TENDERNO. KPI/9A2/OT/52/ICT/18-19

TENDER FOR PROCUREMENT OF ENTERPRISE CYBER SECURITY SOLUTION

May 2019

ALL TENDERERS ARE ADVISED TO READ CAREFULLY THIS TENDER DOCUMENT IN ITS ENTIRETY BEFORE MAKING ANY BID

(ENSURE TO READ THE APPENDIX TO INSTRUCTIONS TO TENDERERS)

THE KENYA POWER & LIGHTING COMPANY LIMITED
CENTRAL OFFICE, STIMA PLAZA,
KOLOBOT ROAD, PARKLANDS,
P.O. BOX 30099-00100,
NAIROBI,
KENYA.
Telephones: +254-20-3201000; 3644000 Pilot Lines
Telephones: +254-720-600070/1-5; 733-755001/2-3 Cellular
Facsimile: +254-20-3514485; 3750240
Telegrams: "ELECTRIC"
E-mail: 1: JNdinya@kplc.co.ke
2: Bmuoki@kplc.co.ke
3: RHassan@kplc.co.ke
4: SAthman@kplc.co.ke
Website: **www.kplc.co.ke**

TABLE OF CONTENTS

Section **Contents** **Page No.**

SECTION I - INVITATION TO TENDER

DATE: MAY 2019

TENDERNO. KPI/9A2/OT/52/ICT/18- PROCUREMENT OF ENTERPRISE CYBER SECURITY SOLUTION

1.1 Introduction.

The Kenya Power & Lighting Company Ltd (KPLC) invites bids from eligible Tenderers for procurement of an Enterprise Cyber Security Solution. Interested Eligible Tenderers may obtain further information from the General Manager- Supply Chain, The Kenya Power & Lighting Company Ltd at Stima Plaza, 3rd Floor, Kolobot Road, P.O. Box 30099 – 00100 Nairobi, Kenya.

1.2 Obtaining tender documents.

1.2.1 Tender documents detailing the requirements may be obtained from the KPLC E-Procurement Portal **from 28th May 2019.**

1.2.2 Prospective bidders may also download the tender document from KPLC's website (www.kplc.co.ke) free of charge.

1.3 Submission of Tender documents

Completed Tenders are to be **saved as PDF** document marked TENDER **NO. KPI/9A.2/OT/52/ICT/18-19 PROCUREMENT OF ENTERPRISE CYBER SECURITY SOLUTION** and submitted in electronic format on the KPLC's E- procurement portal on the due date and time published on the portal. Tenderers are required to visit the portal from time to time for revised closing dates and addendums. The Tender is to be submitted **ONLINE** on or before **10.00am on 18th June 2019.**

1.4 Prices

Offered Price should be inclusive of all taxes, duties, levies and delivery costs to the premises (where applicable) of KPLC or other specified site must be in Kenya Shillings or a freely convertible currency in Kenya and shall remain valid for one hundred and twenty (120) days from the closing date of the tender. ***Please note that prices indicated on the KPLC tendering portal should be exclusive of VAT.***

1.5 Opening of submitted Tenders

Tenders will be opened promptly thereafter in the presence of the Tenderer's or their representatives who choose to attend in KPLC Auditorium at Stima Plaza, Kolobot Road, Parklands, Nairobi.

SECTION II - TENDER SUBMISSION CHECKLIST

SUBMISSION:

FINANCIAL AND NON FINANCIAL PROPOSALS

Bidders are advised to clearly label their documents while uploading on the portal.

VOLUME I - FINANCIAL PROPOSAL

Tenderers shall tick against each item indicating that they have provided it.

No.	Item	Tick Where Provided
1	**Duly completed Tender Form**	
2	**Tender Security – Bank Guarantee or Letters of Credit (issued by Banks Licensed by the Central Bank of Kenya), Guarantee by a deposit taking Microfinance Institution, Sacco Society, the Youth Enterprise Development Fund or the Women Enterprise Fund**	
3	**Price Schedule(s)**	
4	**Audited Financial Statements. The audited financial statements required must be those that are reported within eighteen (18) calendar months of the date of the tender document.** *(For companies or firms that are registered or incorporated within the last one calendar year of the Date of the Tender Document, they should submit certified copies of bank statements covering a period of at least six months prior to the date of the tender document. The copies should be certified by the Bank issuing*	
5	**Any other document or item required by the Tender Document that is financial. (The Tenderer shall specify such other documents or items it has submitted)**	

VOLUME II - NON-FINANCIAL PROPOSAL

Tenderers shall tick against each item indicating that they have provided it.

Tenderers are required to submit copies of the following MANDATORY DOCUMENTS which will be used during preliminary examination to determine responsiveness:

1) Certified Copy of Certificate of Incorporation
2) A valid Business permit
3) PIN Certificate.
4) Certified Copy of Valid Tax Compliance
5) Credit letter from a reputable bank
6) Certified Copy of Valid license in Telecommunications with Communications Authority of Kenya (C.A) for Telecommunication equipment vending, installation and maintenance services.
7) Valid ICT Authority (ICTA) certificate for security. At least category 1 in both information security and infrastructure (Mandatory).
8) Certified Copy of Valid license in Telecommunications with National Constructions Authority (NCA) at least category 1 (NCA-1)
9) Declaration stating that you have NOT been debarred by PPOA.
10) Current Manufacturer's Authorization Form for the solution proposed
11) A valid Site survey certificate
12) Filled Confidential Business Questionnaire
13) Duly filled Anti-Corruption declaration/ Commitment/ Pledge
14) Filled Tender questionnaire form

NB.

At this stage, the Tenderer's submission will either be responsive or non-responsive. The non-responsive submissions will be eliminated from the entire evaluation process and will not be considered further.

Evaluation and comparison of tenders: The following criteria shall be applied not withstanding any other requirement in the tender documents.

NOTES TO TENDERERS

1. Valid Tax Compliance Certificate shall be one issued by the relevant tax authorities and valid for at least up to the tender closing date. All Kenyan registered Tenderers must provide a valid Tax Compliance Certificate.

2. All Kenyan registered Tenderers must provide the Personal Identification Number Certificate (PIN Certificate).

3. Foreign Tenderers must provide equivalent documents from their country of origin as regards Tax Compliance and PIN certificates OR statements certifying that the equivalent documentation is not issued in the Tenderer's country of origin. The Statement(s) that equivalent documentation is not issued by the Tenderer's country should be original and issued by the Tax authorities in the Tenderer's country of origin.

TABLE OF PARAGRAPHS ON INSTRUCTIONS TO TENDERERS

Paragraph No. **Headings** **Page No.**

SECTION III - INSTRUCTIONS TO TENDERERS (ITT)

3.1 Definitions

In this tender, unless the context or express provision otherwise requires: -

a) *Any reference to any Act shall include any statutory extension, amendment, modification, re-amendment or replacement of such Act and any rule, regulation or order made there-under.*

b) *"Date of Tender Document" shall be the* ***start date*** *specified on the KPLC tendering portal.*

c) *"Day" means calendar day and "month" means calendar month.*

d) *"KEBS" wherever appearing means the Kenya Bureau of Standards or its successor(s) and assign(s) where the context so admits.*

e) *"KENAS" wherever appearing means the Kenya National Accreditation Service or its successor(s) and assign(s) where the context so admits*

f) *"PPRA" wherever appearing means The Public Procurement Regulatory Authority or its successor(s) and assign(s) where the context so admits.*

g) *Reference to "the tender" or the "Tender Document" includes its appendices and documents mentioned hereunder and any reference to this tender or to any other document includes a reference to the other document as varied supplemented and/or replaced in any manner from time to time.*

h) *"The Procuring Entity" means The Kenya Power and Lighting Company Limited or its successor(s) and assign(s) where the context so admits (hereinafter abbreviated as KPLC).*

i) *"The Tenderer" means the person(s) submitting its Tender for the supply, installation and commissioning (where applicable) of the goods in response to the Invitation to Tender.*

j) *Where there are two or more persons included in the expression the "Tenderer", any act or default or omission by the Tenderer shall be deemed to be an act, default or omission by any one or more of such persons.*

k) *Words importing the masculine gender only, include the feminine gender or (as the case may be) the neutral gender.*

l) *Words importing the singular number only include the plural number and vice-versa and where there are two or more persons included in the expression the "Tenderer" the covenants, agreements and obligations expressed to be made or performed by the Tenderer shall be deemed to be made or performed by such persons jointly and severally.*

m) *KPLC's "authorised person" shall mean its MD & CEO who is designated by the PPAD Act 2015 to exercise such power, authority or*

discretion as is required under the tender and any contract arising therefrom, or such other KPLC staff delegated with such authority.

n) Citizen contractors-means a person/firm wholly owned and controlled by person(s) who are citizens of Kenya.

o) Local contractors- a firm shall be qualified as a local contractor if it is registered in Kenya.

