KENYA CIVIL AVIATION AUTHORITY

TENDER NO. KCAA/041/2019-2020

TENDER FOR THE SUPPLY, INSTALLATION, CONFIGURATION, INTEGRATION, TESTING, TRAINING AND COMMISIONING OF AN ADVANCED HARDWARE FIREWALL AND NETWORK SEGMENTATION SERVICES AT THE EAST AFRICAN SCHOOL OF AVIATION IN EMBAKASI.

DATE OF NOTICE: TUESDAY 25TH FEBRUARY, 2020

CLOSING DATE: TUESDAY, 11TH MARCH, 2020 AT 11:00AM

Notes:

1. Mandatory pre-bid meeting to be held on Thursday, 5th March, 2020 at 11am to 1pm at EASA in Embakasi

2. All bidders must note that KCAA communicates only in writing to all interested bidders during the entire tendering process

TABLE OF CONTENTS

Introduction

1.1 Kenya Civil Aviation herein referred to KCAA wishes to invite tenders **for the supply, installation, configuration, integration, testing, training and commissioning of an advanced hardware firewall and network segmentation services at EASA.**

1.2 Bidders must possess the necessary professional and technical qualifications and competence, financial resources, equipment and other physical facilities, managerial capability, experience in the provision of the services, reputation and the personnel to perform the contract. They should also have legal capacity to enter into the contract and that they have continuously fulfilled obligations to pay taxes and social security contributions.

SECTION I – INVITATION TO TENDER

TENDER NAME: **TENDER FOR SUPPLY, INSTALLATION, CONFIGURATION, INTEGRATION, TESTING, TRAINING AND COMMISSIONING OF AN ADVANCED HARDWARE FIREWALL AND NETWORK SEGMENTATION SERVICES AT EASA**

TENDER REF NO: KCAA/042/2019-2020

TENDER NOTICE DATE: Tuesday, 25th February, 2020

1.1   KCAA **invites** sealed bids from all interested candidates **for the supply, installation, configuration, integration, testing, training and commissioning of an advanced hardware firewall and network segmentation services at EASA.**

1.2   Interested eligible candidates may obtain further information from and inspect the tender documents at **KCAA Procurement Office on ground floor, Aviation House Jomo Kenyatta International Airport (JKIA)** during normal office working hours (8.00am-1.00pm, 2.00pm – 5.00pm). *Bidders may also view and download the bidding document from KCAA website:www.kcaa.or.ke* or from the *www.supplier.treasury.go.ke* and immediately forward their particulars for records and for the purposes of receiving any further tender clarifications and/or addendums to procurement@kcaa.or.ke.

1.3   **A mandatory pre-bid meeting shall be held on Thursday, 5th March, 2020 at 11am to 1pm at EASA in Embakasi.**

1.4   A complete set of tender documents may be obtained by interested candidates upon payment of a non-refundable fee of One thousand Kenya shillings **(Ksh 1,000.00)** in cash or bankers cheque payable to Director General, Kenya Civil Aviation Authority. Bidders who download the tender document will not be required to pay.

1.5   Prices quoted should be net inclusive of all taxes and delivery costs, must be   expressed in Kenya shillings or easily convertible foreign currency and shall remain valid for a period of 90 days from the Closing date of the tender.

1.6   Completed tender documents are to be enclosed in plain sealed envelopes marked with tender reference number and be deposited in the Tender Box at **Ground Floor, Aviation House, Jomo Kenyatta International Airport,** or be addressed to:

<div align="center">

The Director General,
Kenya Civil Aviation Authority,
P.O Box 30163-00100, Nairobi

</div>

So as to be received on or before **Wednesday, 11th March, 2020 at 11.00 am.**

1.7   Tenders will be opened immediately thereafter in the presence of the Candidates or their representatives who choose to attend at **KCAA Auditorium on Ground Floor, Aviation House, JKIA, Nairobi.**

<div align="center">

Manager Procurement
For: Director General

</div>

SECTION II – INSTRUCTIONS TO TENDERERS

TABLE OF CONTENTS   Page

SECTION II INSTRUCTIONS TO TENDERERS

2.1   Eligible tenderers

2.1.1. This Invitation to tender is open to all tenderers eligible as described in the instructions to tenderers. Successful tenderers shall provide the services for the stipulated duration from the date of commencement (hereinafter referred to as the term) specified in the tender documents.

2.1.2. The procuring entity's employees, committee members, board members and their relatives (spouse and children) are not eligible to participate in the tender unless where specially allowed under section 131 of the Act.

2.1.3. Tenderers shall provide the qualification information statement that the tenderer (including all members, of a joint venture and subcontractors) is not associated, or have been associated in the past, directly or indirectly, with a firm or any of its affiliates which have been engaged by the Procuring entity to provide consulting services for the preparation of the design, specifications, and other documents to be used for the procurement of the services under this Invitation for tenders.

2.1.4. Tenderers involved in corrupt or fraudulent practices or debarred from participating in public procurement shall not be eligible.

2.2   **Cost of tendering**

2.2.1   The Tenderer shall bear all costs associated with the preparation and submission of its tender, and the procuring entity, will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the tendering process.

2.2.2   The price to be charged for the tender document shall not exceed Kshs.1,000/=

2.2.3   The procuring entity shall allow the tenderer to review the tender document free of charge before purchase.

2.3   Contents of tender documents

2.3.1. The tender document comprises of the documents listed below and addenda issued in accordance with clause 6 of these instructions to tenders.

       i)   Instructions to tenderers
       ii)   General Conditions of Contract
       iii)   Special Conditions of Contract
       iv)   Schedule of Requirements
       v)   Details of service
       vi)   Form of tender
       vii)   Price schedules
       viii)   Contract form
       ix)   Confidential business questionnaire form
       x)   Tender security form
       xi)   Performance security form

2.3.2. The Tenderer is expected to examine all instructions, forms, terms, and specifications in the tender documents. Failure to furnish all information required by the tender documents or to submit a tender not substantially responsive to the tender documents in every respect will be at the tenderers risk and may result in the rejection of its tender.

2.4 Clarification of Documents

2.4.1. A prospective candidate making inquiries of the tender document may notify the Procuring entity in writing or by post, fax or email at the entity's address indicated in the Invitation for tenders. The Procuring entity will respond in writing to any request for clarification of the tender documents, which it receives no later than seven (7) days prior to the deadline for the submission of tenders, prescribed by the procuring entity. Written copies of the Procuring entities response (including an explanation of the query but without identifying the source of inquiry) will be sent to all prospective tenderers who have received the tender documents"

2.4.2. The procuring entity shall reply to any clarifications sought by the tenderer within 3 days of receiving the request to enable the tenderer to make timely submission of its tender.

2.5 Amendment of documents
2.5.1. At any time prior to the deadline for submission of tenders, the Procuring entity, for any reason, whether at its own initiative or in response to a clarification requested by a prospective tenderer, may modify the tender documents by issuing an addendum.

2.5.2. All prospective tenderers who have obtained the tender documents will be notified of the amendment by post, fax or email and such amendment will be binding on them.

2.5.3. In order to allow prospective tenderers reasonable time in which to take the amendment into account in preparing their tenders, the Procuring entity, at its discretion, may extend the deadline for the submission of tenders.

2.6 Language of tender
2.6.1. The tender prepared by the tenderer, as well as all correspondence and documents relating to the tender exchanged by the tenderer and the Procuring entity, shall be written in English language. Any printed literature furnished by the tenderer may be written in another language provided they are accompanied by an accurate English translation of the relevant passages in which case, for purposes of interpretation of the tender, the English translation shall govern.

2.7 **Documents Comprising the Tender**
The tender prepared by the tenderer shall comprise the following components:

(a) A Tender Form and a Price Schedule completed in accordance with paragraph 9, 10 and 11 below.

(b) Documentary evidence established in accordance with Clause 2.11 that the tenderer is eligible to tender and is qualified to perform the contract if its tender is accepted;

(c) Tender security furnished is in accordance with Clause 2.12
(d)Confidential business questionnaire

2.8 **Form of Tender**

2.8.1 The tenderers shall complete the Form of Tender and the appropriate Price Schedule furnished in the tender documents, indicating the services to be performed.

2.9 **Tender Prices**

2.9.1 The tenderer shall indicate on the Price schedule the unit prices where applicable and total tender prices of the services it proposes to provide under the contract.

2.9.2 Prices indicated on the Price Schedule shall be the cost of the services quoted including all customs duties and VAT and other taxes payable:

2.9.3 Prices quoted by the tenderer shall remain fixed during the term of the contract unless otherwise agreed by the parties. A tender submitted with an adjustable price quotation will be treated as non-responsive and will be rejected, pursuant to paragraph 2.22.

