Contract;
j) "Government "means the Government of Kenya;
k) "Local Currency "means Kenya shilling;
l) "Member," in case the Service Provider consist of a joint venture of more than one entity, means any of these entities; "Members" means all these entities, and "Member in Charge" means the entity specified in the SC to act on their behalf in exercising all the Service Provider' rights and obligations towards the Procuring Entity under this Contract;
m) "Party" means the Procuring Entity or the Service Provider, as the case maybe, and "Parties" means both of them;
n) "Personnel" means persons hired by the Service Provider or by any Subcontractor as employees and assigned to the performance of the Services or any part there of;
o) "Service Provider" is a person or corporate body whose Tender to provide the Services has been accepted by the Procuring Entity;
p) "Service Provider's Tender" means the completed Tendering Document submitted by the Service Provider to the Procuring Entity
q) "SCC" means the Special Conditions of Contract by which the GCC may be amended or supplemented;
r) "Specifications" means the specifications of the service included in the Tendering Document submitted by the Service Provider to the Procuring Entity
s) "Services" means the work to be performed by the Service Provider pursuant to this Contract, as described in Appendix A; and in the Specifications and Schedule of Activities included in the Service Provider's Tender.
t) "Subcontractor" means any entity to which the Service Provider subcontracts any part of the Services in accordance with the provisions of Sub-Clauses3.5and4;
u) "Public Procurement Regulatory Authority (PPRA)" shall mean the Government Agency responsible for oversight of public procurement.
v) "Project Manager" shall the person appointed by the Procuring Entity to act as the Project Manager for the purposes of the Contract and named in the Particular Conditions of Contract, or other person appointed from time to time by the Procuring Entity and notified to the Contractor."Notice of Dissatisfaction" means the notice given by either Party to the other indicating its dissatisfaction and intention to commence arbitration.

1.2 Applicable Law

The Contract shall be interpreted in accordance with the laws of Kenya**.**

1.3 Language

This Contract has been executed in the English language**,** which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

1.4 Notices

Any notice, request, or consent made pursuant to this Contract shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, hand delivery, or email to such Party at the address **specified in the SCC.**

1.5 Location

The Services shall be performed at such locations as a specified in Appendix A, in the specifications and, where the location of a particular task is not so specified, at such locations, whether in Kenya or elsewhere, as the Procuring Entity may approve.

1.6 Authorized Representatives

Any action required or permitted to be taken, and any document required or permitted to be executed, under this Contract by the Procuring Entity or the Service Provider may be taken or executed by the officials **specified in the SCC.**

1.7 Inspection and Audit by the PPRA

Pursuant to paragraph 2.2 e. of Attachment 1 to the General Conditions, the Service Provider shall permit and shall cause its sub contract or sand sub-consultants to permit, PPRA and/or persons appointed by PPRA to inspect the Site and/or the accounts and records relating to the procurement process, selection and/or contract execution, and to have such accounts and records audited by auditors appointed by PPRA. The Service Provider's and its Subcontractors' and sub-consultants' attention is drawn to Sub-Clause 3.10 which provides, interalia, that acts intended to materially impede the exercise of PPRA's inspection and audit rights constitute a prohibited practice subject to contract termination (as well as to a determination of ineligibility pursuant to PPRA's prevailing sanctions procedures).

1.8 Taxes and Duties

The Service Provider, Subcontractors, and their Personnel shall pay such taxes, duties, fees, and other impositions as may be levied under the Applicable Law, the amount of which is deemed to have been included in the Contract Price.

2. Commencement, Completion, Modification, and Termination of Contract

2.1 Effectiveness of Contract

This Contract shall come into effect on the date the Contract is signed by both parties or such other later date as maybe **stated in the SCC.**

2.2 Commencement of Services

1.2.1 Program

Before commencement of the Services, the Service Provider shall submit to the Procuring Entity for approval a Program showing the general methods, arrangements order and timing for all activities. The Services shall be carried out in accordance with the approved Program as updated.

2.2.2 Starting Date

The Service Provider shall start carrying out the Services thirty (30) days after the date the Contract becomes effective, or at such other date as may be **specified in the SCC.**

2.3 Intended Completion Date

Unless terminated earlier pursuant to Sub-Clause 2.6, the Service Provider shall complete the activities by the Intended Completion Date, as is **specified in the SCC.** If the Service Provider does not complete the activities by the Intended Completion Date, it shall be liable to pay liquidated damage as per Sub-Clause3.8.Inthiscase,the Completion Date will be the date of completion of all activities.

2.4 Modification

Modification of the terms and conditions of this Contract, including any modification of the scope of the Services or of the Contract Price, may only be made by written agreement between the Parties.