3.2 Eligible Tenderers

3.2.1 A tenderer is eligible to bid for this contract only if the tenderer satisfies the following criteria—

(a) the tenderer has the legal capacity to enter into a contract for procurement or asset disposal;
(b) the tenderer is not insolvent, in receivership, bankrupt or in the process of being wound up;
(c) the tenderer, if a member of a regulated profession, has satisfied all the professional requirements;
(d) the tenderer and his or her sub-contractor, if any, is not debarred;
(e) the tenderer has fulfilled tax obligations;
(f) the tenderer has not been convicted of corrupt or fraudulent practices; and
(g) is not guilty of any serious violation of fair employment laws and practices.

In addition, this Invitation to Tender is open to all Tenderers eligible as described in the **Appendix to Instructions to Tenderers**.

Successful Tenderers shall supply the goods in accordance with this tender and the ensuing contract.

3.2.2 In addition the tenderer shall be considered ineligible to bid, where in case of a corporation, private company, partnership or other body, the tenderer, their spouse, child or sub-contractor has substantial or controlling interest and is found to be in contravention of the provisions of section 3.2.1 above.

3.2.5 Despite the provisions of section 3.2.3 and 3.2.4, a tenderer having a substantial or controlling interest shall be eligible to bid where—

(a) such tenderer has declared any conflict of interest; and
(b) performance and price competition for that good, work or service is not available or can only be sourced from that tenderer.

3.2.6 For the purposes of this paragraph, any relative i.e. spouse(s) and child(ren) of any person mentioned in sub-paragraph 3.2.3 is also ineligible to participate in the tender. In addition, a Cabinet Secretary shall include the President, Deputy President or the Attorney General of GoK.

3.2.7 Tenderers shall provide the qualification information statement that the Tenderer (including 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 KPLC to provide consulting services for the preparation of the design, specifications, and other documents to be used for the procurement of the goods under this Invitation to Tender.

3.2.8 Tenderers shall not be under declarations as prescribed at Section XIII.

3.2.9 Tenderers who are not under these declarations shall complete the Declaration Form strictly in the form and content as prescribed at Section XIII.

3.2.10 Those that are under the Declaration as prescribed at Section XIII whether currently or in the past shall not complete the Form. They will submit a suitable Form giving details, the nature and present status of their circumstances.

3.3 Joint Venture

3.3.1 Tenders submitted by a joint venture of two or more firms, as partners shall comply with the following requirements: -

a) the Tender Form and in case of a successful tender, the Contract Agreement Form, shall be signed so as to be legally binding on all partners of the joint venture.

b) one of the partners shall be nominated as being lead contractor, and this authorization shall be evidenced by submitting a Power of Attorney signed by legally authorized signatories of all the partners.

c) The Power of Attorney which shall accompany the tender, shall be granted by the authorized signatories of all the partners as follows:-

(i.) for local bidders, before a Commissioner of Oaths or a Notary Public or Magistrate of the Kenyan Judiciary.

(ii.) for a foreign bidder, before a Notary Public, or the equivalent of a Notary Public, and in this regard the bidder shall provide satisfactory proof of such equivalence.

d) the lead contractor shall be authorized to incur liability and receive instructions for and on behalf of any and all the partners of the joint venture and the entire execution of the contract including payment shall be done exclusively with the lead contractor.

3.3.2 All partners of the joint venture shall be liable jointly and severally for the execution of the contract in accordance with the contract terms, and a relevant statement to this effect shall be included in the authorization mentioned in paragraph 3.3.1 (b) above as well as in the Form of Tender and the Contract Agreement Form (in case of the accepted tender).

3.3.3 A copy of the agreement entered into by the joint venture partners shall be submitted with the tender.

3.4 Cost of Tendering

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

3.5 Contents of the Tender Document

3.5.1 The Tender Document comprises the documents listed below and Addendum (where applicable) issued in accordance with paragraph 3.7 of these Instructions to Tenderers: -

a) Invitation to Tender
b) Tender Submission Checklist
c) Instructions to Tenderers
d) Appendix to Instructions to Tenderers
e) Schedule of Requirements
f) Project Implementation Schedule
g) Price Schedule for Services
h) Evaluation Criteria
i) General Conditions of Contract
j) Special Conditions of Contract
k) Tender Form
l) Confidential Business Questionnaire Form
m) Tender Security Form
n) Manufacturer's Authorization Form
o) Manufacturer's Warranty
p) Declaration Form
q) Contract Form
r) Performance Security Form
s) Details of Service
    (i.) General Requirements
    (ii.) Specific Details of Services

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

3.5.3 All recipients of the documents for the proposed Contract for the purpose of submitting a tender *(whether they submit a tender or not)* shall treat the details of the documents as "Private and Confidential".

3.6 Clarification of Documents

A prospective Tenderer requiring any clarification of the Tender Document may notify the General Manager Supply Chain in writing and ensure receipt is acknowledged at KPLC's Physical address indicated on the Tender Document. KPLC will respond in writing to any request for clarification of the Tender documents, which it receives not later than seven (7) days prior to the deadline for the submission of Tenders, prescribed by KPLC. Written copies of KPLC's response *(including an explanation of the query but without identifying the source of inquiry)* will be published and accessible to all prospective Tenderers on the KPLC's tendering portal.

3.7 Amendment of Documents

3.7.1 At any time prior to the deadline for submission of Tenders, KPLC, 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 amendment.

3.7.2 All prospective Tenderers that have registered in the portal for the Tender will be notified of the amendment(s) *(hereinafter referred to or otherwise known as addendum)* in writing and will be binding on them.

3.7.3 In order to allow prospective Tenderers reasonable time in which to take the amendment into account in preparing their Tenders, KPLC, at its discretion, may extend the deadline for the submission of Tenders.

3.8 Language of Tender

The Tender prepared by the Tenderer, as well as all correspondence and documents relating to the tender, exchanged between the Tenderer and KPLC, shall be written in English language. Any printed literature furnished by the Tenderer written in any other language shall be 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. The English translation shall be on the Tenderer's letterhead and shall be signed by the duly authorized signatory signing the Tender and stamped with the Tenderer's stamp.

3.9 Documents Comprising the Tender

The Tender prepared and submitted by the Tenderers shall include but not be limited to all the following components: -

a) Declaration Form, Tender Form and a Price Schedule completed in compliance with paragraphs 3.2, 3.10, 3.11 and 3.12.

b) Documentary evidence established in accordance with paragraph 3.13 that the Tenderer is eligible to tender and is qualified to perform the contract if its tender is accepted.

c) Documentary evidence established in accordance with paragraph 3.14 that the services and any ancillary thereto to be provided by the Tenderer conform to the tender documents, and,

d) Tender Security furnished in accordance with paragraph 3.17

e) A detailed list of previous customers as prescribed for similar services on tender and their contact addresses shall be submitted with the Tender for the purpose of reference, or for evaluation where the Details of Service so dictate.

f) And all other documents indicated in Section II (Tender Submission Checklist)

3.10 Tender Form

The Tenderer shall complete and sign the Tender Form and all other documents furnished in the Tender Document, indicating the services to be performed, a brief description of the services, quantity (where applicable), and prices amongst other information required.

3.11 Tender Prices

3.11.1 The Tenderer shall indicate on the appropriate Price Schedule, the unit prices (where applicable) and total tender price of the services it proposes to provide under the contract.

3.11.2 Prices indicated on the Price Schedule shall be of all costs for the services including insurances, duties, Value Added Tax (V.A.T) and other taxes payable. No other basis shall be accepted for evaluation, award or otherwise.

3.11.3 Section 20 of the Insurance Act Cap 487 requires all imports to the country to be insured with a local insurance company. It is now mandatory for all marine cargo imports to adhere to this requirement.

3.11.4 Tender prices to be submitted (quoted) by the Tenderer shall remain fixed for the contract duration.

3.11.5 A price that is derived by a disclosed incorporation or usage of an international accepted standard formula shall be acceptable within the meaning of this paragraph.

3.12 Tender Currencies

3.12.1 For services that the Tenderer will provide from within or outside Kenya, the prices shall be quoted in Kenya Shillings, or in another freely convertible currency in Kenya. The currency quoted must be indicated clearly on the Price Schedule of Services.

3.12.2 The exchange rate to be used for currency conversion shall be the Central Bank of Kenya selling rate prevailing on the Tender closing date. *(Please visit the Central Bank of Kenya website).*

3.13 Tenderer's Eligibility and Qualifications

3.13.1 Pursuant to paragraph 3.2, the Tenderer shall furnish, as part of its Tender, documents establishing the Tenderer's eligibility to tender and its qualifications to

perform the contract if its Tender is accepted.

3.13.2 The documentary evidence of the Tenderer's qualifications to perform the contract if its Tender is accepted shall be established to KPLC's satisfaction –

a) *that, in the case of a Tenderer offering to perform the services under the contract which the Tenderer is not the Principal, the Tenderer has been duly authorized by the Manufacturer, Principal or Producer to provide the services. The authorization shall strictly be in the form and content as prescribed in the Manufacturer's or Principal's Authorization Form in the Tender Document*

b) *that the Tenderer has the financial capability necessary to perform the contract. The Tenderer shall be required to provide the documents as specified in the Appendix to Instructions to Tenderers including a current Tax Compliance Certificate issued by the relevant tax authorities.*

c) *that the Tenderer has the technical and production capability necessary to perform the contract.*

d) *that, in the case of a Tenderer not doing business within Kenya, the Tenderer is or will be (if awarded the contract) represented by an agent in Kenya equipped, and able to carry out the Tenderer's maintenance, repair, spare parts and stocking obligations prescribed in the Conditions of Contract and or in the Details of Service.*

e) *that the Tenderer is duly registered and is a current member of a recognized body or institution accredited and or pertaining to that service.*

3.13.3 The Tenderer will furnish KPLC with a copy of the accreditation or recognition certificate as applicable. KPLC reserves the right to subject the certificate to authentication.