2.9.4 Contract price variations shall not be allowed for contracts not exceeding one year (12 months)

2.9.5 Where contract price variation is allowed, the variation shall not exceed 10% of the original contract price.

2.9.6 Price variation requests shall be processed by the procuring entity within 30 days of receiving the request.

2.10 **Tender Currencies**

2.10.1 Prices shall be quoted in Kenya Shillings unless otherwise specified in the appendix to in Instructions to Tenderers

2.11 Tenderers Eligibility and Qualifications.

2.11.1 Pursuant to Clause 2.1 the tenderer shall furnish, as part of its tender, documents establishing the tenderers eligibility to tender and its qualifications to perform the contract if its tender is accepted.

2.11.2 The documentary evidence of the tenderers qualifications to perform the contract if its tender is accepted shall establish to the Procuring entity's satisfaction that the tenderer has the financial and technical capability necessary to perform the contract.

2.12 **Tender Security**

2.12.1 The tenderer shall furnish, as part of its tender, a tender security for the amount and form specified in the Invitation to tender.

2.12.2 The tender security shall be in the amount not exceeding 2 per cent of the tender price.

2.12.2 The tender security is required to protect the Procuring entity against the risk of Tenderer's conduct which would warrant the security's forfeiture, pursuant to paragraph 2.12.7

2.12.3 The tender security shall be denominated in a Kenya Shillings or in another freely convertible currency and shall be in the form of:

> a) A bank guarantee.
> b) Cash.
> c) Such insurance guarantee approved by the Authority.
> d) Letter of credit

2.12.4 Any tender not secured in accordance with paragraph 2.12.1 and 2.12.3 will be rejected by the Procuring entity as non responsive, pursuant to paragraph 2.20

2.12.5 Unsuccessful tenderer's security will be discharged or returned as promptly as possible as but not later than thirty (30) days after the expiration of the period of tender validity prescribed by the procuring entity.

2.12.6 The successful tenderer's tender security will be discharged upon the tenderer signing the contract, pursuant to paragraph 2.29, and furnishing the performance security, pursuant to paragraph 2.30.

2.12.7 The tender security may be forfeited:

(a) If a tenderer withdraws its tender during the period of tender validity specified by the procuring entity on the
Tender Form; or
(b) In the case of a successful tenderer, *if* the tenderer fails:
(i) to sign the contract in accordance with paragraph 30
or
(ii) to furnish performance security in accordance with paragraph 31.

(c) If the tenderer rejects, correction of an error in the tender.

2.13 **Validity of Tenders**

2.13.1 Tenders shall remain valid for 90 days or as specified in the invitation to tender after date of tender opening prescribed by the Procuring entity, pursuant to paragraph 2.18. A tender valid for a shorter period shall be rejected by the Procuring entity as nonresponsive.

2.13.2 In exceptional circumstances, the Procuring entity may solicit the Tenderer's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The tender security provided under paragraph 2.12 shall also be

suitably extended. A tenderer may refuse the request without forfeiting its tender security. A tenderer granting the request will not be required nor permitted to modify its tender.

2.14 Format and Signing of Tender

2.14.1 The tenderer shall prepare two copies of the tender, clearly / marking each **"ORIGINAL TENDER"** and **"COPY OF TENDER,"** as appropriate. In the event of any discrepancy between them, the original shall govern.

2.14.2 The original and all copies of the tender shall be typed or written in indelible ink and shall be signed by the tenderer or a person or persons duly authorized to bind the tenderer to the contract. All pages of the tender, except for unamended printed literature, shall be initialed by the person or persons signing the tender.

2.14.3 The tender shall have no interlineations, erasures, or overwriting except as necessary to correct errors made by the tenderer, in which case such corrections shall be initialed by the person or persons signing the tender.

2.15 Sealing and Marking of Tenders

2.15.1 The tenderer shall seal the original and each copy of the tender in separate envelopes, duly marking the envelopes as "ORIGINAL" and "COPY." The envelopes shall then be sealed in an outer envelope.
The inner and outer envelopes shall:

(a) be addressed to the Procuring entity at the address given in the invitation to tender

(b) Bear, tender number and name in the invitation to tender and the words: "**DO NOT OPEN BEFORE WEDNESDAY, 11TH MARCH, 2020 AT 11.00AM.**

2.15.3 The inner envelopes shall also indicate the name and address of the tenderer to enable the tender to be returned unopened in case it is declared "late".

2.15.4 If the outer envelope is not sealed and marked as required by paragraph 2.15.2, the Procuring entity will assume no responsibility for the tender's misplacement or premature opening.

2.16 Deadline for Submission of Tenders

2.16.1 Tenders must be received by the Procuring entity at the address specified under paragraph 2.15.2 no later Than **Wednesday, 11th March, 2020 at 11.00am**

2.16.2 The procuring entity may, at its discretion, extend this deadline for the submission of tenders by amending the tender documents in accordance with paragraph 6, in which case all rights and obligations of the procuring entity and candidates previously subject to the deadline will thereafter be subject to the deadline as extended.

2.16.3 Bulky tenders which will not fit in the tender box shall be received by the procuring entity as provided for in the appendix.

2.17   Modification and withdrawal of tenders

2.17.1 The tenderer may modify or withdraw its tender after the tender's submission, provided that written notice of the modification , including substitution or withdrawal of the tender's is received by the procuring entity prior to the deadline prescribed for the submission of tenders.

2.17.2 The Tenderer's modification or withdrawal notice shall be prepared, sealed, marked, and dispatched in accordance with the provisions of paragraph 2.15. A withdrawal notice may also be sent by cable, but followed by a signed confirmation copy, postmarked not later than the deadline for submission of tenders.

2.17.3 No tender may be modified after the deadline for submission of tenders.

2.17.4 No tender may be withdrawn 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 Tender Form. Withdrawal of a tender during this interval may result in the Tenderer's forfeiture of its tender security, pursuant to paragraph 2.12.7.

2.17.5 The procuring entity may at any time terminate procurement proceedings before contract award and shall not be liable to any person for the termination.

2.17.6 The procuring entity shall give prompt notice of the termination to the tenderers and on request give its reasons for termination within 14 days of receiving the request from any tenderer.

2.18   Opening of Tenders

2.18.1 The Procuring entity will open all tenders in the presence of tenderers' representatives who choose to attend, at **11.00am, Wednesday, 11ᵗʰ March, 2020 at KCAA Auditorium on Ground Floor, Aviation House, JKIA, Nairobi.** The tenderers' representatives who are present shall sign a register evidencing their attendance.

2.18.3 The tenderers' names, tender modifications or withdrawals, tender prices, discounts, and the presence or absence of requisite tender security and such other details as the Procuring Entity, at its discretion, may consider appropriate, will be announced at the opening.

2.18.4 The procuring entity will prepare minutes of the tender opening which will be submitted to the tenderers that signed the tender opening register and will have made the request.

2.19   Clarification of tenders

2.19.1 To assist in the examination, evaluation and comparison of tenders the procuring entity may at its discretion, ask the tenderer for a clarification of its tender. The request for clarification and the response shall be in writing, and no change in the prices or substance shall be sought, offered, or permitted.

2.19.2 Any effort by the tenderer to influence the procuring entity in the procuring entity's tender evaluation, tender comparison or contract award decisions may result in the rejection of the tenderers tender.

Comparison or contract award decisions may result in the rejection of the tenderers' tender.

2.20   **Preliminary Examination and Responsiveness**

2.20.1 The Procuring entity will examine the tenders to determine whether they are complete, whether any computational errors have been made, whether required securities have been furnished whether the documents have been properly signed, and whether the tenders are generally in order.

2.20.2 Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected. If the candidate does not accept the correction of the errors, its tender will be rejected, and its tender security may be forfeited. If there is a discrepancy between words and figures, the amount in words will prevail.

2.20.3 The Procuring entity may waive any minor informality or nonconformity or irregularity in a tender which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any tenderer.

2.20.4 Prior to the detailed evaluation, pursuant to paragraph 23, the Procuring entity will determine the substantial responsiveness of each tender to the tender documents. For purposes of these paragraphs, a substantially responsive tender is one which conforms to all the terms and conditions of the tender documents without material deviations. The Procuring entity's determination of a tender's responsiveness is to be based on the contents of the tender itself without recourse to extrinsic evidence.

2.20.5 If a tender is not substantially responsive, it will be rejected by the Procuring entity and may not subsequently be made responsive by the tenderer by correction of the nonconformity.