2.4.1 Value Engineering

The Service Provider 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, if applicable) the Procuring Entity may incur in implementing the value engineering proposal; and

c) A description of any effect(s)of the change on performance/functionality.

The Procuring Entity may accept the value engineering proposal if the proposal demonstrates benefits that:

a) accelerates the delivery period; or

b) reduces the Contract Price or the lifecycle costs to the Procuring Entity; or

c) improves the quality, efficiency, safety or sustainability of the services; or

d) yields any other benefits to the Procuring Entity, without compromising the necessary functions of the Facilities.

If the value engineering proposal is approved by the Procuring Entity and results in:

a) a reduction of the Contract Price; the amount to be paid to the Service Provider 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 lifecycle costs due to any benefit described in (a) to(d)above, the amount to be paid to the Service Provider shall be the full increase in the Contract Price.

2.5 Force Majeure

2.5.1 Definition

For the purposes of this Contract,"ForceMajeure"meansaneventwhichisbeyondthereasonablecontrolofa Party and which makes a Party's performance of its obligations under the Contract impossible or so impractical as to be considered impossible under the circumstances.

2.5.2 No Breach of Contract

The failure of a Party to fulfill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and(b) has informed the other Party as soon as possible about the occurrence of such an event.

2.5.3 Extension of Time

Any period with in which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

2.5.4 Payments

During the period of their inability to perform the Services as a result of an event of Force Majeure, the Service Provider shall be entitled to continue to be paid under the terms of this Contract, as well as to be reimbursed for additional costs reasonably and necessarily incurred by them during such period for the purposes of the Services and in reactivating the Service after the end of such period.

2.6 Termination

2.6.1 By the Procuring Entity

The Procuring Entity may terminate this Contract, by not less than thirty(30) days' written notice of termination to the Service Provider, to be given after the occurrence of any of the events specified in paragraphs(a)through (d) of this Sub-Clause 2.6.1:

a) If the Service Provider does not remedy a failure in the performance of its obligations under the Contract, within thirty (30) days after being notified or within any further period as the Procuring Entity may have subsequently approved in writing;

b) if the Service Provider become insolvent or bankrupt;

c) if, as the result of Force Majeure, the Service Provider is unable to perform a material portion of the Services for a period of not less than sixty (60) days; or

d) if the Service Provider, in the judgment of the Procuring Entity has engaged in Fraud and Corruption, as defined in paragraph2.2a. of Attachment1 to the GCC, in competing for or in executing the Contract

2.6.2 By the Service Provider

The Service Provider may terminate this Contract, by not less than thirty (30) days' written notice to the Procuring Entity, such notice to be given after the occurrence of any of the events specified in paragraphs (a) and
(b) of this Sub-Clause 2.6.2:

a) If the Procuring Entity fails to pay any monies due to the Service Provider pursuant to this Contract and not subject to dispute pursuant to Clause 7 within forty-five (45) days after receiving written notice from the Service Provider that such payment is overdue; or

b) if, as the result of Force Majeure, the Service Provider is unable to perform a material portion of the Services for a period of not less than sixty (60) days.

2.6.3 Payment up on Termination

Upon termination of this Contract pursuant to Sub-Clauses 2.6.1 or 2.6.2, the Procuring Entity shall make the following payments to the Service Provider:

a) remuneration pursuant to Clause 6 for Services satisfactorily performed prior to the effective date of termination;

b) except in the case of termination pursuant to paragraphs (a), (b), (d) of Sub-Clause 2.6.1, reimbursement of any reasonable cost incident to the prompt and orderly termination of the Contract, including the cost of the return travel of the Personnel.

3 Obligations of the Service Provider

3.1 General

The Service Provider shall perform the Services in accordance with the Specifications and the Activity Schedule, and carry out its obligations with all due diligence, efficiency, and economy, in accordance with generally accepted professional techniques and practices, and shall observe sound management practices, and employ appropriate advanced technology and safe methods. The Service Provider shall always act, in respect of any matter relating to this Contractor to the Services, as faithful adviser to the Procuring Entity, and shall at all times support and safeguard the Procuring Entity's legitimate interests in any dealings with Subcontractors or third parties.

3.2 Conflict of Interests

3.2.1 Service Provider Not to Benefit from Commissions and Discounts.

The remuneration of the Service Provider pursuant to Clause 6 shall constitute the Service Provider's sole remunerationinconnectionwiththisContractortheServices,andtheServiceProvidershallnotacceptfortheir own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this

Contractor to the Services or in the discharge of their obligations under the Contract, and the Service Provider shall use their best efforts to ensure that the Personnel, any Subcontractors, and agents of either of them similarly shall not receive any such additional remuneration.

3.2.2 Service Provider and Affiliates Not to be Otherwise Interested in Project

The Service Provider agree that, during the term of this Contract and after its termination, the Service Provider and its affiliates, as well as any Subcontractor and any of its affiliates, shall bed is qualified from providing goods, works, or Services(other than the Services and any continuation thereof) for any project resulting from or closely related to the Services.