3.13.4 Tenderers with a record of unsatisfactory or default in performance obligations in any contract shall not be considered for evaluation or award. For the avoidance of doubt, this shall include any Tenderer with unresolved case(s) in its obligations for more than two (2) months in any contract.

3.14 Conformity of Services to Tender Documents

3.14.1 The Tenderer shall furnish, as part of its tender, documents establishing the conformity to the Tender Document of all services that the Tenderer proposes to perform under the contract.

3.14.2 The documentary evidence of conformity of the services to the Tender Document may be in the form of literature, drawings, and data, and shall (where applicable) consist of: -

a) *a detailed description of the essential technical and performance characteristics of the services whether in catalogues, drawings or otherwise,*

b) *a list giving full particulars, including available source and current prices of spare parts, special tools and other incidental apparatus necessary for the proper and*

continuing performance of the services for a minimum period of two (2) years following commencement of the provision of the services to KPLC, and,

c) *duly completed Statement of Compliance to KPLC's Details of Service demonstrating substantial responsiveness of the service to those Details or, a statement of deviations and exceptions to the provisions of the Details of Service.*

3.14.3 For purposes of the documentary and other evidence to be furnished pursuant to sub-paragraphs 3.14.1, 3.14.2 and paragraph 3.15, the Tenderer shall note that standards for workmanship, material, and equipment, designated by KPLC in its Details of Service are intended to be descriptive only and not restrictive. The Tenderer may adopt higher standards in its Tender, provided that it demonstrates to KPLC's satisfaction that the substitutions ensure substantial equivalence to those designated in the Details of Service.

3.15 Demonstration(s), Inspection(s) and Test(s)

3.15.1 Where required in the tender, all Tenderers shall demonstrate ability of performance of the required service in conformity with the Details of Services.

3.15.2 KPLC or its representative(s) shall have the right to inspect/ test the Tenderer's capacity, equipment, premises, and to confirm their conformity to the tender requirements. This shall include the quality management system. KPLC's representative(s) retained for these purposes shall provide appropriate identification at the time of such inspection/ test.

3.15.3 KPLC shall meet its own costs of the inspection/ test. Where conducted on the premises of the Tenderer(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to KPLC.

3.15.4 Demonstration, Inspection/ Test Report(s) shall be completed upon conclusion of the inspection/ tests. This Report will be considered at time of evaluation and or award.

3.16 Warranty

3.16.1 Where required in the Tender, all Tenderers must also provide a Warranty that services to be rendered in the Tenderer's bid have no defect arising from manufacture, materials or workmanship or from any act or omission of the Tenderer that may develop under normal use or application of the services under the conditions obtaining in Kenya.

3.16.2 This warranty will remain valid for the period indicated in the special conditions of contract after the services, or any portion thereof as the case may be, have been rendered.

3.17 Tender Security

3.17.1 The Tenderer shall furnish, as part of its Tender, a tender security for the amount specified in the Appendix to Instructions to Tenderers. The Original Tender Security, in a clearly labelled envelop, shall be deposited in the Tender Security Box on or before the opening date and time and receipt acknowledged by KPLC evidenced by a stamped copy.

3.17.2 The tender security shall be either one or a combination of the following: -

a) an original Bank Guarantee that is strictly in the form and content as prescribed in the Tender Security Form (Bank Guarantee) in the Tender Document.

b) For Local bidders, Standby Letters of Credit (LC). All costs, expenses and charges levied by all banks party to the LC shall be prepaid/borne by the Tenderer. The LC must contain all the mandatory conditions of payment to KPLC as prescribed in the Tender Security (Letters of Credit) provided in the Tender Document.

c) For Foreign bidders, Standby Letters of Credit (LC) confirmed by a bank in Kenya. All costs, expenses and charges levied by all banks party to the LC including confirmation charges shall be prepaid/borne by the Tenderer. The LC must contain all the mandatory conditions of payment to KPLC as prescribed in the Tender Security (Letters of Credit) provided in the Tender Document.

d) An original Guarantee by a deposit taking Microfinance Institution, Sacco Society, Youth Enterprise Development Fund or the Women Enterprise Fund, that is strictly in the form and content as prescribed in the Tender Security Form

3.17.3 The tender security is required to protect KPLC against the risk of the Tenderer's conduct which would warrant the security's forfeiture pursuant to paragraph 3.17.10.

3.17.4 The Tender Security shall be denominated in Kenya Shillings or in another freely convertible currency in Kenya. A Tender Security in form of a Bank Guarantee or a Standby Letter of Credit issued on behalf of local bidders, should be from a commercial bank licensed by the Central Bank of Kenya. A Tender Security in form of a Standby Letter of Credit issued on behalf of foreign bidders by foreign banks, should be confirmed by a commercial bank licensed by the Central Bank of Kenya.

3.17.5 The Tender Security shall be valid for thirty (30) days beyond the validity of the tender.

3.17.6 KPLC shall seek authentication of the Tender Security from the issuing bank. It is the responsibility of the Tenderer to sensitize its issuing bank on the need to respond directly and expeditiously to queries from KPLC. The period for response shall not exceed five (5) days from the date of KPLC's query. Should there be no conclusive response by the bank within this period, such Tenderer's Tender Security may be deemed as invalid and the bid rejected.

3.17.7 Any Tender not secured in accordance with this paragraph will be rejected by KPLC as non-responsive, pursuant to paragraph 3.26.

3.17.8 The unsuccessful Tenderer's Tender Security will be released as promptly as possible, in any of the following circumstances: -

a) the procurement proceedings are terminated

b) KPLC determines that none of the submitted Tenders is responsive

c) a contract for the procurement is entered into.

3.17.9 The successful Tenderer's Tender Security will be released upon the successful Tenderer's signing the contract, pursuant to paragraph 3.39 and furnishing an authentic Performance Security, pursuant to paragraph 3.40.

3.17.10 The Tender Security shall be forfeited –

a) if the Tenderer withdraws its Tender after the deadline for submitting Tenders but before the expiry of the period during which the Tenders must remain valid

b) if the Tenderer fails to enter into a written contract in accordance with paragraph 3.39

c) if the successful Tenderer fails to furnish the performance security in accordance with paragraph 3.40

d) if the Tenderer fails to extend the validity of the tender security where KPLC has extended the tender validity period in accordance with paragraph 3.18.

3.18 Validity of Tenders

3.18.1 Tenders shall remain valid for one twenty (120) days after the date of tender opening as specified in the Invitation to Tender or as otherwise may be prescribed by KPLC, pursuant to paragraph 3.23. A Tender that is valid for a shorter period shall be rejected by KPLC as non-responsive.

3.18.2 In exceptional circumstances, KPLC may extend the Tender validity period. The extension shall be made in writing. The tender security provided under paragraph 3.17 shall also be extended. A Tenderer shall not be required nor permitted to modify its tender during the extended period

3.19 Alternative Offers

Only main offers shall be considered, as alternative offers are not acceptable.

3.20 Number of Sets of and Tender Format

3.20.1 The Tender shall be typed or written in indelible ink. It shall be signed by the Tenderer or a person or persons duly authorized to bind the Tenderer to the contract.

3.20.2 The authorization shall be indicated by a written Power of Attorney granted by the Tenderer to the authorized person before any of the following persons:-

a) For local Tenderers, a Commissioner of Oaths or a Notary Public or a Magistrate of the Kenyan Judiciary.

b) For foreign Tenderers, a Notary Public in the country of the Tenderer.

In either case above, the Power of Attorney shall accompany the Tender.

3.20.3 All pages of the Tender, including un-amended printed literature, shall be initialed by the person or persons signing the Tender and serially numbered.

3.20.4 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.

3.20.5 KPLC will assume no responsibility whatsoever for the Tenderer's failure to comply with or observe the entire contents of this paragraph 3.20.

3.20.6 Any Tender not prepared and signed in accordance with this paragraph may be rejected by KPLC as non-responsive, pursuant to paragraph 3.20

3.21 Deadline for Submission of Tenders

3.21.1 Tenders must be received by KPLC by the date and time specified in KPLC's tendering portal in PDF form.

3.21.2 KPLC may, at its discretion, extend this deadline for submission of Tenders by amending the tender documents in accordance with paragraph 3.7, in which case all rights and obligations of KPLC and the Tenderer previously subject to the initial deadline, will therefore be subject to the deadline as extended.

3.22 Modification and Withdrawal of Tenders

3.22.1 The Tenderer may modify or withdraw its Tender after it has submitted, provided that the modification, including substitution or withdrawal of the Tender is received by KPLC prior to the deadline prescribed for submission of tenders.