2.21   **Conversion to a single currency**

2.21.1 Where other currencies are used, the procuring entity will convert those currencies to Kenya shillings using the selling exchange rate on the date of tender closing provided by the central bank of Kenya.

2.22   **Evaluation and comparison of tenders**.

2.22.1 The procuring entity will evaluate and compare the tenders which have been determined to be substantially responsive, pursuant to paragraph 2.20

2.22.2 The comparison shall be of the price including all costs as well as duties and taxes payable on all the materials to be used in the provision of the services.

2.22.3 The Procuring entity's evaluation of a tender will take into account, in addition to the tender price, the following factors, in the manner and to the extent indicated in paragraph 2.22.4 and in the technical specifications:

        (a) Operational plan proposed in the tender;

(b) Deviations in payment schedule from that specified in the Special Conditions of Contract;

2.22.4   Pursuant to paragraph 22.3 the following evaluation methods will be applied:

(a) *Operational Plan.*

The Procuring entity requires that the services under the Invitation for Tenders shall be performed at the time specified in the Schedule of Requirements. Tenders offering to perform longer than the procuring entity's required delivery time will be treated as non-responsive and rejected.

(b) *Deviation in payment schedule.*

Tenderers shall state their tender price for the payment on a schedule outlined in the special conditions of contract. Tenders will be evaluated on the basis of this base price. Tenderers are, however, permitted to state an alternative payment schedule and indicate the reduction in tender price they wish to offer for such alternative payment schedule. The Procuring entity may consider the alternative payment schedule offered by the selected tenderer.

2.22.5   The tender evaluation committee shall evaluate the tender within 15 days from the date of opening the tender.

2.22.6   To qualify for contract awards, the tenderer shall have the following:-

(a)	Necessary qualifications, capability experience, services, equipment and facilities to provide what is being procured.
(b)	Legal capacity to enter into a contract for procurement
(c)	Shall not be insolvent, in receivership, bankrupt or in the process of being wound up and is not the subject of legal proceedings relating to the foregoing
(d)	Shall not be debarred from participating in public procurement.

2.23.   Contacting the procuring entity

2.23.1   Subject to paragraph 2.19, no tenderer shall contact the procuring entity on any matter relating to its tender, from the time of the tender opening to the time the contract is awarded.

2.23.2   Any effort by a tenderer to influence the procuring entity in its decisions on tender evaluation tender comparison or contract award may result in the rejection of the tenderers tender.

2.24 Award of Contract

a) Post qualification

2.24.1   In the absence of pre-qualification, the Procuring entity will determine to its satisfaction whether the tenderer that is selected as having submitted the lowest evaluated responsive tender is qualified to perform the contract satisfactorily.

2.24.2 The determination will take into account the tenderer's financial and technical capabilities. It will be based upon an examination of the documentary evidence of the tenderers qualifications submitted by the tenderer, pursuant to paragraph 2.1.2, as well as such other information as the Procuring entity deems necessary and appropriate.

2.24.3 An affirmative determination will be a prerequisite for award of the contract to the tenderer. A negative determination will result in rejection of the Tenderer's tender, in which event the Procuring entity will proceed to the next lowest evaluated tender to make a similar determination of that Tenderer's capabilities to perform satisfactorily.

b)   **Award Criteria**

2.24.3 Subject to paragraph 2.29 the Procuring entity will award the contract to the successful tenderer whose tender has been determined to be substantially responsive and has been determined to be the lowest evaluated tender, provided further that the tenderer is determined to be qualified to perform the contract satisfactorily.

2.24.4 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 thereby incurring any liability to the affected tenderer or tenderers or any obligation to inform the affected tenderer or tenderers of the grounds for the procuring entity's action. If the procuring entity determines that none of the tenderers is responsive; the procuring entity shall notify each tenderer who submitted a tender.

2.24.5 A tenderer who gives false information in the tender document about its qualification or who refuses to enter into a contract after notification of contract award shall be considered for debarment from participating in future public procurement.

2.25   **Notification of award**

2.25.1 Prior to the expiration of the period of tender validity, the Procuring entity will notify the successful tenderer in writing that its tender has been accepted.

2.25.2 The notification of award will signify the formation of the Contract subject to the signing of the contract between the tenderer and the procuring entity pursuant to clause 2.29. Simultaneously the other tenderers shall be notified that their tenders have not been successful.

2.25.3 Upon the successful Tenderer's furnishing of the performance security pursuant to paragraph 31, the Procuring entity will promptly notify each unsuccessful Tenderer and will discharge its tender security, pursuant to paragraph 2.12

2.26   **Signing of Contract**

2.26.1 At the same time as the Procuring entity notifies the successful tenderer that its tender has been accepted, the Procuring entity will simultaneously inform the other tenderers that their tenders have not been successful.

2.26.2 Within Thirty (30) days of receipt of the Contract Form, the successful tenderer shall sign and date the contract and return it to the Procuring entity.

2.26.3   The parties to the contract shall have it signed within 30 days from the date of notification of contract award unless there is an administrative review request.

2.27   **Performance Security**

2.27.1   Within fourteen (14) days of the receipt of notification of award from the Procuring entity, the successful tenderer shall furnish the performance security in accordance with the Conditions of Contract, in the Performance Security Form provided in the tender documents, or in another form acceptable to the Procuring entity.

2.27.2   Failure of the successful tenderer to comply with the requirement of paragraph 2.29 or paragraph 2.30.1 shall constitute sufficient grounds for the annulment of the award and forfeiture of the tender security, in which event the Procuring entity may make the award to the next lowest evaluated or call for new tenders.

2.28   **Corrupt or Fraudulent Practices**

2.28.1   The Procuring entity requires that tenderers observe the highest standard of ethics during the procurement process and execution of contracts. A tenderer shall sign a declaration that he has not and will not be involved in corrupt or fraudulent practices.

2.28.1   The procuring entity will reject a proposal for award if it determines that the tenderer recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question;

2.28.2   Further, a tenderer who is found to have indulged in corrupt or fraudulent practices risks being debarred from participating in public procurement in Kenya.

Appendix to instructions to tenderers

The following information for procurement of services shall complement or amend the provisions of the instructions to tenderers. Wherever there is a conflict between the provisions of the instructions to tenderers and the provisions of the appendix, the provisions of the appendix herein shall prevail over those of the instructions to tenderers

Instructions to tenderers	Particulars of appendix to instructions to tenderers
2.1	The Form of Tender must be filled and signed.
2.10	*Particulars of other currencies allowed.* Price should be in Kenya shillings only or a freely convertible currency.
2.12	Tender security required is **Kshs 190,000.00** in form of a bank guarantee or a banker's cheque from a reputable bank in Kenya or an insurance from insurance agencies allowed by public procurement Oversight Authority) valid for **120 days** from the date of closing date of the tender.
2.13	**A mandatory pre-bid meeting to be held on Thursday, 5th March, 2020 at 11am to 1pm at EASA.**
2.13.1	Tender shall remain valid for a period of **120 days** from the date of opening
2.14	**All the pages of the original and copies of the tender submitted by the bidders must be serialized (paged)**
2.14.1	Bidders shall provide **1 ORIGINAL** copy of the tender document clearly marked original and **1** other copy marked COPY all placed in one envelope and tender title and number and closing date clearly written on top of the envelope
2.15	**Deadline for Submission of Tenders/Closing date shall be Wednesday, 11th March, 2020 at 11:00am**
2.16	Performance security of 10% of the contract price will **NOT** be required from the winning bidder after the award of the tender

EVALUATION CRITERIA

Kenya Civil Aviation Authority will consider the following three categories of criteria to evaluate the bids:-
a) Part A: Mandatory Tender Documentation,
b) General requirements (Mandatory)
c) Part B: Mandatory Technical Requirements,
d) Financial Evaluation (Quoted Prices).