3.2.3 Prohibition of Conflicting Activities

Neither the Service Provider nor its Subcontractors nor the Personnel shall engage, either directly or indirectly, in any of the following activities:

a) During the term of this Contract, any business or professional activities in Kenya which would conflict with the activities assigned to them under this Contract;

b) during the term of this Contract, neither the Service Provider nor their Subcontractors shall hire public employees' inactive duty or on any type of leave, to perform any activity under this Contract;

c) After the termination of this Contract, such other activities as may be **specified in the SCC.**

3.3 Confidentiality

The Service Provider, its Subcontractors, and the Personnel of either of them shall not, either during the term or within two (2) years after the expiration of this Contract, disclose any proprietary or confidential information relating to the Project, the Services, this Contract, or the Procuring Entity's business or operations without the prior written consent of the Procuring Entity.

3.4 **The Service Provider** (a) shall take out and maintain, and shall cause any Subcontractors to take out and maintain, at its (or the Sub contractors', as the case may be)own cost but on terms and conditions approved by the Procuring Entity, insurance against the risks, and for the coverage, as shall be **specified in the SCC;** and (b) at the Procuring Entity's request, shall provide evidence to the Procuring Entity showing that such insurance has been taken out and maintained and that the current premiums have been paid.

3.5 Service Provider's Actions Requiring Procuring Entity's Prior Approval

The Service Provider shall obtain the Procuring Entity's prior approval in writing before taking any of the following actions:

a) Entering into a subcontract for the performance of any part of the Services,

b) appointing such members of the Personnel not listed by name in Appendix C ("Key Personnel and Subcontractors"),

c) changing the Program of activities; and

d) Any other action that may be **specified in the SCC.**

3.6 Reporting Obligations

The Service Provider shall submit to the Procuring Entity the reports and documents specified in Appendix B in the form, in the numbers, and within the periods set forth in the said Appendix.

3.7 Documents Prepared by the Service Provider to Be the Property of the Procuring Entity

All plans, drawings, specifications, designs, reports, and other documents and software submitted by the Service Provider in accordance with Sub-Clause 3.6 shall become and remain the property of the Procuring Entity, and the Service Provider shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the Procuring Entity, together with a detailed inventory thereof. The Service Provider may retain a copy of such documents and software. Restrictions about the future use of these documents, if any, shall be **specified in the SCC.**

3.8 Liquidated Damages

3.8.1 Payments of Liquidated Damages

The Service Provider shall pay liquidated damages to the Procuring Entity at the rate per day **stated in the SCC** for each day that the Completion Date is later than the Intended Completion Date. The total amount of liquidated damages shall not exceed the amount **defined in the SCC.** The Procuring Entity may deduct liquidated damages from payments due to the Service Provider. Payment of liquidated damages shall not affect the Service Provider's liabilities.

3.8.2 Correction for Over-payment

If the Intended Completion Date is extended after liquidated damages have been paid, the Procuring Entity shall correct any overpayment of liquidated damages by the Service Provider by adjusting the next payment certificate. The Service Provider shall be paid interest on the overpayment, calculated from the date of payment to the date of repayment, at the rates specified in Sub-Clause 6.5.

3.8.3 Lack of performance penalty

If the Service Provider has not corrected a Defect within the time specified in the Procuring Entity's notice, a penalty for Lack of performance will be paid by the Service Provider. The amount to be paid will be calculated as a percentage of the cost of having the Defect corrected, assessed as described in Sub-Clause7.2 and **specified in the SCC.**

3.9 Performance Security

The Service Provider shall provide the Performance Security to the Procuring Entity no later than the date specified in the Form of acceptance. The Performance Security shall be issued in an amount and form and by a bank or surety acceptable to the Procuring Entity, and denominated in the types and proportions of the currencies in which the Contract Price is payable. The performance Security shall be valid until a date 28 day from the Completion Date of the Contract in case of a bank guarantee, and until one year from the Completion Date of the Contract in the case of a Performance Bond.

3.10 Fraud and Corruption

The Procuring Entity requires compliance with the Government's Anti-Corruption laws and its prevailing sanctions. The Procuring Entity requires the Service Provider to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the tendering process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee.

3.11 Sustainable Procurement

The Service Provider shall conform to the sustainable procurement contractual provisions, if and as specified in the SCC.

4 Service Provider's Personnel

4.1 Description of Personnel

The titles, agreed job descriptions, minimum qualifications, and estimated periods of engagement in the carrying out of the Services of the Service Provider's Key Personnel are described in Appendix C. The Key Personnel and Subcontractors listed by title as well as by name in Appendix Care hereby approved by the Procuring Entity.