3.22.2 No Tender may be modified after the deadline for submission of Tenders.

3.22.3 No Tender may be withdrawn in the interval between the deadline for submission of tenders and the expiration of the period during which the Tender must remain valid except where KPLC extends the initial validity period. Any withdrawal of a Tender during this interval shall result in forfeiture of the Tenderer's Tender Security except where KPLC extends the initial validity period.

3.23 Opening of Tenders

3.23.1 KPLC shall open all Tenders promptly at the date and time specified in the KPLC tendering portal and at the location specified in the Invitation to Tender or as may otherwise be indicated.

3.23.2 The Tenderer's names, tender modifications or withdrawals, the presence or absence of requisite Tender Security and such other details as KPLC, at its discretion, may consider appropriate, will be announced at the opening.

3.23.3 At the Tender opening, tender prices, discounts, and such other details as KPLC, at its discretion, may consider appropriate will be read out.

3.23.4 The Tenderers or their representatives may attend the opening and those present shall sign a register evidencing their attendance.

3.24 Process to be Confidential

3.24.1 After the opening of tenders, information relating to the examination, clarification, evaluation and comparisons of tenders and recommendations arising there-from shall not be disclosed to a Tenderer or other person(s) not officially concerned with such process until conclusion of that process.

3.24.2 Conclusion of that process shall be deemed to have occurred, at the latest, by the date and time KPLC notifies the successful bidder(s). In any event, official disclosure by KPLC of any information upon conclusion of that process may only be to the unsuccessful bidders and may contain only the information permissible by law in summary form.

3.24.3 Any effort by a Tenderer to influence KPLC or any of its staff members in the process of examination, evaluation and comparison of tenders and information or decisions concerning the Tender may result in the disqualification of the Tenderer.

3.25 Clarification of Tenders and Contacting KPLC

3.25.1 To assist in the examination, evaluation and comparison of Tenders KPLC 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 of the Tender shall be sought, offered, or permitted.

3.25.2 The Tenderer is required to provide timely clarification or substantiation of the information that is essential for effective evaluation of its qualifications. It is the responsibility of the Tenderer to provide in writing the clarification or substantiation which should reach KPLC within five (5) days from the date of KPLC's query. Such writing may include by electronic mail, facsimile or postal mail. Should there be no conclusive response within this period, it shall result in the Tenderer's disqualification.

3.25.3 Save as is provided in this paragraph and paragraph 3.22 above, no Tenderer shall contact KPLC on any matter related to its Tender, from the time of the tender opening to the time the successful Tenderer is announced..

3.25.4 Any effort by a Tenderer to influence KPLC in its decisions on tender evaluation, tender comparison, tender recommendation(s) or signing of Agreement may result in the disqualification of the Tenderer.

3.26 Preliminary Evaluation and Responsiveness

3.26.1 Prior to the detailed Technical and Financial evaluation, KPLC will determine the substantial responsiveness of each Tender. For purposes of this tender, a substantially responsive Tender is one that conforms to the requirements of Preliminary Evaluation. KPLC's determination of

a Tender's responsiveness is to be based on the contents of the Tender itself without recourse to extrinsic evidence.

3.26.2 KPLC will examine the Tenders to determine whether they conform to the Preliminary Evaluation Criteria set out in Section VI Evaluation Criteria.

3.26.3 Notwithstanding the contents of the foregoing sub-paragraphs, if a Tender is not substantially responsive, it will be rejected at the earliest stage of evaluation by KPLC and cannot subsequently be made responsive by the Tenderer by correction of any non–conformity.

3.27 Minor Deviations, Errors or Oversights

3.27.1 KPLC may waive any minor deviation in a Tender that does not materially depart from the requirements of the goods and or services set out in the Tender Document.

3.27.2 Such minor deviation -

3.27.2.1 shall be quantified to the extent possible,

3.27.2.2 shall be taken into account in the evaluation process, and,

3.27.2.3 shall be applied uniformly and consistently to all qualified Tenders duly received by KPLC.

3.27.3 KPLC may waive errors and oversights that can be corrected without affecting the substance of the Tender.

3.28 Technical Evaluation and Comparison of Tenders

3.28.1 KPLC will further evaluate and compare the Tenders that have been determined to be substantially responsive, in compliance to the Details of Services set out in the Tender Document and as per the prescribed Evaluation Criteria.

3.28.2 The Operational Plan is a critical aspect of the Tender. KPLC requires that the Services shall be performed at the time specified in the Schedule of Requirements. KPLC's evaluation of a tender will also take into account the Operational Plan proposed in the Tender. Tenderers offering to perform longer than KPLC's required delivery time will be treated as non-responsive and rejected.

3.29 Financial Evaluation

3.29.1 The financial evaluation and comparison shall be as set out in the Summary of Evaluation Process. The comparison shall be

a) 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.

b) deviations in Payment Schedule from that specified in the Special Conditions of Contract

3.29.2 Where other currencies are used, KPLC will convert those currencies to the same currency using the selling exchange rate ruling on the date of tender closing provided by the Central Bank of Kenya.

3.30 Preferences

3.30.1 Subject to availability and realization of the applicable international or local standards, only such manufactured articles, materials or supplies wholly mined and produced in Kenya shall be subject to preferential procurement.

3.30.2 Despite the above provisions, preference shall be given to —

(a) manufactured articles, materials and supplies partially mined or produced in Kenya or where applicable have been assembled in Kenya; or

(b) firms where Kenyans are shareholders.

3.30.3 The threshold for the provision under 3.30.2 (b) shall be above fifty-one percent of Kenyan shareholders.

3.30.1 In the evaluation of tenders, exclusive preference shall firstly be given to citizen contractors where the amount of the tender as evaluated is below Ksh. 500 Million in respect of works, goods and services.

3.30.2 Where a person is entitled to more than one preference scheme, the scheme with the highest advantage to the person shall be applied.

3.30.3 For purposes of this paragraph the Tenderer shall submit with its Tender, a valid copy of certificate of Confirmation of Directorships and Shareholding issued **and signed** by either the Registrar of Companies or Registrar of Business Names. This certificate must not be more than three (3) months old from the Date of the Tender Document. Kenya Power reserves the right to subject the certificate to authentication.

3.31 Debarment of a Tenderer

A Tenderer who gives false information in the Tender 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.

3.32 Confirmation of Qualification for Award

3.32.1 KPLC may confirm to its satisfaction whether the Tenderer that is selected as having submitted the lowest evaluated responsive tender is qualified to perform the contract satisfactorily.

3.32.2 The confirmation will take into account the Tenderer's financial, technical, and performance capabilities. It will be based upon an examination of the documentary evidence of the Tenderer's qualifications submitted by the Tenderer, pursuant to paragraph 3.13 as well as confirmation of such other information as KPLC deems necessary and appropriate. This may include factory, office and other facilities inspection and audits.

3.32.3 An affirmative confirmation will be a prerequisite for award of the contract to

the Tenderer. A negative confirmation will result in rejection of the Tenderer's Tender, in which event KPLC will proceed to the next lowest evaluated responsive tender to make a similar confirmation of that Tenderer's capabilities to perform satisfactorily.

3.33 Award of Contract

3.33.1 KPLC will award the contract to the successful Tenderer whose Tender has been determined to be substantially responsive, compliant with the evaluation criteria and has been determined to be the lowest evaluated tender, and further, where deemed necessary, that the Tenderer is confirmed to be qualified to perform the contract satisfactorily.

3.33.2 Award will be done as indicated in the Appendix to Instructions to Tenderers.

3.34 Termination of Procurement Proceedings

3.34.1 KPLC may at any time terminate procurement proceedings before contract award and shall not be liable to any person for the termination.

3.34.2 KPLC shall give prompt notice of the termination to the Tenderers, and, on request from any Tenderer, give its reasons for termination within fourteen (14) days of such request.

3.35 Notification of Award

3.35.1 Prior to the expiration of the period of tender validity, KPLC shall notify the successful Tenderer in writing that its Tender has been accepted.

3.35.2 The notification of award shall not constitute the formation of the contract until one is finally signed by both parties.

3.35.3 Simultaneously, and without prejudice to the contents of paragraph 3.25, on issuance of Notification of Award to the successful Tenderer, KPLC shall notify each unsuccessful Tenderer.

3.38.4 A notification of the tender outcome does not reduce the validity period for any tender security whether the Tenderer is successful or not, except where such tender security is officially released to the Bank and/or the Tenderer and such Bank discharged of all its obligations by KPLC prior to the expiry of its stated validity period.

3.36 Signing of Contract

3.36.1 At the same time as KPLC notifies the successful Tenderer that its Tender has been accepted, KPLC will send the Tenderer the Contract Agreement provided in the Tender Document together with any other necessary documents incorporating all agreements between the Parties.

3.36.2 Within fourteen (14) days of the date of notification of award, the successful Tenderer shall only sign the Contract Form and all the documents specified in that Form and return them to KPLC within that period of fourteen (14) days.