Part A: Mandatory Tender Documentation

No.	Documents to be submitted	Pass/Fail
1.	**Ineligibility: -** Bidders and associated firms who have existing ongoing contracts with KCAA which have delayed beyond the original scheduled completion period in the contract or having none performing records or terminated contracts are not eligible to participate.	
2.	**Project commitment/plan** – Bidders **MUST** attach sample project plan/work programme clearly indicating the **expected completion of the project within shortest time possible**. Please note, there shall be no extension of period.	
3.	**Tender security of Kshs. 190,000.00** - in form of a bank guarantee or a banker's cheque from a reputable bank in Kenya or from insurance companies allowed by public procurement Oversight Authority and valid for 120 days from the date of closing of the tender.	
4.	Written power of attorney of the signatory of the tender to commit the tenderer.	
5.	**Manufacturer's Authorization:** Bidders MUST attach proof of a valid appointment of dealership by the manufacturer of the firewall hardware. **NB:** KCAA will have the rights of confirmation of the same.	
6.	Certificate of Incorporation/Registration.	
7.	**A mandatory filled site survey form/pre-bid meeting attendance** • Site visit forms must be filled and signed by the appointed **Kenya Civil Aviation Authority (KCAA/ EASA)** representative for the bidder interested to bid. Bidders will be registered during the meeting.	
8.	Attach a Valid Tax Compliance certificate.	
9.	Provide a warranty for three (3) years	
10.	**1 Original, 1 Copy of bid documents and MUST be serialized (paged) and a soft copy in a CD/DVD**	
11.	Duly filled, signed and stamped confidential business questionnaire (Indicate all the directors and respective shares).	
12.	Duly signed Sworn Anti-corruption affidavit by the commissioner of oaths	
13.	Audited Accounts for the past two (2) years **(2019/2018 and 2017)**	
14.	Submit a statement in the bidder's letter head that the company is not insolvent, in receivership, bankrupt or in the process of being wound up.	
15.	Submit a statement in the bidder's letter head indicating that the person or his or her sub-contractor, if any is not debarred from participating in procurement proceedings.	
16.	Submit a statement in the bidder's letter head indicating that the person participating in procurement proceedings has not been convicted of corrupt or fraudulent practices	
	PASS/FAIL	

INSTRUCTIONS TO BIDDERS

1. The specifications requirements consist of four parts. All the requirements are mandatory. Bidders must indicate their response on all the requirements.
2. Bidders MUST be certified partners at least Silver and above for the appliance they are providing (attach manufacturer's authorization partnership certificate)
3. Bidders MUST respond in writing (detailed sentence responses) in each table on the Vendor's response column. Responses such as marking compliant, partially compliant, non-compliant, (√) or (X) shall be treated as **INVALID entries** and shall not be evaluated.
4. Datasheets/Brochures MUST be attached for the appliance to be supplied. The datasheet **MUST specify exact make, series and model**.

Part 1: General Requirements

No	Requirement	Bidder's Response (indicate cross reference in the bid document)
Firewall Requirements (evidences MUST be attached for each requirement)		
1.	The proposed solution MUST be in the Leaders Quadrant of Gartner magic quadrant for Enterprise Network Firewall (ENF).	
2.	The proposed solution MUST be in the NSS Labs Scoring; a) 2019 Next Generation Firewall (NGFW) Test (Recommended) b) 2018 and 2019 Datacenter Intrusion Prevention Systems (DCIPS) Test (Recommended) c) 2019 Breach Prevention Systems (Recommended)	
3.	The proposed solution MUST be certified by ICSA Labs in the following tests; a) 2019 ICSA labs Firewall test b) 2019 ICSA labs Network IPS test c) 2019 ICSA labs SSL-TLS test	
Capacity Requirements		
4.	Client References - Vendor shall provide at least 3 references from enterprise clients showing proof of implementation of an enterprise level IT data center firewall. The evidence submitted shall include: - Project completion certificates, project sign-offs and service level agreement where applicable	
5.	Certificate of Accreditation from ICT Authority. At least category 2 in both Information Security and Infrastructure.	
6.	Personnel Competencies -Vendor shall provide a tabulated matrix of key personnel indicating relevant skills and competencies for each. The Bidder Must have Engineers certified to high level of security certifications	

	for the proposed solutions i.e. **Expert and Professional level (attach certificate / any other relevant evidence)**	
7.	Partnership level - Vendor must be a certified partner for the appliance they are providing. At a minimum the Vendor's partnership level MUST, be Silver or higher. (Certified Manufacturer's partnership certificate MUST be attached **(NB: Not distributor or reseller letter**)	
Infrastructure Requirements		
8.	Firewall Services - The solution shall facilitate publishing and access of web applications hosted on a virtual machine through https. Ability to map multiple web applications to a single public IP or different public IP's.	
9.	Application services: The solution MUST allow granular access or denial of various web services and ports. Additionally, support the creation of custom web ports or applications in which one can grant or block access.	
10.	Segmentation - Segment network through implementation of a DMZ for public facing Servers and a Server farm VLAN for internal Servers. Implementation shall be done in such a manner that web applications can be provisioned easily and Server services shall be readily available to cable and Wi-Fi connected internal users. **NB: EASA shall provide the Core-switch.**	
11.	Network monitoring & visibility - Real time visibility of inbound and outbound traffic. Visibility shall be granular to the extent of obtaining per user and/or application visibility, furthermore a bandwidth management feature allowing priority to applications e.g. locally hosted web business applications. Additionally, the solution shall provide real time monitoring and logging of events displayed through status dashboard.	
12.	Reporting - Availability of system and custom reports. At a minimum the following reports shall be extracted: - Top domains. Top users, top applications and top threats detected.	
Other Mandatory Requirements		
13.	Site survey form - Bidders MUST carry out site survey and have the site survey from dully filled and stamped.	
14.	Network diagram - Bidders MUST attach proposed network diagram detailing all the infrastructure components, their integration and logical routing from WAN to DMZ, Server farm and internal LAN. Proposed firewall MUST be support segmentation of network services based (Staff, students, CCTV, Biometric)	

Part 2: MANDATORY TECHNICAL REQUIRMENTS – FUNCTIONAL

No	Features & Requirements	Bidders Response (provide cross-reference in the bid document where the requirement is met)
1.	ISP redundancy with high availability option- The system shall support multiple ISP connections with interconnected Active-Active primary and secondary appliances	
2.	Web filtering and URL filtering: Support monitoring All web activities. Granular blocking and filtering provide web categories to allow, log, or block. Comprehensive URL database provides rapid and comprehensive protection	
3.	Application Control: Create policies to allow, deny, or restrict access to applications or entire categories of applications. Advanced detection signatures identify Apps, DB applications, web applications and protocols; both blacklist and white list approaches can allow or deny traffic. Ability to prioritize applications.	
4.	Intrusion prevention system (IPS): Real-time threat intelligence updates to block and prevent advanced cyber threats.	
5.	Advanced malware protection: Advanced protection, detection and prevention that includes: Antivirus, Anti-bot, content disarm and reconstruction (CDR), Virus outbreak protection service (VOS) and sandboxing.	
6.	Indicators of compromise: Automated breach defense system that continuously monitors network for attacks, vulnerabilities, and persistent threats. Protection against legitimate threats, guarding customer data and defending against fraudulent access, malware, and breaches. Detect and prevent fraud from compromised devices or accounts	
7.	**Threat Extraction (Sandboxing)**. Advanced threat detection solution that performs dynamic analysis to identify previously unknown malware. The solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created.	
8.	**User Identity Acquisition**: Must be able to acquire user identity by querying Microsoft Active Directory based on security events Must have a browser-based User Identity authentication method for non-domain users or assets. Must be able to acquire user identity from Microsoft Active Directory without any type of agent installed on the domain controllers	
9.	Event Logging and Status reporting: Support for event logging and generation of custom reports.	
10.	Licensing and Support: Enterprise protection licensing suite, management license and analyser license with 24/7 support. Licenses MUST be for 3 years. Direct SLA vendor support for 3 years from commissioning date.	