4.2 Removal and/or Replacement of Personnel

a) Except as the Procuring Entity may otherwise agree, no changes shall be made in the Key Personnel. If, for any reason beyond the reasonable control of the Service Provider, it becomes necessary to replace any of the Key Personnel, the Service Provider shall provide as a replacement a person of equivalent or better qualifications.

b) If the Procuring Entity finds that any of the Personnel have (i) committed serious misconduct or have been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Service Provider shall, at the Procuring Entity's written request specifying the grounds thereof, provide as a replacement a person with qualifications and experience acceptable to the Procuring Entity.

c) The Service Provider shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of Personnel.

5 Obligations of the Procuring Entity

5.1 Assistance and Exemptions

The Procuring Entity shall use its best efforts to ensure that the Government shall provide the Service Provider such assistance and exemptions as **specified in the SCC.**

5.2 Change in the Applicable Law

If, after the date of this Contract, there is any change in the Applicable Law with respect to taxes and duties which increases or decreases the cost of the Services rendered by the Service Provider, then the remuneration and reimbursable expenses otherwise payable to the Service Provider under this Contract shall be increased or decreased accordingly by agreement between the Parties, and corresponding adjustments shall be made to the amounts referred to in Sub-Clauses 6.2(a) or (b), as the case may be.

5.3 Services and Facilities

The Procuring Entity shall make available to the Service Provider the Services and Facilities listed under Appendix F.

6 Payments to the Service Provider

6.1 Lump-Sum Remuneration

The Service Provider's remuneration shall not exceed the Contract Price and shall be a fixed lump-sum including all Subcontractors' costs, and all other costs incurred by the Service Provider in carrying out the Services described in Appendix A. Except as provided in Sub-Clause 5.2, the Contract Price may only be increased above the amounts stated in Sub-Clause 6.2 if the Parties have agreed to additional payments in accordance with Sub- Clauses2.4and6.3.

6.2 Contract Price

a) The price payable is **set forth in the SCC.**

b) Price may be payable in foreign currency, if so allowed in this document.

6.3 PaymentforAdditionalServices,andPerformanceIncentiveCompensation

6.3.1 For the purpose of determining the remuneration due for additional Services as may be agreed under Sub-Clause 2.4, a breakdown of the lump-sum price is provided in Appendices D and E.

6.3.2 **If the SCC so specify,** the service provider shall be paid performance incentive compensation asset out in the Performance Incentive Compensation appendix.

6.3.3 Where the contract price is different from the corrected tender price, in order to ensure the contractor is not paid less or more relative to the contract price (*which would be the tender price*), payment valuation certificates and variation orders on omissions and additions valued based on rates in the schedule of rates in the Tender, will be adjusted by a plus or minus percentage. The percentage already worked out during tender evaluation is worked out as follows:*(corrected tender price–tender price)/tender price X100*.

6.4 Terms and Conditions of Payment

Payments will be made to the Service Provider according to the payment schedule **stated in the SCC. Unless otherwise stated in the SCC**, the advance payment (Advance for Mobilization, Materials and Supplies) shall be made against the provision by the Service Provider of a bank guarantee for the same amount, and shall be valid for the period **stated in the SCC.** Any other payment shall be made after the conditions **listed in the SCC** for such payment have been met, and the Service Provider have submitted an invoice to the Procuring Entity specifying the amount due.

6.5 Interest on Delayed Payments

If the Procuring Entity has delayed payments beyond thirty (30) days after the due date stated in the SCC, interest shall be paid to the Service Provider foreach day of delay at the rate stated in **the SCC**.

6.6 Price Adjustment

6.6.1 Prices shall be adjusted for fluctuations in the cost of inputs only if **provided for in the SCC.** If so provided, the amounts certified in each payment certificate, after deducting for Advance Payment, shall be adjusted by applying the respective price adjustment fact or to the payment amounts due in each currency. A separate formula of the type indicated below applies to each Contract currency:

$$\mathbf{P_c = A_c + B_c\, Lmc / Loc + C_c\, Imc / Ioc}$$

Where:

P_c is the adjustment factor for the portion of the Contract Price payable in a specific currency “c”.

A_c, B_c and C_c are coefficients specified in the SCC, representing: A_c the non-adjustable portion; B_c the adjustable portion relative to labor costs and C_c the adjustable portion for other inputs, of the Contract Price payable in that specific currency “c”; and

Lmc is the index prevailing at the first day of the month of the corresponding invoiced ate and Loc is the index prevailing28 days before Tender opening for labor; both in the specific currency “c”.

Imc is the index prevailing at the first day of the month of the corresponding invoice date and Ioc is the index prevailing 28 days before Tender opening for other inputs payable; both in the specific currency “c”.