3.36.3 KPLC shall sign and date the Contract in the period between not earlier than fourteen (14) days from the date of notification of contract award. Further, KPLC shall not sign the contract until and unless the authentic performance security is received in accordance with paragraph 3.36.

3.36.4 Failure of the successful Tenderer to sign the Contract, the award shall be annulled and its tender security forfeited in which event KPLC shall notify the next lowest evaluated Tenderer that its Tender has been accepted.

3.36.5 Paragraph 3.33 together with the provisions of this paragraph 3.35 will apply with necessary modifications with respect to the Tenderer notified under sub-paragraph 3.35.3.

3.37 Performance Security

3.37.1 Within fourteen (14) days of the date of notification of award from KPLC, the successful Tenderer shall furnish KPLC with a Performance Security which shall be either one or a combination of the following:

a) an original Bank Guarantee that is strictly in the form and content as prescribed in the Performance Security Form (Bank Guarantee) in the Tender Document.

b) For Local bidders, Standby Letters of Credit (LC). All costs, expenses and charges levied by all banks party to the LC shall be prepaid/borne by the Tenderer. The LC must contain all the mandatory conditions of payment to KPLC as prescribed in the Tender Security (Letters of Credit) provided in the Tender Document.

c) For Foreign bidders, Standby Letters of Credit (LC) confirmed by a bank in Kenya. All costs, expenses and charges levied by all banks party to the LC including confirmation charges shall be prepaid/borne by the Tenderer. The LC must contain all the mandatory conditions of payment to KPLC as prescribed in the Tender Security (Letters of Credit) provided in the Tender Document.

3. 37.2 The Performance Security shall be issued by a commercial bank licensed by the Central Bank of Kenya. The bank must be located in Kenya.

3. 37.3 The Performance Security shall be the sum of ten percent (10%) of the contract value. It shall be in the currency of the contract price.

3. 37.4 KPLC shall seek authentication of the Performance Security from the issuing bank. It is the responsibility of the successful Tenderer to sensitize its issuing bank on the need to respond directly and expeditiously to queries from KPLC. The period for response shall not exceed three (3) days from the date of KPLC's

query. Should there be no conclusive response by the Bank within this period, such successful Tenderer's Performance Security may be deemed as invalid.

3. 37.5 Failure of the successful Tenderer to furnish an authentic Performance Security, the award shall be annulled and the Tender Security forfeited, in which event KPLC may notify the next lowest evaluated Tenderer that its Tender has been accepted.

3. 37.6 Paragraph 3.35, 3.36 together with the provisions of this paragraph 3. 37 will apply with necessary modifications, and as far as circumstances permit, with respect to the Tenderer notified under sub-paragraph 3.37.5.

3.38 Corrupt or Fraudulent Practices

3.38.1 KPLC requires that Tenderers observe the highest standard of ethics during the procurement process and execution of contracts. When used in the present Regulations, the following terms are defined as follows: -

a) *"Corrupt practice" means the offering, giving, receiving or soliciting of any thing of value to influence the action of public official in the procurement process or in contract execution;*

b) *"Fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of KPLC, and includes collusive practice among Tenderers (prior to or after Tender submission) designed to establish tender prices at artificial non-competitive levels and to deprive KPLC of the benefits of free and open competition.*

3. 38.2 KPLC will nullify its notification of award if it determines that the Tenderer recommended has engaged in corrupt or fraudulent practices in competing for the contract in question.

3. 38.3 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 regarding the particulars of the tender shall complement and or amend the provisions of the Instructions to Tenderers *hereinafter abbreviated as ITT*. Wherever there is a conflict between the provisions of the ITT and the Appendix, the provisions of the Appendix herein shall prevail over those of the ITT.

No.	ITT Reference Clause	Particulars of Appendix
1.	**3.2 Eligible tenderers**	*Open*
2.	**3.3 Origin of Eligible goods**	*Tenderer shall Specify origin of goods*
3.	**1.6 Pre-bid site survey**	***Not applicable for this tender.***
4.	**3.13.3 (a) Manufacturer's Authorization Form**	*Required*
5.	**3.13.3(b)Documentary evidence of financial capability**	*The audited financial statements required must be those that are reported within eighteen (18) calendar months of the date of the tender document.*
9.	**3.15.3 (a) Catalogues, Brochures, Manufacturer's Drawings**	*Required*
10.	**3.16 Sample(s)**	*N/A for this tender*
11.	**3.17.2 Period of Warranty**	*One year*
12.	**3.18.1 Tender Security**	*Ksh 2,200,000*
13.	**3.37.2 Mode of Award of Contract**	*Lowest evaluated bidder*
14.	**3.39 Performance Security**	*Successful bidder will be required to provide 10% performance bond of the total value contract value.*

SECTION IV – SCHEDULE OF REQUIREMENT

The specifications for the products are as follow and bidders MUST response in detail to all the questions asked. The cross reference should identify the relevant document(s), page number(s), and paragraph(s) and must highlight the relevant reference within the paragraph.

Table 1.0

Index	General Requirements	Response
1.1	***General Requirements:***	
1	All the proposed solutions should include 3 Years licenses (Subscription)	
2.	These FW, NAC WLAN and related components will be configured to work as suite of security devices or appliances or software applications to provide a total integrated security solution from the internet edge, data centers and LAN/WAN branches. The summary of the key component is as follows.	
2.1	Advanced Endpoint Protection (with malware and on spot, behavioral analysis and protection)	
2.2	Email Security Gateway (with content filters, antispam, etc)	
2.3	Network Access Control (NAC) Solution (with SIEM, BYOD, inventory, network scanning among others)	
2.4	Wireless Controllers & Wireless Access Points (guest, user, GBE ready, among others)	
2.5	Branch SD-WAN Firewalls (branch software defined firewall)	
2.6	Central Logging & Reporting Server/Appliance	
2.7	Central Management Appliance / Server	
2.8	Global & Application Load Balancers (Active –Active load balancer for HR & DR sites)	
2.9	Internet Edge Firewalls at HQ & DR (Next generation firewalls)	
2.10	Data Centre Firewalls at HQ & DR (Next generation firewalls)	
2.11	Web Application Firewall (General web access, Control & Proxy)	
2.12	Entity and End User Behaviors Analytics (EUBA)	

Details of each of the modules or the Enterprise Cyber Security suite are found in the details technical specifications section.

SECTION V - PRICE SCHEDULE FOR GOODS AND SERVICE

Table 1.2

Item	Description	QTY	Unit Cost	Total Cost
1	Advanced Endpoint Protection	4500		
2	Email Security Gateway	2		
3	NAC Solution, 5000 users each	2		
4	Wireless Access Points	40		
5	Branch SD-WAN Firewalls	2		
6	Central Logging & Reporting Appliance	1		
7	Central Management Appliance	1		
8	Application and Global Load Balancers	2		
9	HQ Internet Edge Firewalls	4		
10	DC Firewalls	4		
11	Web Application Firewall	2		
12	Entity and End User Behaviors Analytics (EUBA)	500		
13	OEM Training cost for network administrators	5		
14	Bidders MUST also include 1st year Support & Warranty on their bid and this must be inclusive on the final financial proposal. (this price will be used as indicative figure for subsequent SLAs)	LOT		
15	Installation and commissioning	LOT		
	Sub Total			
	16% VAT			
	Grand Total			

Name of Tenderer

Name and Capacity of authorized person signing the Tender

_____

Signature of authorized person signing the Tender

Stamp of Tenderer

NOTES:-

1. If and/or where KPLC is an appointed withholding agent in respect of taxes for the Government of Kenya, no payment shall be made to the successful bidder for Value Added Tax *(VAT) (if any)* which may be imposed by Kenya Government in respect of the Supplies being made under the contract.

2. Offered unit prices for the initial year shall be firm and not subject to adjustment for changes or unexpected contingencies of any kind whatsoever including without restricting the generality of the foregoing, changes in the coefficients of the price which includes, changes in wages, material costs, but excluding taxes which may in future be imposed by lawful authority within Kenya.

3. Where any offered unit price contains a figure that has decimal places, that unit price must be rounded to have ONLY two decimal places. For the avoidance of doubt, no unit price shall include a figure that has more than two decimal places. Where any Tenderer does not comply with this requirement, its unit price shall be rounded down-wards to two decimal places and used for the purposes of this tender and ensuing contract.

SECTION VI - EVALUATION CRITERIA

Evaluation of duly submitted tenders will be conducted along the following stages: -

6.1 Part 1 - Preliminary Evaluation Under Paragraph 3.28 of the ITT. These are mandatory requirements. This shall include confirmation of the following: -

6.1.1 Submission of Tender Security - Checking its validity, whether it is Original; whether it is issued by a local bank/institution; whether it is strictly in the format required in accordance with the sample Tender Security Form(s).

6.1.2 Submission of Declaration Form(s) duly completed and signed.

6.1.3 Submission and considering Tender Form duly completed and signed.

6.1.4 Submission and considering the following:-

6.1.4.1 For Local Tenderers

a) Company or Firm's Registration Certificate

b) PIN Certificate.

c) Valid Tax Compliance Certificate.