Part 3: MANDATORY DEVICE AND SYSTEM REQUIREMENTS

No	Features & Requirements	Bidders Response (provide cross-reference in the bid document where the requirement is met)
	Device	
1.		
	a) Must support at least 8 x 1GE RJ45 interfaces	
	b) Must support at least 8 x 1GE SFP slots	
	c) Must be support at least 2 x 10GE SFP+ slots	
	d) Must support at least 7 Million Maximum Concurrent Sessions	
	e) Must support at least 400,000 New Sessions/Second	
	f) Must support at least 30Gbps of firewall throughput	
	g) Must support at least 10 Gbps Enterprise/Production IPS Throughput	
	h) Must support at least 9 Gbps Enterprise/Production NGFW Throughput	
	i) Must support at least 7 Gbps SSL Inspection Throughput	
	j) Must support at least 7 Gbps Enterprise/Production Threat Protection Throughput	
	k) Must support at least 480GB SSD storage	
	l) Must be supplied with at least 2,000 SSL VPN licenses	
	m) Must support at least 10,000 IPSec site-to-site VPN tunnels	
	n) Must have the following licenses included Application Control, IPS, Anti Malware, Web Filtering, DNS Filtering, Mobile Security, and Sandbox	
2.	**Stateful Firewall**	
	a) The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified, if not the same model	
	b) It Must be possible to operate the firewall in "bridge mode" or "transparent mode" apart from the standard NAT mode	
	c) The Firewall must provide NAT functionality, including PAT.	
	d) Must support "Policy-based NAT"	
	e) The Firewall Must provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP	
	f) Firewall Must support Voice based protocols like H.323, SIP, SCCP, MGCP etc and RTP Pinholing.	
	g) The Firewall Must support User-Group based Authentication (Identity based Firewalling) & Scheduling	
	h) IPv6 support for both NAT and Transparent Mode	
3.	**Authentication Features**	

	a) Support for authentication at the firewall policy level (Local and Remote)	
	b) Support for RSA SecureID or other Token based products	
	c) Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication	
	d) Support for Native Windows Active Directory or Novell eDirectory Integration	
	e) Must support authentication based on LDAP Groups	
	f) Must support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators	
4.	**VPN**	
	a) The VPN Must be integrated with firewall and Must be ICSA Labs certified for both IPSec and SSL-TLS	
	Must support the following protocols: -	
	b) DES & 3DES	
	c) MD5, SHA-1 & the more secure SHA-256 authentication	
	d) Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.	
	e) Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm	
	f) The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)	
	g) Must support Hub and Spoke VPN topology	
	h) IPSec NAT Traversal & Dead Peer Detection Must be supported	
	i) IPSec VPN Must support XAuth over RADIUS and RSA SecurID or similar product.	
	j) Must have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy	
	k) Must support SSL Two-factor Authentication with Digital Certificates	
	l) Must support Single Sign-On Bookmarks for SSL Web VPN	
	m) Must support Windows, Linux and MAC OS for SSL-VPN (Must have always-on clients for these OS apart from browser based access)	
	n) Must support NAT within IPSec/SSL VPN tunnels	
	o) Must also support PPTP and L2TP over IPSec VPN protocols.	
5.	**High Availability**	
	a) The device must support Active-Active as well as Active-Passive redundancy.	
	b) The Firewall must support stateful failover for both Firewall and VPN sessions.	

	c)	The HA Architecture Must have the ability for Device Failure Detection and Notification as well as Link Status Monitor	
	d)	Must support Virtual router redundancy protocol (VRRP) and Link Failure Control	
6.	**Management Features**		
	a)	The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management	
	b)	Must have configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet (i.e. Trusted Hosts for Management)	
	c)	There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)	
	d)	The device must have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).	
	e)	Provision to generate automatic notification of events via mails / syslog	
	f)	Provision to send alerts to multiple email recipients	
	g)	Support for role based administration of firewall	
	h)	Must support simultaneous login of Multiple Administrators.	
	i)	Must have provision to customize the dashboard (e.g.: by selecting suitable Widgets)	
	j)	The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP	
	k)	Support for Image upgrade via FTP, TFTP and WebUI	
	l)	Must support system software rollback to the previous version after upgrade	
7.	**Intrusion Prevention**		
	a)	Must have integrated Network Intrusion Prevention System (NIPS) and must be ICSA Labs certified.	
	b)	Must have a built-in Signature and Anomaly based IPS engine on the same unit	
	c)	Must have protection for 3000+ signatures	
	d)	Able to prevent denial of service and Distributed Denial of Service attacks.	
	e)	Must be able to exclude certain hosts from scanning of particular signatures	
	f)	Supports CVE-cross referencing of threats where applicable.	
	g)	Must provide the facility to configure Profile based sensors (Client/Server) for ease of deployment	
	h)	Must support granular tuning with option to configure Overrides for individual signatures.	
	i)	Supports automatic Attack database updates directly over the internet. (i.e. no dependency on any intermediate device)	
	j)	Supports attack recognition inside IPv6 encapsulated packets.	

	k) Supports user-defined signatures (i.e. Custom Signatures) with Regular Expressions.	
	l) Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options	
	m) Must offer a variety of built-in responses including dashboard alerts, syslog / email notifications, SNMP traps and Packet Capture log. List all response options, excluding prevention responses	
	n) Must Identify and control over 1000+ applications (i.e. Application control feature)	
	o) Must perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc	
	p) Must control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc.	
8.	**Antivirus and Antimalware**	
	a) The appliance Must facilitate embedded antivirus support which is ICSA Labs certified	
	b) Must include Antispyware and Worm Prevention	
	c) Must have option to schedule automatic updates of the new virus pattern.	
	d) Gateway AV Must be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP, NNTP and IM	
	e) Must have configurable policy options to select what traffic to scan for viruses	
	f) Must have option to configure to respond to virus detection at the gateway in several ways i.e. Delete the file, Alert email, Quarantine etc.	
	g) Must have options to prevent user downloads based on file extension as well as file type.	
	h) Must have support for "Flow-Based Antivirus Scanning Mode" for high throughput requirements.	
	i) The solution Must be capable of scanning encrypted VPN tunnel traffic originating from the unit for virus	
	j) Must support Antivirus scanning of IPv6 traffic	
9.	**Threat Emulation/Extraction**	
	a) The solution must be tightly integrated with the cloud threat mitigation in order to make the protection more effective and updated so as to minimize the occurrence of false positives.	
	b) The solution must have multi-layer of detection process with the malicious code emulation and execution in the VM environment.	
	c) The solution must be able to inspect the web session to detect and notify the malicious web activity including malicious file downloads through the web/internet.	
	d) The solution must be able to store payload and artifacts of the detected threats for further analysis and incident time lines that is with the third party as well.	

	e)	The proposed solution Must have the ability to analyze, detect and block malware in common file formats including but not limited to executable, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks.	
	f)	The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution must also assign a unique identification number to each identified/detected threat for future reference.	
	g)	The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration	
	h)	The solution Must be part of an integrated model therefore it Must interact with other security network element in order to give full proof detection and correction model rather than having a point product.	
	i)	The solution must be able to detect and report malware by using multiple client environments (operating systems with multiple service pack levels) supporting both x64 and x86 architectures.	
	j)	The solution Must support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions	
	k)	The solution must be based on algorithm, which must be able to detect maximum Malware or rogue elements with each signature.	
	l)	The solution Must have ability to block all outbound call- back communication initiated by the internal clients (infected)	
10.	**URL Filtering**		
	a)	The appliance Must facilitate embedded Web Content Filtering feature	
	b)	Web content filtering solution Must work independently without the need to integrate with External proxy server.	
	c)	Must have facility to block URL' based on categories. Must support HTTP and HTTPS based traffic?	
	d)	URL database Must have more than 2 billion URLs under 70+ categories.	
	e)	Must be able to block different categories/sites based on User Authentication.	
	f)	Must have configurable parameters to block/allow unrated sites. Must have option to locally rate sites.	
	g)	Must have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable	
	h)	Must have options to customize the "Blocked Webpage Message" information displayed to end users	

	i) Must have facility to schedule the configurations so that non-work related sites are blocked during office hours and allow access to all sites except harmful sites during non-office hrs. Must also have time-based quota	
	j) The solution Must have options to block java applets, ActiveX as well as cookies	
	k) The solution Must be able to block URLs hosting spywares / adwares etc.	
	l) Must have configurable policy options to define the URL exempt list	
11.	**Traffic Optimization**	
	a) Must support WAN load balancing (weighted) algorithms by volume, sessions, source-destination IP, Source IP, and spillover	
	b) Must support multi-path intelligence using rules defined by:	
	c) Source address and/or user group	
	d) Destination address and/or a selection of over 3,000 applications	
	e) Path selection using particular link quality criteria or SLAs defined	
	f) Must support traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support	
	g) Must support an option to set up traffic shaping profile by defining the percentage of interface bandwidth for each classified traffic and then bind to interfaces	
	h) Must support traffic shaping policies that asigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.	
	i) Must support inline and out-of-path WAN optimization topology, peer to peer, and remote client support	
	j) Must support at least CIFS, FTP, HTTP(S), MAPI and TCP WAN optimization protocols	
	k) Must support multiple WAN optimization sessions on the same tunnel	
	Other Mandatory Requirements	
12.	The platform must use a security-hardened, purpose-built operating system, and Must support the deployment option in NGFW mode.	
13.	The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.	
14.	Licensing: Must be per device license for unlimited users for Firewall and other features. There Must not have any user/IP/host based licenses.	
15.	The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).	