If a price adjustment factor is applied to payments made in a currency other than the currency of the source of the index for a particular indexed input, a correction factor Zo/Zn will be applied to the respective component factor of pn for the formula of the relevant currency. Zo is the number of units of Kenya Shillings of the index, equivalent to one unit of the currency payment on the date of the base index, and Zn is the corresponding number of such currency units on the date of the current index.

6.6.2 If the value of the index is changed after it has been used in a calculation, the calculation shall be corrected and an adjustment made in the next payment certificate. The index value shall be deemed to take account to fall changes in cost due to fluctuations in costs.

6.7 Day works

6.7.1 If applicable, the Day work rates in the Service Provider's Tender shall be used for small additional amounts of Services only when the Procuring Entity has given written instructions in advance for additional services to be paid in that way.

6.7.2 All work to be paid for as Day works shall be recorded by the Service Provider on forms approved by the Procuring Entity. Each completed form shall be verified and signed by the Procuring Entity representative as indicated in Sub-Clause1.6 within two days of the Services being performed.

6.7.3 The Service Provider shall be paid for Day works subject to obtaining signed Day works forms as indicated in Sub-Clause6.7.2

7 Quality Control

7.1 Identifying Defects

The principle and modalities of Inspection of the Services by the Procuring Entity shall be as **indicated in the SCC.** The Procuring Entity shall check the Service Provider's performance and notify him of any Defects that are found. Such checking shall not affect the Service Provider's responsibilities. The Procuring Entity may instruct the Service Provider to search for a Defect and to uncover and test any service that the Procuring Entity considers may have a Defect. Defect Liability Period is as **defined in the SCC**.

Correction of Defects, and Lack of Performance Penalty

a) The Procuring Entity shall give notice to the Service Provider of any Defects before the end of the Contract. The Defects liability period shall be extended for as long as Defects remain to be corrected.

b) Every time notice a Defect is given, the Service Provider shall correct the notified Defect within the length of time specified by the Procuring Entity's notice.

c) If the Service Provider has not corrected a Defect within the time specified in the Procuring Entity's notice, the Procuring Entity will assess the cost of having the Defect corrected, the Service Provider will pay this amount and a Penalty for Lack of Performance calculated as described in Sub-Clause 3.8.

8 Settlement of Disputes

8.1 Contractor's Claims

8.1.1 If the Contractor considers himself to be entitled to any extension of the Time for Completion and/or any additional payment, under any Clause of these Conditions or otherwise in connection with the Contract, the Contractor shall give notice to the Project Manager, describing the event or circumstance giving rise to the claim. The notice shall be given as soon as practicable, and not later than 28 days after the Contractor became aware, or should have become aware, of the event or circumstance.

8.1.2 If the Contractor fails to give notice of a claim within such period of 28days, the Time for Completion shall not be extended, the Contractor shall not be entitled to additional payment, and the Procuring Entity shall be discharged from all liability in connection with the claim. Otherwise, the following provisions of this Sub-Clauses hall apply.

8.1.3 The Contractor shall also submit any other notices which are required by the Contract, and supporting particulars for the claim, all s relevant to such event or circumstance.

8.1.4 The Contractor shall keep such contemporary records as may be necessary to substantiate any claim, either on the Site or at another location acceptable to the Project Manager. Without admitting the Procuring Entity's liability, the Project Manager may, after receiving any notice under this Sub-Clause, monitor the record-keeping and /or instruct the Contractor to keep further contemporary records. The Contractor shall permit the Project Manager to inspect all these records, and shall (if instructed) submit copies to the Project Manager.

8.1.5 Within 42 days after the Contractor became aware (or should have become aware) of the event or circumstance giving rise to the claim, or within such other period as may be proposed by the Contractor and approved by the Project Manager, the Contractor shall send to the Project Manager a fully detailed claim which includes full supporting particulars of the basis of the claim and of the extension of time and /or additional payment claimed. If the event or circumstance giving rise to the claim has a continuing effect:

8.1.5.1 This fully detailed claim shall be considered as interim;

a) The Contractor shall send further interim claims at monthly intervals, giving the accumulated delay and /or amount claimed, and such further particulars as the Project Manager may reasonably require; and

b) The Contractor shall send a final claim within 28 days after the end of the effects resulting from the event or circumstance, or within such other period as may be proposed by the Contractor and approved by the Project Manager.

8.1.6 Within 42 days after receiving a claim or any further particulars supporting a previous claim, or within such other period as may be proposed by the Project Manager and approved by the Contractor, the Project Manager shall respond with approval, or with disapproval and detailed comments. He may also request any necessary further particulars, but shall nevertheless give his response on the principles of the claim within the above defined time period.