6.1.4.2 For Foreign Tenderers

a) Company or Firm's Registration Certificate

b) PIN Certificate or its equivalent in the country of bidder or a statement from the tax authorities in the Tenderer's country of origin indicating that such certificate or its equivalent is not issued.

c) Valid Tax Compliance Certificate or its equivalent in the country of bidder or a statement from the tax authorities in the Tenderer's country of origin indicating that such certificate or its equivalent is not issued.

6.1.5 That the Tender is valid for the period required.

6.1.6 Submission and considering the Confidential Business Questionnaire:-

a) Is fully filled.

b) That details correspond to the related information in the bid.

c) That the Tenderer is not ineligible as per paragraph 3.2 of the ITT.

6.1.7 Submission and considering the Certificate of Confirmation of Directors (CR12)

6.1.8 Record of unsatisfactory or default in performance obligations in any contract shall be considered. This shall include any Tenderer with unresolved case(s) in its performance obligations for more than two (2) months in any contract.

6.1.8 Notwithstanding the above, considering any outstanding orders/Supplier Performance Review Scheme (SPRS) where applicable and the performance capacity indicated by the Tenderer.

Tenders will proceed to the Technical Evaluation Stage only if they qualify in compliance with Part 1 above, Preliminary Evaluation under Paragraph 3.28.

6.2 Part II – Technical Evaluation and Comparison of Tenders Under Paragraph 3.30 of the ITT. These are mandatory requirements.

6.2.1 Verification of the following information:

a) Applicable relevant ISO 9001:2015 certification/ KEBS Standardization certificates where applicable.

b) Relevant requested certificates and or documents.

c) Manufacturer's or Principal's Authorization.

d) Submitted with the Tender –

(i.) Catalogues and or Brochures

(ii.) Manufacturer's or Principal's authorisation

(iii.) Commentary of Compliance to the Details of Service.

(iv.) Any other details required of the Tender.

(V). Tenderer's membership of a recognized or accredited organisation

6.2.2 Submission of Copies of relevant Type Test Certificates and their Reports or Test Certificate and their Reports from the designated bodies.

6.2.3 Submission of a copy of ISO/ IEC 17025 accreditation certificate for the testing body/ authority.

6.2.4 Submission of a copy of:-

a) the Manufacturer's/ Principal's valid quality management system certification i.e. ISO 9001:2015

b) KEBS Standardization certificates where applicable

6.2.2 Detailed Evaluation

The technical responses will be marked out of 100 to arrive at the technical score (St) and the minimum technical score required to proceed to financial evaluation is 80. Tenderers who fail to secure the minimum technical score will be eliminated from the entire evaluation process and will not be considered further.

The Bidders who are Compliant with the solution proposed i.e Fully Supported as per the Technical Specifications in **SECTION IV**; shall be considered for the next stage of Financial Evaluation.

The evaluation committee will compare solutions proposed from different bidders and note type of technology/model proposed. The evaluation committee will judge and make an appropriate decision giving evidence. The Evaluation Committee may verify authenticity of the documents provided at this stage.

The detailed scoring plan shall be as shown in table below: -

Due diligence will be carried out to verify the information presented.

Item	Technical Evaluation	Point	Max. Point
	Part 1:Technical specifications		
I	Compliance to the technical specifications as outlined on section IV – Technical Specifications	Mandatory	
Part 2: Manufacturer (OEM) & Solution Evaluation			
II	The proposed solution MUST be in the Leaders Quadrant of the Gartner magic quadrant for Enterprise Network Firewall (ENF). a) In the leader's quadrant: - In the last two years-2018 & 2017 (5 pts) - In one of the last two years – 2017 or 2018 (2 pts) - Not a leader in the last two years (0 pt.)		5
	b) Enterprise Network Firewall Magic Quadrant Position inside the leader quadrant (ability to execute and completeness of vision) for 2018 - 1st Position (5 pts) - 2nd Position (4 pts), - 3rd Position (3 pts) -4th Position (2 pts) -5th Position & below (1 pt.)		5
	c) Enterprise Network Firewall Magic Quadrant Position inside the leader quadrant (ability to execute and completeness of vision) for 2017 - 1st Position (5 pts) - 2nd Position (4 pts), - 3rd Position (3 pts) -4th Position (2 pts) -5th Position & below (1 pt)		5

III	The proposed solution MUST be in the NSS Labs Scoring; a) 2018 Next Generation Firewall (NGFW) Test i. Recommended (5 pts) ii. Neutral (2 pts) iii. Caution/Non-Participation (0 Pts)		5

	b) 2018 Datacenter Intrusion Prevention Systems (DCIPS) Test i. Recommended (5 pts) ii. Neutral (2 pts) iii. Caution/Non-Participation (0 Pts)		5
	c) 2017/2018 Breach Prevention Systems (BPS)/Advanced threat Defense (Protection) Test i. Recommended (5 pts) ii. Neutral (2 pts) iii. Caution/Non-Participation (0 Pts)		5
IV	The proposed solution MUST be certified by ICSA Labs in the following tests; a) 2018 ICSA labs Firewall test - certified		5
	b) 2018 ICSA labs Network IPS test - certified		5
	c) 2018 ICSA labs Advanced Threat Defense (Prevention) test - certified		5
	d) 2017 ICSA labs Firewall Test - certified		5
	Part 3: OEM partner/Integrator capacity		
V	a) Proof of implementation of an enterprise level IT Cyber security solution from the SAME proposed OEM in the last 2 years for a government / Corporate institution in Kenya. (Attach completion certificate) • 5 Sites or more completed ----10 points • 3 Sites completed ------5 points • Less than 3 --------- 0 points		10
	b) Skills and certification for proposed solution: The partner Must have Engineers certified to high level of security certifications for the proposed solutions • At least 1 Expert/Architect level certified Engineers-----10 • At least 2 Professional level certified Engineers----5 • No professional certified Engineers----0		10
	c) Skills for Current environment Integration: KPLC has Cisco based core network infrastructure. The Partner must have a High-level expertise in cisco for proper deployment. • At least 1 CCIE---------10 • At least 2 CCNP--------5 • No CCNP and above ----------0		10
	d) IT Change management Skills: Given the critical nature of KPLC IT production environment, the partner should have project resources who are trained and certified on ITIL change management processes. • At least 1 ITIL certified team member ---------5 • No ITIL certified team members ---------0		5

	e) Level of business partnership. The bidder MUST be a credible business partner of the proposed OEM. • Premier/Gold/Platinum---------5 • NOT Premier/Gold/Platinum-----0		5
	f) COMPLIANCE for specifications: The Bidder MUST provide cross references to the relevant supporting information, if any, included in the bid. The cross reference should identify the relevant document(s), page number(s), and paragraph(s). • Full documented compliance----10 • Partial documented compliance ----5 • No documented compliance ----0		10

6.2.2.1 Tenderers shall be expected to indicate full compliance to Details of Service outlined in Section XXVII Part B..

6.2.2.2 Evaluation of Demonstration of ability of the offered service, to comply with the Details of Service (where required).

6.2.2.3 Considering the Demonstration, Inspection/ Test Report(s).

6.2.2.4 Identifying and determining any deviation(s) from the requirements; errors and oversights.

6.2.2.5 Confirmation of compliance of previous contract(s) in accordance with its/ their terms and conditions where applicable.

6.3 Part III – Financial Evaluation Criteria Under Paragraph 3.31 of the ITT. These are mandatory requirements.

6.3.1 This will include the following: -

a) *Confirmation of the authenticity and sufficiency of the submitted Tender Security.*

b) *Confirmation of and considering Price Schedule duly completed and signed.*

c) *Checking that the Tenderer has quoted prices based on all costs including duties and taxes*

*d)** *Checking submission of audited financial statements required which must be those that are reported within eighteen (18) calendar months of the date of the tender document.*

e) *Conducting a financial comparison, including conversion of tender currencies into one common currency,*

f) *Taking into account the cost of any deviation(s) from the tender requirements,*

g) Considering information submitted in the Confidential Business Questionnaire against other information in the bid including: -

a) Declared maximum value of business

b) Shareholding and citizenship for preferences where applicable.

h) Apply Exclusive margin of preference, where applicable as per Clause 3.32 of the tender document

6.3.2 Confirming the following: -

6.3.2.1 that the Supplier's offered Delivery Schedule meets KPLC's requirements.

6.3.2.2 that the Supplier's offered Terms of Payment meets KPLC's requirements.

6.4 The Successful Tenderer shall be the one with the lowest evaluated price.

OVERALL TENDER EVALUATION CRITERIA

The effectiveness of the solution is very key to the company's operations, as such the technical capability of the solution is very important to KPLC. The evaluation of the responsive bids will take into account technical factors, in addition to cost factors.

Response to compliance to all Technical Specifications is **MANDATORY.** Bidders must score a minimum of 80 points out of 100. Bidders MUST respond to ALL the requirements on a clause by clause basis stating clearly how their solution meets the requirements. Responses to compliance to technical specifications in any other way other than clause by clause will be treated as NON-RESPONSIVE.

All firms with technical scores points above 80/100 will proceed to financial evaluation as per Section 6.3.1 & 6.3.2 of the tender.