16.	Each Virtual Domain Must be allowed to connect to Specific 3rd Party Authentication service, AD, Radius, Tacacs or other…	
17.	Must support more than one ISP with automatic ISP failover	
18.	Must have support for Explicit Proxy and Transparent Proxy	
19.	Must form the heart of the security fabric by integrating networking and security solutions and 3rd party solutions	
20.	Must provide integrations to different security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs on your network in real time including 3rd party security products	
21.	Must support centralized management of the proposed firewall appliances	
22.	Must support centralized software upgrades and security updates for the managed devices	
23.	Must support Hierarchical Objects Database, reuse of common configurations	
24.	Must support automated device discovery support and maintain policies on same device types	
25.	Must support granular device and role based administration for large enterprises and multi-tenancy deployments	
26.	Must support centralized SD-WAN provisioning and monitoring	
27.	Must support automated templates and scripts for device provisioning automation and policy installation with JSON APIs or XML API, to reduce your management burden and operational costs	

Part 4: Mandatory Documentation and Training

No	Requirement	Vendors Response (Attach documentation and/or commitment in writing to meet the requirements)
1.	**Project plan & schedule** – bidders to attach sample project plan & schedule. Bidders shall provide a detailed work plan of how the project will be implemented indicating key milestones and delivery timelines.	
2.	**SLA** - 3 Years' Service Level Agreement (Attach sample SLA which must include proposed routine services/activities, contacts of key personnel with escalation matrix and response & resolution times for various issues reported)	
3.	**On Premise Training** - Comprehensive Administration and technical on premise knowledge transfer training for at least 3 ICT staff (training plan shall focus on implementation and configuration of implemented solution and shall include but not limited to: - appliance setup and maintenance, administration and backup, rules & policies, configuration & routing and application mapping & publishing).	

c) Financial Evaluation:

The winning bidder will be the lowest evaluated bidder among those who will have passed the mandatory technical evaluation as outlined in (a & b) above.

SECTION III: GENERAL CONDITIONS OF CONTRACT

TABLE OF CONTENTS

SECTION III: GENERAL CONDITIONS OF CONTRACT

3.1   **Definitions**

In this contract the following terms shall be interpreted as indicated:

a) "The contract" means the agreement entered into between the Procuring entity and the tenderer as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

b) "The Contract Price" means the price payable to the tenderer under the Contract for the full and proper performance of its contractual obligations.

c) "The services" means services to be provided by the contractor including materials and incidentals which the tenderer is required to provide to the Procuring entity under the Contract.

d) "The Procuring entity" means the organization sourcing for the services under this Contract.

e) "The contractor means the individual or firm providing the services under this Contract.

f) "GCC" means general conditions of contract contained in this section

g) "SCC" means the special conditions of contract

h) "Day" means calendar day

3.2   **Application**
These General Conditions shall apply to the extent that they are not superseded by provisions of other part of contract.

3.3   **Standards**

3.3.1   The services provided under this Contract shall conform to the 7 standards mentioned in the Schedule of requirements

3.5   **Patent Right's**
The tenderer shall indemnify the Procuring entity against all third-party claims of infringement of patent, trademark, or industrial design tights arising from use of the services under the contract or any part thereof .

3.6   **Performance Security**
Within twenty fourteen (14) days of receipt of the notification of Contract award, the successful tenderer shall furnish to the Procuring entity the performance security where applicable in the amount specified in Special Conditions of Contract.

3.6.2 The proceeds of the performance security shall be payable to the Procuring entity as compensation for any loss resulting from the Tenderer's failure to complete its obligations under the Contract.

3.6.3 The performance security shall be denominated in the currency of the Contract or in a freely convertible currency acceptable to the Procuring entity and shall be in the form of:

a) Cash.

b) A bank guarantee.

c) Such insurance guarantee approved by the Authority.

d) Letter of credit.

3.6.4 The performance security will be discharged by the procuring entity and returned to the candidate not later than thirty (30) days following the date of completion of the tenderer's performance of obligations under the contract, including any warranty obligations under the contract.

3.7 Inspections and Tests

3.7.1 The Procuring entity or its representative shall have the right to inspect and/or to test the services to confirm their conformity to the Contract specifications. The Procuring entity shall notify the tenderer in writing, in a timely manner, of the identity of any representatives retained for these purposes.

3.7.2 The inspections and tests may be conducted on the premises of the tenderer or its subcontractor(s). If conducted on the premises of the tenderer or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring entity.

3.7.3 Should any inspected or tested services fail to conform to the Specifications, the Procuring entity may reject the services, and the tenderer shall either replace the rejected services or make alterations necessary to meet specification requirements free of cost to the Procuring entity.

3.7.4 Nothing in paragraph 3.7 shall in any way release the tenderer from any warranty or other obligations under this Contract.

3.8 Payment

3.8.1 The method and conditions of payment to be made to the tenderer under this Contract shall be specified in SCC

3.9 Prices

Prices charged by the contractor for services performed under the Contract shall not, with the exception of any Price adjustments authorized in SCC, vary from the prices by

the tenderer in its tender or in the procuring entity's request for tender validity extension as the case may be. No variation in or modification to the terms of the contract shall be made except by written amendment signed by the parties.

3.10 Assignment

The tenderer shall not assign, in whole or in part, its obligations to perform under this contract, except with the procuring entity's prior written consent.

3.10 Termination for Default

The Procuring entity may, without prejudice to any other remedy for breach of Contract, by written notice of default sent to the tenderer, terminate this Contract in whole or in part:

a) If the tenderer fails to provide any or all of the services within the period(s) specified in the Contract, or within any extension thereof granted by the Procuring entity.

b) If the tenderer fails to perform any other obligation(s) under the Contract.

c) If the tenderer, in the judgment of the Procuring entity has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

d) In the event the Procuring entity terminates the Contract in whole or in part, it may procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered, and the tenderer shall be liable to the Procuring entity for any excess costs for such similar services.

3.12 Termination of insolvency

The procuring entity may at the any time terminate the contract by giving written notice to the contractor if the contractor becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the contractor, provided that such termination will not produce or affect any right of action or remedy, which has accrued or will accrue thereafter to the procuring entity.

3.13 Termination for convenience

3.13.1 The procuring entity by written notice sent to the contractor may terminate the contract in whole or in part, at any time for its convenience. The notice of termination shall specify that the termination is for the procuring entity convenience, the extent to which performance of the contractor of the contract is terminated and the date on which such termination becomes effective.

3.13.2 For the remaining part of the contract after termination the procuring entity may elect to cancel the services and pay to the contractor on agreed amount for partially completed services.

3.14 Resolution of disputes

The procuring entity's and the contractor shall make every effort to resolve amicably by direct informal negotiations any disagreement or dispute arising between them under or in connection with the contract.

If after thirty (30) days from the commencement of such informal negotiations both parties have been unable to resolve amicably a contract dispute either party may require that the dispute be referred for resolution to the formal mechanisms specified in the SCC.

3.15 Governing Language

The contract shall be written in the English language. All correspondence and other documents pertaining to the contract, which are exchanged by the parties, shall be written in the same language.

3.16 Force Majeure

The contractor shall not be liable *for* forfeiture of its performance security, or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

3.17 Applicable Law.

The contract shall be interpreted in accordance with the laws of Kenya unless otherwise specified in the SCC

3.18 Notices
Any notices given by one party to the other pursuant to this contract shall be sent to the other party by post or by fax or E-mail and confirmed in writing to the other party's address specified in the SCC

A notice shall be effective when delivered or on the notices effective date, whichever is later.

SECTION IV: SPECIAL CONDITIONS OF CONTRACT

4.1   Special conditions of contract shall supplement the general conditions of contract, wherever there is a conflict between the GCC and the SCC, the provisions of the SCC herein shall prevail over those in the GCC.

4.2   Special conditions of contract with reference to the general conditions of contract.

General conditions of contract reference	Special conditions of contract
3.8	Payment shall be made after the services have been satisfactorily provided and upon submission of an invoice after attaining agreed deliverables.
3.9	Prices shall be maintained for a period of one year.
23.14	In case of a dispute between the purchaser and the supplier, the dispute shall be referred arbitration in accordance with the laws of Kenya.
3.17	The applicable law shall be Kenyan Law
3.18	Kenya Civil Aviation Authority, P.O Box 30163-00100, NAIROBI, GPO.

SECTION V: DESCRIPTION OF SERVICES

FUNCTIONAL SPECIFICATIONS FOR THE ADVANCED HARDWARE FIREWALL AND NETWORK SEGMENTATION SERVICES:

1.0 INTRODUCTION

This section provides functional specifications and requirements for an advanced hardware firewall and network segmentation services.