8.1.7 Within the above defined period of 42 days, the Project Manager shall proceed in accordance with Sub-Clause 3.5[Determinations] to agree or determine (i) the extension (if any) of the Time for Completion (before or after its expiry) in accordance with Sub-Clause 8.4 [Extension of Time for Completion], and/or (ii) the additional payment (if any) to which the Contractor is entitled under the Contract.

8.1.8 Each Payment Certificate shall include such additional payment for any claim as has been reasonably substantiated as due under the relevant provision of the Contract. Unless and until the particulars supplied are sufficient to substantiate the whole of the claim, the Contractor shall only been titled to payment for such part of the claim as he has be enable to substantiate.

8.1.9 If the Project Manager does not respond within the time framed fined in this Clause, either Party may consider that the claim is rejected by the Project Manager and any of the Parties may refer to Arbitration in accordance withSub-Clause8.2 [Matters that may be referred to arbitration].

8.1.10 The requirements of this Sub-Clause are in addition to those of any other Sub-Clause which may apply to a claim. If the Contract or fails to comply with this or another Sub-Clause in relation to any claim, any extension of time and/or additional payment shall take account of the extent (if any) to which the failure has prevented or prejudiced proper investigation of the claim, unless the claim is excluded under the second paragraph of this Sub- Clause.

8.2 Matters that may be referred to arbitration

8.2.1 Notwithstanding anything stated herein the following matters may be referred to arbitration before the practical completion of the Services or abandonment of the Services or termination of the Contract by either party:

a) The appointment of a replacement Project Manager upon the said person ceasing to act.

b) Whether or not the issue of an instruction by the Project Manager is empowered by these Conditions

c) Whetherornotacertificatehasbeenimproperlywithheldorisnotinaccordance with these Conditions.

e) Any dispute arising in respect of war risks or war damage.

f) All other matters shall only be referred to arbitration after the completion or alleged completion of the Services or termination or alleged termination of the Contract, unless the Procuring Entity and the Contractor agree otherwise in writing.

8.3 Amicable Settlement

8.3.1 Where a Notice of Dis satisfaction has been given, both Parties shall attempt to settle the dispute amicably before the commencement of arbitration. However, unless both Parties agree otherwise, the Party giving a Notice of Dissatisfaction in accordance with Sub-Clause 8.1 above should move to commence arbitration after the fifty-sixth day from the day on which a Notice of Dissatisfaction was given, even if no attempt at an amicable settlement has been made.

8.4 Arbitration

8.4.1 Any claim or dispute between the Parties arising out of or in connection with the Contract not settled amicably in accordance with Sub-Clause 8.3 shall be finally settled by arbitration. Arbitration shall be conducted in accordance with the Arbitration Laws of Kenya.

8.4.2 The arbitrators shall have full power to open up, review and revise any certificate, determination, instruction, opinion or valuation of the Project Manager, relevant to the dispute. Nothing shall disqualify representatives of the Parties and the Project Manager from being called as a witness and giving evidence before the arbitrators on any matter whatsoever relevant to the dispute.

8.4.3 Neither Party shall be limited in the proceedings before the arbitrators to the evidence, or to the reasons for dissatisfaction given in its Notice of Dissatisfaction.

8.4.4 Arbitration may be commenced prior to or after completion of the services. The obligations of the Parties, and the Project Manager shall not be altered by reason of any arbitration being conducted during the progress of the services.

8.4.5 The terms of the remuneration of each or all the members of Arbitration shall be mutually agreed upon by the Parties when agreeing the terms of appointment. Each Party shall be responsible for paying one-half of this remuneration.

8.5 Arbitration with proceedings

8.5.1 In case of any claim or dispute, such claim or dispute shall be notified in writing by either party to the other with a request to submit to arbitration and to concur in the appointment of an Arbitrator within thirty days of the notice. The dispute shall be referred to the arbitration and final decision of a person to be agreed between the parties. Failing agreement to concur in the appointment of an Arbitrator, the Arbitrator shall be appointed, on the request of the applying party, by the Chairman or Vice Chairman of any of the following professional institutions;

a) Law Society of Kenya or

b) Chartered Institute of Arbitrators (Kenya Branch)

8.5.2 The institution written to first by the aggrieved party shall take precedence over all other institutions.

8.5.3 The arbitration maybe on the construction of this Contractor on any matter or thing of what so ever nature arising there under or in connection there with, including any matter or thing left by this Contract to the discretion of the Project Manager, or the withholding by the Project Manager of any certificate to which the Contractor may claim to been titled to or the measurement and valuation referred to in clause 23.0 of these conditions, or the rights and liabilities of the parties subsequent to the termination of Contract.

8.5.4 Provided that no arbitration proceedings shall be commenced on any claim or dispute where notice of a claim or dispute has not been given by the applying party within ninety days of the occurrence or discovery of the matter or issue giving rise to the dispute.