<u>*NOTES</u>: -

1. For purposes of evaluation, the exchange rate to be used for currency conversion shall be the selling exchange rate prevailing on the date of tender closing provided by the Central Bank of Kenya. (Visit the Central Bank of Kenya website).

2. Total tender value means the Tenderer's total tender price inclusive of Value Added Tax (V.A.T) for the services it offers to provide.

4. For companies or firms that are registered or incorporated within the last one calendar year of the Date of the Tender Document, they should submit certified copies of bank statements covering a period of at least six months prior to the date of the tender document. The copies should be certified by the Bank issuing the statements. The certification should be original.

TABLE OF CLAUSES ON GENERAL CONDITIONS OF CONTRACT

Clause No. **Headings** **Page No.**

SECTION VII – GENERAL CONDITIONS OF CONTRACT

The General Conditions of Contract *hereinafter referred abbreviated as the GCC* shall form part of the Conditions of Contract in accordance with the law and KPLC's guidelines, practices, procedures and working circumstances. The provisions in the GCC will apply unless an alternative solution or amendment is made under other parts of the Contract including the Special Conditions of Contract.

7.1 Definitions

In this contract, the following terms shall be interpreted as follows: -

a) *"Day" means calendar day and "month" means calendar month.*

b) *"The Contract" means the agreements entered into between KPLC and the Contractor, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.*

c) *"The Contract Price" means the price payable to the Contractor under the contract for the full and proper performance of its contractual obligations.*

d) *"The Services" means services or art thereof to be provided by the Contractor and includes all of the materials and incidentals, which the Contractor is required to perform and provide to KPLC under the contract.*

e) *"The Procuring Entity" means The Kenya Power and Lighting Company Limited or its successor(s) and assign(s) where the context so admits (hereinafter abbreviated as KPLC).*

f) *"The Contractor" means the individual or firm providing the services under this contract or his/ her/ its permitted heir(s), personal representative(s), successor(s) or permitted assign(s) where the context so admits. For the avoidance of doubt this shall mean the successful Tenderer(s) pursuant to the tender.*

g) *Wherever used in the contract, "performance" shall be complete or be deemed to be complete, unless the circumstances indicate otherwise, when the services have been performed in accordance with the Contract and where KPLC does not signify its approval to the Contractor, but without giving notice of dissatisfaction, on the expiration of thirty (30) days from date of documented completion of performance of the service.*

h) *Supplier Rating Performance Scheme (SPRS) means the continuous evaluation of the Supplier's performance of the contract based on the parameters of timely delivery, quality of service, frequency of communication, timely response, innovation, dispute resolution.*

7.2 Application

These General Conditions shall apply to the extent that provisions of other parts of the contract do not supersede them.

7.3 Standards

The Services supplied under this contract shall conform to the standards mentioned in the Details of Service.

7.4 Supplier Performance Rating Scheme

7.4.1 KPLC shall use a Supplier Performance Rating Scheme (SPRS) to measure the annual performance of the Supplier's obligations and its conduct of the contract.

7.4.2 The Scheme will be updated periodically commencing with the date of execution of the contract by both parties. KPLC shall provide the Supplier with a copy of the SPRS report.

7.4.3 KPLC shall consider the Supplier's overall performance at the end of the performance period.

7.4.4 At the request of either party, the parties shall discuss and conclude deliberations on the annual SPRS report. At any such meetings and/or for the purposes of the deliberations, KPLC Supply Chain – Procurement Department shall appoint the Chairperson as well as the Secretariat.

7.4.5 The SPRS measures shall be according to Supplier Performance Rating Form in Section XXVI

7.4.6 A KP1, KP2 & KP3 assessment of the Supplier on the SPRS will be a consideration for continued engagement between the parties in the subsequent year. A KP4 assessment of the Supplier shall be a termination event.

7.5 Use of Contract Documents and Information

7.5.1 The Contractor shall not, without KPLC's prior written consent, disclose the contract, or any provision thereof or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of KPLC in connection therewith, to any person other than a person employed by the Contractor in the performance of the contract.

7.5.2 The Contractor shall not, without KPLC's prior written consent, make use of any document or information enumerated in clause 7.5.1 above.

7.5.3 Any document, other than the contract itself, enumerated in clause 7.5.1 shall remain the property of KPLC and shall be returned (including all copies) to KPLC on completion of the Contractor's performance under the contract if so required by KPLC.

7.6 Patent Rights

The Contractor shall indemnify KPLC against all third party claims of infringement of patent, trademark, or industrial design rights arising from provision of the services or any part thereof.

7.6 Performance Security

7.6.1 Within fourteen (14) days of the date of the notification of contract award, the Contractor shall furnish to KPLC the Performance Security which shall be either one or a combination of the following: -

a) an original Bank Guarantee that is strictly in the form and content as prescribed in the Performance Security Form (Bank Guarantee) in the Tender Document.

b) Confirmed Standby Letters of Credit (LC). All costs, expenses and charges levied by all banks party to the LC including confirmation charges shall be prepaid by the successful Tenderer. Certain mandatory conditions of the LC shall be as prescribed in the Performance Security Form (LC) in the Tender Document.

7.6.2 The Performance Security shall be issued by a commercial bank licensed by the Central Bank of Kenya. The bank must be located in Kenya.

7.6.3 The Performance Security shall be the sum of ten percent (10%) of the contract price. It shall be in the currency of the contract price.

7.6.4 Failure of the Contractor to furnish the Performance Security, the award shall be annulled and the Tender Security forfeited, in which event KPLC may notify the next lowest evaluated Tenderer that its Tender has been accepted.

7.6.5 The proceeds of the Performance Security shall be payable to KPLC as compensation for any loss resulting from the Contractor's failure to comply with its obligations in accordance with the contract without KPLC being required to demonstrate the loss it has suffered.

7.6.6 The Performance Security shall be valid for a minimum of sixty (60) days after satisfactory delivery for both Foreign and Local Contractors.

7.6.7 KPLC shall seek authentication of the Performance Security from the issuing bank. It is the responsibility of the Contractor to sensitize its issuing bank on the need to respond directly and expeditiously to queries from KPLC. The period for response shall not exceed three (3) days from the date of KPLC's query. Should there be no conclusive response by the Bank within this period, such Contractor's Performance Security may be deemed as invalid and the Contract nullified, unless information to the contrary is received by KPLC two (2) days before the expiry of the Contractor's Tender Security.

7.6.8 Subject to the provisions of this contract, the Performance Security will be discharged by KPLC and returned to the Contractor not earlier than thirty (30) days following the date of completion of the Contractor's obligations under the contract, including any warranty obligations, under the contract.

7.7 Inspection and Tests

7.7.1 KPLC or its representative(s) shall have the right to inspect and/or to test the services to confirm their conformity to the contract specifications. KPLC shall notify the Contractor in writing in a timely manner, of the identity of any representative(s) retained for these purposes. Such visit and or inspection/ test shall in no way prejudice KPLC's rights and privileges.

7.7.2 In appropriate circumstances, Inspection/ Test Report(s) shall be completed upon conclusion of the inspection/ tests.

7.7.3 The inspections and tests may be conducted in the premises of the Contractor or its subcontractor(s). If conducted on the premises of the Contractor 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 KPLC.

7.7.4 Should any inspected or tested services fail to conform to the specifications, KPLC may reject the Service(s), and the Contractor shall either replace or remedy the rejected

services or make alterations necessary to meet specification requirements free of cost to KPLC.

7.7.5 KPLC's right to inspect, test and where necessary, reject the services after provision shall in no way be limited or waived by reason of the services having previously been inspected, tested and passed by KPLC or its representative(s)

prior to the services performance / delivery.

7.7.6 For the avoidance of doubt, any acknowledgement by KPLC on the Contractor's or sub-contractor's document shall not be conclusive proof or evidence of satisfactory performance without duly authorized approval by KPLC.

7.7.7 Nothing in this clause 7.7 shall in any way release the Contractor from any warranty or other obligations under this Contract.

7.8 Packaging and Labelling

7.8.1 Where applicable, the Contractor shall provide such packaging of the material and equipment as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract.

7.8.2 The method of packaging, labeling and marking shall comply strictly with such special requirements as shall be specified and attached to the Contract and particular Order.

7.8.3 The labelling, marking and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract.

7.8.4 The materials and equipment shall be packed in good condition suitable for sea/air/road/rail dispatch. Hazard in transit to the final destination shall include rough handling and storage in tropical conditions.

7.8.5 The Contractor shall enclose a packing list in each package and all documents relating to the Order shall show the Tender reference number and name against the items or package indicating the supplier or supplier's agent as the consignee.

7.9 Delivery and Documents for Materials/ Equipment

7.9.1 Where applicable, delivery of the materials/ equipment shall be made by the Contractor to the place and in accordance with the terms specified by KPLC in its Schedule of Requirements or as may be otherwise indicated.