No	Features & Requirements
1.	ISP redundancy with high availability option- The system shall support multiple ISP connections with interconnected Active-Active primary and secondary appliances
2.	Web filtering and URL filtering: Support monitoring All web activities. Granular blocking and filtering provide web categories to allow, log, or block. Comprehensive URL database provides rapid and comprehensive protection
3.	Application Control: Create policies to allow, deny, or restrict access to applications or entire categories of applications. Advanced detection signatures identify Apps, DB applications, web applications and protocols; both blacklist and white list approaches can allow or deny traffic. Ability to prioritize applications.
4.	Intrusion prevention system (IPS): Real-time threat intelligence updates to block and prevent advanced cyber threats.
5.	Advanced malware protection: Advanced protection, detection and prevention that includes: Antivirus, Anti-bot, content disarm and reconstruction (CDR), Virus outbreak protection service (VOS) and sandboxing.
6.	Indicators of compromise: Automated breach defense system that continuously monitors network for attacks, vulnerabilities, and persistent threats. Protection against legitimate threats, guarding customer data and defending against fraudulent access, malware, and breaches. Detect and prevent fraud from compromised devices or accounts
7.	**Threat Extraction (Sandboxing)**. Advanced threat detection solution that performs dynamic analysis to identify previously unknown malware. The solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created.
8.	**User Identity Acquisition**: Must be able to acquire user identity by querying Microsoft Active Directory based on security events Must have a browser-based User Identity authentication method for non-domain users or assets. Must be able to acquire user identity from Microsoft Active Directory without any type of agent installed on the domain controllers
9.	Event Logging and Status reporting: Support for event logging and generation of custom reports.
10.	Licensing and Support: Enterprise protection licensing suite, management license and analyser license with 24/7 support. Licenses MUST be for 3 years. Direct SLA vendor support for 3 years from commissioning date.

SECTION VII   -   PRICE   SCHEDULE

NAME OF TENDER: TENDER NUMBER: KCAA/041/2019- 2020

TENDER FOR THE SUPPLY, INSTALLATION, CONFIGURATION, INTEGRATION, TESTING, TRAINING AND COMMISIONING OF AN ADVANCED HARDWARE FIREWALL AND NETWORK SEGMENTATION SERVICES AT EASA

NAME OF TENDERER: ....

Note: Costs MUST include ALL applicable taxes

No	Item Description		Quantity	Unit Cost	Total Cost
1.	Supply delivery and installation of appliance - Configured for high availability		2		
2.	Delivery of licenses	Appliance license inclusive of support- Enterprise protection license bundle for 3 years	2		
		Management license for 3 years	1		
		Analyzer license for 3 years	1		
3.	Implementation: Installation & configuration (2 appliances configured for high availability), Integration with gateway routers, configuring zones and segmenting servers, configuring rules & policies, Creating DMZ and provisioning web applications, integration testing and commissioning		LOT		
4.	Comprehensive Administration and technical on-premise knowledge transfer training for at least 3 ICT staff (training plan shall focus on implementation and configuration of implemented solution and shall include but not limited to: - appliance setup and maintenance, administration and backup, rules & policies, configuration & routing and application mapping & publishing).		3		
5.	Service Level Agreement (SLA) cost for 3 years		3		
	Grand Total (inclusive of ALL applicable taxes)				

Installation Period...

PLEASE NOTE AND COMPLY WITH THE FOLLOWING:
  i.   All Prices to be inclusive of all applicable taxes.
  ii.   In case of discrepancy between unit price and total, the unit price shall prevail.

Authorized Official:

_____   _____
Name   Signature, date and official stamp

SECTION VIII: - STANDARD FORMS

Notes on standard forms

1. The tenderer shall complete and submit with its tender the form of tender and price schedules pursuant to instructions to tenderers clause 9 and in accordance with the requirements included in the special conditions of contract.

2. When requested by the appendix to the instructions to tenderers, the tenderer should provide the tender security, either in the form included herein or in another form acceptable to the procuring entity pursuant to instructions to tenderers clause 12.3

3. The contract form, the price schedules and the schedule of requirements shall be deemed to form part of the contract and should be modifies accordingly at the time of contract award to incorporate corrections or modifications agreed by the tenderer and the procuring entity in accordance with the instructions to tenderers or general conditions of contract.

4. The performance security and bank guarantee for advance payment forms should not be completed by the tenderers at the time of tender preparation. Only the successful tenderer will be required to provide performance/entity and bank guarantee for advance payment forms in accordance with the forms indicated herein or in another form acceptable to the procuring entity and pursuant to the – conditions of contract.

5. The principal's or manufacturer's authorization form should be completed by the principal or the manufacturer, as appropriate in accordance with the tender documents.

SECTION VIII- STANDARD FORMS

1. Site survey form – to be filled and signed by KCAA representative
2. Form of tender
3. Price schedules
4. Contract form
5. Confidential Questionnaire form
6. Tender security form
7. Anti-corruption Affidavit form
8. Manufacturers authorization form

KENYA CIVIL AVIATION AUTHORITY

PRE-BID MEETING FORM FOR TENDER FOR THE SUPPLY, INSTALLATION, CONFIGURATION, INTEGRATION, TESTING, TRAINING AND COMMISIONING OF AN ADVANCED HARDWARE FIREWALL AND NETWORK SEGMENTATION SERVICES: TENDER NO: KCAA/041/2019-2020

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

THE EAST AFRICAN SCHOOL OF AVIATION

Details	Please √ if Visited

NAME OF INTERESTED BIDDER: - ---

THIS IS TO CERTIFY THAT THE NAMED BIDDER VISITED THE STATION AND HAS PARTICIPATED IN THE PRE-BID MEETING AS REQUIRED IN THE TENDER DOCUMENT FOR QUOTATION PURPOSES IN THE TENDER FOR AN ADVANCED HARDWARE FIREWALL AND NETWORK SEGMENTATION SERVICES.

COMPANY REPRESENTATIVE

NAME --

DESIGNATION--

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

EASA/KCAA REPRESENTATIVE

NAME --

DESIGNATION--

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

OFFICIAL STAMP

NB: Interested bidders must attend a mandatory pre-bid meeting to be held on Thursday, 5th March, 2020 at 11am to 1pm EASA - Auditorium.

FORM OF TENDER

Date_____   **Tender No. KCAA/041/2019-2020**

To: Kenya Civil Aviation Authority, P.O BOX 30163-00100, Nairobi

Gentlemen and/or Ladies:

1. Having examined the tender documents including Addenda Nos………………………….. *[insert numbers)* of which is hereby duly acknowledged, we the undersigned, offer to **supply, installation, configuration, integration, testing, training and commissioning of an advanced hardware firewall and network segmentation services at EASA** in conformity with the said tender documents for the sum of…………………………………………………………………………………
………………………….*[total tender amount in words and figures]* or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Tender.

2. We undertake, if our Tender is accepted, to provide the services in accordance with the services schedule specified in the Schedule of Requirements.

3. If our Tender is accepted, we will obtain the tender guarantee in a sum equivalent to _____ percent of the Contract Price for the due performance of the Contract, in the form prescribed by (Procuring entity).

4. We agree to abide by this Tender for a period of ……………………*[number]* days from the date fixed for tender opening of the Instructions to consultants, and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

5. Until a formal Contract is prepared and executed, this Tender, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

Dated this _____ day of_____ 2020
[signature]   *[In the capacity of]*

 Duly authorized to sign tender for and on behalf of

_____

CONTRACT FORM

THIS AGREEMENT made the ___day of _____20____between………… [Name of procurement entity] of ……………….[country of Procurement entity](hereinafter called "the Procuring entity") of the one part and ……………………[name of tenderer] of ……….[city and country of tenderer](hereinafter called "the tenderer") of the other part.

WHEREAS the procuring entity invited tenders for certain materials and spares. Viz……………………..[brief description of materials and spares] and has accepted a tender by the tenderer for the supply of those materials and spares in the spares in the sum of ……………………………………[contract price in words and figures]

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:

    (a) The Tender Form and the Price Schedule submitted by the tenderer;
    (b) the Schedule of Requirements;
    (c) the Technical Specifications;
    (d) the General Conditions of Contract;
    (e) the Special Conditions of Contract; and
    (f) the Procuring entity's Notification of Award.

3. In consideration of the payments to be made by the Procuring entity to the tenderer as hereinafter mentioned, the tenderer hereby covenants with the Procuring entity to provide the materials and spares and to remedy defects therein in conformity in all respects with the provisions of the Contract

4. The Procuring entity hereby covenants to pay the tenderer in consideration of the provision of the materials and spares and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, sealed, delivered by_____the _____(for the Procuring entity)

Signed, sealed, delivered by_____the _____(for the tenderer)

in the presence of_____.