8.5.5 Notwithstanding the issue of a notice as stated above, the arbitration of such a claim or dispute shall not commence unless an attempt has in the first instance been made by the parties to settle such claim or dispute amicably with or without the assistance of third parties. Proof of such attempt shall be required.

8.5.6 The Arbitrator shall, without prejudice to the generality of his powers, have powers to direct such measurements, computations, tests or valuations as may in his opinion be desirable in order to determine the rights of the parties and assess and award any sums which ought to have been the subject of or included in any certificate.

8.5.7 The Arbitrator shall, without prejudice to the generality of his powers, have powers to open up, review and revise any certificate, opinion, decision, requirement or notice and to determine all matters in dispute which shall be submitted to him in the same manner as if no such certificate, opinion, decision requirement or notice had been given.

8.5.8 The award of such Arbitrator shall be final and binding upon the parties.

8.6 Failure to Comply with Arbitrator's Decision

8.6.1 In the event that a Party fails to comply with a final and binding Arbitrator's decision, then the other Party may, without prejudice to any other rights it may have, refer the matter to a competent court of law.

9.1 The Adjudicator

9.1.1 Should the Adjudicator resign or die, or should the Procuring Entity and the Service Provider agree that the Adjudicator is not functioning in accordance with the provisions of the Contract; a new Adjudicator will be jointly appointed by the Procuring Entity and the Service Provider. In case of disagreement between the Procuring Entity and the Service Provider, within 30days, the Adjudicator shall be designated by the Appointing Authority **designated in the SCC** at the request of either party, within 14 days of receipt of such request.

9.2 The Adjudicator shall be paid by the hour at the rate **specified in the TDS and SCC,** together with reimbursable expenses of the type's **specified in the SCC**, and the cost shall be divided equally between the Procuring Entity and the Service Provider, whatever decision is reached by the Adjudicator. Either party may refer a decision of the Adjudicator to an Arbitrator within28 days of the Adjudicator's written decision. If neither party refers the dispute to arbitration within the above 28 days, the Adjudicator's decision will be final and binding.

B. SPECIAL CONDITIONS OF CONTRACT

SECTION IX - SPECIAL CONDITIONS OF CONTRACT *(TO BE COMPLETED WITH THE WINNING BIDDER DURING CONTRACTING)*

Number of GC Clause	Amendments of, and Supplements to, Clauses in the General Conditions of Contract
1.1(a)	The Adjudicator is _____
1.1(w)	Project Manager is _____
1.1(e)	The contract name is _____
1.1(h)	The Procuring Entity is _____
1.1(m)	The Member in Charge is _____
1.1(p)	The Service Provider is _____
1.4	The addresses are:_____ Procuring Entity: _____ Attention: _____ Telex: _____ Service Provider:_____ Attention: _____ Email address_____
1.6	The Authorized Representatives are: For the Procuring Entity: _____ For the Service Provider:_____
2.1	The date on which this Contract shall come into effect is _____.
2.2.2	The Starting Date for the commencement of Services is _____.
2.3	The Intended Completion Date is _____.
2.4.1	If the value engineering proposal is approved by the Procuring Entity the amount to be paid to the Service Provider shall be ___% (insert appropriate percentage. The percentage is normally up to 50%) of the reduction in the Contract Price.
3.2.3	Activities prohibited after termination of this Contract are: _____ _____
3.4	The risks and coverage by insurance shall be: (i) Third Party motor vehicle _____ (ii) Third Party liability _____ (iii) Procuring Entity's liability and workers' compensation _____ (iv) Professional liability _____ (v) Loss or damage to equipment and property _____
3.5(d)	The other actions are _____.]
3.7	Restrictions on the use of documents prepared by the Service Provider are: _____

3.8.1	The liquidated damages rate is _____ per day The maximum amount of liquidated damages for the whole contract is _____percent of the final Contract Price.
3.8.3	The percentage _____ to be used for the calculation of Lack of performance Penalty(ies) is _____.
5.1	The assistance and exemptions provided to the Service Provider are: _____
6.2(a)	The amount in Kenya Shillings _____.
6.3.2	The performance incentive paid to the Service Provider shall be: _____ _____
6.4	Payments shall be made according to the following schedule: • Advance for Mobilization, Materials and Supplies: _____ percent of the Contract Price shall be paid on the commencement date against the submission of a bank guarantee for the same. • Progress payments in accordance with the milestones established as follows, subject to certification by the Procuring Entity, that the Services have been rendered satisfactorily, pursuant to the performance indicators: _____ (indicate milestone and/or percentage)_____ _____ (indicate milestone and/or percentage)_____ and _____ (indicate milestone and/or percentage)_____ Should the certification not be provided, or refused in writing by the Procuring Entity within one month of the date of the milestone, or of the date of receipt of the corresponding invoice, the certification will be deemed to have been provided, and the progress payment will be released at such date. • The amortization of the Advance mentioned above shall commence when the progress payments have reached 25% of the contract price and be completed when the progress payments have reached 75%. • The bank guarantee for the advance payment shall be released when the advance payment has been fully amortized.
6.5	Payment shall be made within _____ days of receipt of the invoice and the relevant documents specified in Sub-Clause 6.4, and within _____days in the case of the final payment. The interest rate is _____.
6.6.1	Price adjustment is _____ in accordance with Sub-Clause 6.6. The coefficients for adjustment of prices are _____: (a) For local currency: A_L is _____ B_L is _____ C_L is _____ L_{mc} and L_{oc} are the index for Labor from _____ I_{mc} and I_{oc} are the index for _____ from _____ (b) For foreign currency A_F is _____ B_F is _____ C_F is _____ L_{mc} and L_{oc} are the index for Labor from _____ I_{mc} and I_{oc} are the index for _____ from _____