7.2   CONFIDENTIAL BUSINESS QUESTIONNAIRE FORM

You are requested to give the particulars indicated in Part 1 and either Part 2(a), 2(b) or 2 (c) whichever applied to your type of business

You are advised that it is a serious offence to give false information on this form

Part 1 – General:

Business Name …………………………………………………………………………..

Location of business premises. …………………………………………………………..

Plot No…………………………………………… Street/Road ……………….………..

Postal Address ……………………….. Tel No. ………………. Fax …………. E mail ………….

Nature of Business ,…………………………………………………………………..

Registration Certificate No. …………………………………………………..…………

Maximum value of business which you can handle at any one time – Kshs. ………………….…

Name of your bankers ………………………….. Branch …………… (Attach letter from the bank)…………………………

	Part 2 (a) – Sole Proprietor
	Your name in full ……………………………………….. Age …………………....
	Nationality ……………………… Country of origin …….………………….…….
	• Citizenship details ……………………………………………………………………

Part 2 (b) Partnership

Given details of partners as follows:

Name	Nationality	Citizenship Details	Shares
1.	……………………………………………………………………………		
2.	…………………………………………………………………..……………		
3.	………………………………………………………………………………		
4.	………………………………………………………………………………		

Part 2 (c) – Registered Company

Private or Public ……………………………………………………………………

State the nominal and issued capital of company-

    Nominal Kshs. ………………………………

    Issued   Kshs. …………………………………

Given details of all directors as follows

Name	Nationality	Citizenship Details	Shares
1.	…………………………………………………………………………………		
2.	……………………………………………………………………..……………….		
3.	…………………………………………………………………………………		
4.	……………………………………………………………………..……………		

(Attach certificate of incorporation)

Date ……………………………Seal/Signature of Candidate ………………………..

TENDER SECURITY FORM

Whereas …………………………………….. [Name of the tenderer]

(Hereinafter called "the tenderer") has submitted its tender dated……………….. [Date of submission of tender] for the provision of ……………………………………………..

[Name and/or description of the services]

(Hereinafter called "the Tenderer")……………………………………………..

KNOW ALL PEOPLE by these presents that WE……………………………………

Of……………………………………….having registered office at

[Name of procuring entity](Hereinafter called "the Bank") are bound unto………………

[Name of procuring entity](Hereinafter called "the procuring entity") in the sum of ………..

for which payment well and truly to be made to the said Procuring entity, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Common Seal of the said Bank this_____ day of 20_____.

THE CONDITIONS of this obligation are:
1. If the tenderer withdraws its Tender during the period of tender validity specified by the tenderer on the Tender Form; or
2. If the tenderer, having been notified of the acceptance of its Tender by the Procuring entity during the period of tender validity:

> (a) Fails or refuses to execute the Contract Form, if required; or
> (b) Fails or refuses to furnish the performance security, in accordance with the instructions to tenderers;

we undertake to pay to the Procuring entity up to the above amount upon receipt of its first written demand, without the Procuring entity having to substantiate its demand, provided that in its demand the Procuring entity will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.
This guarantee will remain in force up to and including thirty (30) days after the period of tender validity, and any demand in respect thereof should reach the Bank not later than the above date.

_____
[signature of the bank]

(Amend accordingly if provided by Insurance Company)

PERFORMANCE SECURITY FORM

To: …………………………………………………………………………………………………..

[Name of the Procuring entity]

WHEREAS………………………………. [Name of tenderer]

(Hereinafter called "the tenderer") has undertaken, in pursuance of Contract No._____[reference number of the contract] dated _____20_____to

Supply…………………………………………………………………………………………..

[Description services](Hereinafter called "the contract")

AND WHEREAS it bas been stipulated by you in the said Contract that the tenderer shall furnish you with *a* bank guarantee by a reputable bank for the sum specified therein as security for compliance with the Tenderer's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the tenderer a guarantee:

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the tenderer, up to a total of ……………………………………………………. *[Amount of the guarantee in words and figures],*

and we undertake to pay you, upon your first written demand declaring the tenderer to be in default under the Contract and without cavil or argument, any sum or sums within the limits of ……………………….. *[Amount of guarantee]* as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the _____ day of 20

_____
Signature and seal of the Guarantors

_____
[name of bank or financial institution]

_____
[address]

_____
[date]

(Amend accordingly if provided by Insurance Company)

BANK GUARANTEE FOR ADVANCE PAYMENT

To…………………………

[Name of tender]…………………………………

Gentlemen and/or Ladies:

In accordance with the payment provision included in the special conditions of contract, which amends the general conditions of contract to provide for advance payment,

………………………………………………………………………

[Name and address of tenderer][hereinafter called "the tenderer"] shall deposit with the Procuring entity a bank guarantee to guarantee its proper and faithful performance under the said clause of the contract in an amount of
……………………………………………………………………………………………
[Amount of guarantee in figures and words].
We, the …………………………………………………………………………………

[bank or financial institution], as instructed by the tenderer, agree unconditionally and irrevocably to guarantee as primary obligator and not as surety merely, the payment to the Procuring entity on its first demand without whatsoever right of objection on our part and without its first claim to the tenderer, in the amount not exceeding
                                            [amount of guarantee in figures and words].

We further agree that no change or addition to or other modification of the terms of the Contract to be performed there under or of any of the Contract documents which may be made between the Procuring entity and the tenderer, shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition, or modification.

This guarantee shall remain valid and in full effect from the date of the advance payment received by the tenderer under the Contract until *[date]*.

Yours truly,

Signature and seal of the Guarantors

_____
[name of bank or financial institution]

_____
[address]

_____
[date]

LETTER OF NOTIFICATION OF AWARD

Address of Procuring Entity

_____

_____

To:_____

_____

_____

_____

RE: Tender No._____

    Tender Name_____

This is to notify that the contract/s stated below under the above mentioned tender have been awarded to you.

_____

_____

1. Please acknowledge receipt of this letter of notification signifying your acceptance.

2. The contract/contracts shall be signed by the parties within 30 days of the date of this letter but not earlier than 14 days from the date of the letter.

3. You may contact the officer(s) whose particulars appear below on the subject matter of this letter of notification of award.

    *(FULL PARTICULARS)*_____

    _____

SIGNED FOR ACCOUNTING OFFICER

REPUBLIC OF KENYA

IN THE MATTER OF OATHS AND STATUTORY DECLARATION ACT CHAPTER 15 OF THE LAWS OF KENYA

AND

IN THE MATTER OF THE PUBLIC PROCUREMENT AND DISPOSAL ACT, NO. 3 OF 2005.

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

THAT I am the Chief Executive/Managing Director/Principal Officer /Director of ……………………………… (name of the Candidate) which is a Candidate in respect of Tender Number ……………………. to supply goods, render services and/or carry out works for Kenya Civil Aviation Authority and duly authorized and competent to make this Affidavit.

THAT the aforesaid Candidate has not been requested to pay any inducement to any member of the Board, Management, Staff and/or employees and/or agents of Kenya Civil Aviation Authority, which is the procuring entity.

THAT the aforesaid Candidate, its servants and/or agents have not offered any inducement to any member of the Board, Management, Staff and/or employees and/or agents of Kenya Civil Aviation Authority.

THAT what is deponed to hereinabove is true to the best of my knowledge information and belief.

SWORN at ……………………….. by the said   }

………………………………………………..   }

Name of Chief Executive/Managing Director/   }

Principal Officer/Director   }

on this …………… day of ……………....... 2020   }

          }

          } _____

          }   DEPONENT

Before me   }

          }

          }

Commissioner for Oaths   }

8.7 MANUFACTURER'S AUTHORIZATION FORM

To   [*name of the Procuring entity*] …………………

WHEREAS …………………………………………………………… [*Name of the manufacturer*] who are established and reputable manufacturers of ………………….. [*Name and/or description of the goods*] having factories at ………………………………… [*Address of factory*] do hereby authorize ………………………… [*Name and address of Agent*] to submit a tender, and subsequently negotiate and sign the Contract with you against tender No. ………………………. [*Reference of the Tender*] for the above goods manufactured by us.

We hereby extend our full guarantee and warranty as per the General Conditions of Contract for the goods offered for supply by the above firm against this Invitation for Tenders.

_____

[*Signature for and on behalf of manufacturer*]

Note: This letter of authority should be on the letterhead of the Manufacturer and should be signed by a person competent.