7.1	The principle and modalities of inspection of the Services by the Procuring Entity are as follows: _____ The Defects Liability Period is _____.
9.1	The designated Appointing Authority for a new Adjudicator is_____ _____
9.2	The Adjudicator is _____. Who will be paid a rate of _____ per hour of work. The following reimbursable expenses are recognized: _____

C. APPENDICES

Appendix A - Description of the Services

Give detailed descriptions of the Services to be provided, dates for completion of various tasks, place of performance for different tasks, specific tasks to be approved by Procuring Entity, etc.

Appendix B - Schedule of Payments and Reporting Requirements

List all milestones for payments and list the format, frequency, and contents of reports or products to be delivered; persons to receive them; dates of submission; etc. If no reports are to be submitted, state here "Not applicable."

Appendix C - Breakdown of Contract Price

List here the elements of cost used to arrive at the breakdown of the lump-sum price:

1. *Rates for Equipment Usage or Rental or for Personnel (Key Personnel and other Personnel).*
2. *Reimbursable expenditures.*

This appendix will exclusively be used for determining remuneration for additional Services.

Appendix D - Services and Facilities Provided by the Procuring Entity

D. FORMS

SECTION X -CONTRACT FORMS

FORM NO. 1 - PERFORMANCE SECURITY – (Unconditional Demand Bank Guarantee)

[Guarantor letterhead or SWIFT identifier code]

Beneficiary:_____*[insert name and Address of* Procuring Entity*]*

Date:_____*[Insert date of issue]*

PERFORMANCE GUARANTEE No.:_____

Guarantor:..... *[Insert name and address of place of issue, unless indicated in the letterhead]*

1. We have been informed that_____(hereinafter called "the Applicant") has entered into Contract No._____*dated*_____with the Beneficiary, for the execution of_____ (herein after called "the Contract").

2. Furthermore, we understand that, according to the conditions of the Contract, a performance guarantee is required.

3. At the request of the Applicant, we as Guarantor, hereby irrevocably under take to pay the Beneficiary any sum or sums not exceeding in total an amount of_____(),[1] such sum being payable in the types and proportions ofcurrenciesinwhichtheContractPriceispayable,uponreceiptbyusoftheBeneficiary'scomplyingdemand supported by the Beneficiary's statement, whether in the demand itself or in a separate signed document accompanying or identifying the demand, stating that the Applicant is in breach of its obligation(s) under the Contract, without the Beneficiary needing to prove or to show grounds for your demand or the sum specified therein.

4. This guarantee shall expire, no later than the….Day of……, 2…[2], and any demand for payment under it must be received by us at this office indicated above on or before that date.

5. The Guarantor agrees to a one-time extension of this guarantee for a period not to exceed *[six months] [one year],* in response to the Beneficiary's written request for such extension, such request to be presented to the Guarantor before the expiry of the guarantee."_____

[Name of Authorized Official, signature(s) and seals/stamps]

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

SITE VISIT FORM

(TO BE RETURNED DULY SIGNED AND STAMPED WITH TENDER DOCUMENT)

THE PROVISION OF OFFICE SUITE SOFTWARE AND RELATED END POINT SECURITY.

TENDER NO: KCAA/018/2025-2026.

THIS IS TO CONFIRM THAT ---------- (COMPANY NAME) HAS MADE A SITE VISIT TO THE KENYA CIVIL AVIATION AUTHORITY ON **FRIDAY, 20TH FEBRUARY,2026 AT 1000 HOURS.**

COMPANY REPRESENTATIVE

NAME ----------DESIGNATION----------

SIGNED ---------- DATE ----------

OFFICIAL STAMP

KCAA REPRESENTATIVE

NAME ----------DESIGNATION----------

SIGNED ---------- DATE ----------OFFICIAL

STAMP