7.9.2 The Contractor shall notify KPLC of the full details of the delivered materials/ equipment by delivering the materials/ equipment with a full set of the following documents: -

a) Contractor's invoice showing the materials/ equipment description, quantity, unit price and total price

b) Delivery note

c) Packing list identifying contents of each package

7.9.3 It is the responsibility of the Contractor to ensure that the delivery documents are received by KPLC at the designated delivery point at the time of delivery.

7.10 Insurance

7.10.1 The Contractor shall be responsible for and keep in force current appropriate insurance covers for its property and persons engaged in the performance and or provision of the Services under the contract.

7.10.2 The Contractor shall *(except in respect to losses, injuries or damage resulting from any act or neglect of KPLC)* indemnify and keep indemnified KPLC against all losses and claims for injuries or damage to any person or property whatsoever which may arise out of or in consequence of the contract and against all claims, demands, proceedings, damages, costs, charges, and expenses whatsoever in respect thereof or in relation thereto.

7.11 Payment

7.11.1 Payments shall be made promptly by KPLC and shall not be less than thirty (30) days from completion of satisfactory performance and submission of invoice together with other required and related documents or as otherwise prescribed in the contract.

7.11.2 Payment shall primarily be through KPLC's cheque or Real Time Gross Settlement *(RTGS)* or telegraphic transfer. Where applicable, a copy of a valid Performance Security, stamped, certified as authentic by KPLC, shall form part of the documents to be presented to KPLC before any payment is made.

7.11.3 A Contractor who requests for a Letter of Credit *(hereinafter abbreviated as LC)*–

a) Shall meet the LC bank charges levied by its bank while KPLC shall meet the LC bank charges levied by its bank.

b) Any extension and or amendment charges and any other costs that may result from the Contractor's delays, requests, mistakes or occasioned howsoever by the Contractor shall be to the Beneficiary's account.

c) The maximum number of extensions and amendments shall be limited to two (2).

d) Notwithstanding sub-clause 7.11.3 (a), should the Contractor require a confirmed LC, then all confirmation and any other related charges levied by both the Contractor's and KPLC's bank shall be to the Beneficiary's account.

e) The LC shall be opened only for the specific Order within the validity period of the contract.

f) LCs shall be partial for partial performance or full for whole performance as per the contract.

g) The Contractor shall be required to submit a proforma invoice for each lot

for use in the placement of order and opening of the LC. The proforma invoice shall be on total all-inclusive costs basis.

h) A copy of the Performance Security, stamped and certified as authentic by KPLC, whose expiry date should not be less than sixty (60) days from the LC expiry date, shall form part of the documents to be presented to the Bank before any payment is effected.

7.11.4 KPLC shall have the sole discretion to accept or decline any Contractor's payment request through Letters of Credit without giving any reason for any decline.

7.12 Interest

Interest payment by KPLC is inapplicable in the contract.

7.13 Prices

7.13.1 Subject to clause 7.14 herein below, prices charged by the Contractor for services performed under the contract shall be fixed for the period of the contract with no variations.

7.13.2 A price that is derived by a pre-disclosed incorporation or usage of an internationally accepted standard formula shall not be deemed to be a price variation within the meaning of this clause.

7.14 Variation of Contract

KPLC and the Supplier may vary the contract only in accordance with the following: -

a) the quantity variation of services shall not exceed twenty percent (20%) of the original contract quantity.

b) The cumulative value variation shall not exceed twenty five percent (25%) of the original contract value.

c) the quantity variation must be executed within the period of the contract.

7.15 Assignment

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

7.16 Subcontracts

7.16.1 The Contractor shall notify KPLC in writing of all subcontracts awards under this contract if not already specified in the tender. Such notification, in the original tender or obligation under the Contract shall not relieve the Contractor from any liability or obligation under the Contract.

7.16.2 In the event that an award is given and the contract is sub-contracted, the responsibility and onus over the contract shall rest on the Contractor who was awarded.

7.17 Termination of Contract

7.17.1 KPLC may, without prejudice to any other remedy for breach of contract, by written notice sent to the Contractor, terminate this contract in whole or in part due to any of the following: -

a) if the Contractor fails to perform any or all of the services within the period(s) specified in the contract, or within any extension thereof granted by KPLC.

b) if the Contractor fails to perform any other obligation(s) under the contract.

c) if the Contractor, in the judgment of KPLC has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

d) by an act of force majeure.

e) if the Contractor becomes insolvent or bankrupt

f) if the Contractor has a receiving order issued against it, compounds with its creditors, or an order is made for its winding up (except for the purposes of its amalgamation or reconstruction), or a receiver is appointed over its or any part of its undertaking or assets, or if the Contractor suffers any other analogous action in consequence of debt.

g) if the Contractor abandons or repudiates the Contract.

7.17.2 In the event that KPLC 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 or not rendered, and the Contractor shall be liable to KPLC for any excess costs for such similar services and or any other loss PROVIDED that the Contractor shall not be so liable where the termination is for convenience of KPLC.

7.17.3 The Parties may terminate the Contract by reason of an act of *force majeure* as provided for in the contract.

7.17.4 The Contract may automatically terminate by reason of an act of *force majeure* as provided for in the Contract.

7.18 Liquidated Damages

Notwithstanding and without prejudice to any other provisions of the contract, if the Contractor fails to perform any or all of the services within the period specified in the contract, KPLC shall, without prejudice to its other remedies under the contract, deduct from the contract prices, liquidated damages sum equivalent to 0.5% of the performance price per day of delay of the delayed due services up to a maximum of ten percent (10%) of the performance price of the delayed due services.

7.19 Warranty

7.19.1 Where applicable, the Contractor warrants that the Services provided under the contract are of the highest quality or current specification and incorporate all recent improvements unless provided otherwise in the contract. The Contractor further warrants that any materials/ equipment provided under this contract shall have no defect arising from manufacture, materials or workmanship or from any act or omission of the Contractor that may develop under normal use of the materials/ equipment provided under the conditions obtaining in Kenya.

7.19.2 This warranty will remain valid for the period indicated in the special conditions of contract after the goods, or any portion thereof as the case may be, have been delivered to the final destination indicated in the contract.

7.19.3 KPLC shall promptly notify the Contractor in writing of any claims arising under this Warranty.

7.19.4 Upon receipt of such a notice, the Contractor shall, with all reasonable speed, remedy the defective services without cost to KPLC.

7.19.5 If the Contractor having been notified, fails to remedy the defect(s) within a reasonable period, KPLC may proceed to take such remedial action as may be necessary, at the

Contractor's risk and expense and without prejudice to any other rights which KPLC may have against the Contractor under the contract.

7.20 Resolution of Disputes

7.20.1 KPLC and the Contractor may make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with the contract.

7.20.2 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 resort to resolution before a recognized local forum for the resolution of disputes.

7.21 Language and Law

The language of the contract and the law governing the contract shall be the English language and the laws of Kenya respectively unless otherwise stated.

7.22 Waiver

Any omission or failure by KPLC to exercise any of its rights or enforce any of the penalties arising from the obligations imposed on the Contractor shall in no way, manner or otherwise howsoever, alter, amend, prejudice, vary, waive or be deemed to alter, amend, prejudice, vary, waive or otherwise whatsoever any of KPLC's powers and rights as expressly provided in and as regards this contract.

7.23 Force Majeure

7.23.1 Force majeure means any circumstances beyond the control of the parties, including but not limited to:

a) war and other hostilities (whether war be declared or not), invasion, act of foreign enemies, mobilization, requisition or embargo;

b) ionizing radiation or contamination by radio-activity from any nuclear fuel or from any nuclear waste from the combustion of nuclear fuel, radioactive toxic explosives or other hazardous properties of any explosive nuclear assembly or nuclear components thereof;

c) rebellion, revolution, insurrection, military or usurped power & civil war;

d) riot, commotion or disorder except where solely restricted to employees servants or agents of the parties;

e) un-navigable storm or tempest at sea.

7.23.2 Notwithstanding the provisions of the contract, neither party shall be considered to be in default or in breach of its obligations under the Contract to the extent that performance of such obligations is prevented by any circumstances of *force majeure* which arise after the contract is entered into by the parties.

7.23.3 If either party considers that any circumstances of *force majeure* are occurring or have occurred which may affect performance of its obligations it shall promptly notify the other party and provide reasonable proof of such circumstances.

7.23.4 Upon the occurrence of any circumstances of *force majeure*, the Contractor shall endeavour to continue to perform its obligations under the contract so far as is reasonably practicable. The Contractor shall notify KPLC of the steps it proposes to take including any reasonable alternative means for performance, which is not prevented by *force majeure*. The Contractor shall not take any such steps unless directed so to do by KPLC.

7.23.5 If the Contractor incurs additional costs in complying with KPLC's directions under sub clause 7.23.4, then notwithstanding the provisions of the contract, the amount thereof shall be agreed upon with KPLC and added to the contract price.

7.23.6 If circumstances of *force majeure* have occurred and shall continue for a period of twenty one (21) days then, notwithstanding that the Contractor may by reason thereof have been granted an extension of time for performance of the contract, either party shall be entitled to serve upon the other seven (7) days' notice to terminate the contract. If at the expiry of the period of twenty-eight (28) days, *force majeure* shall still continue, the contract shall terminate.

SECTION VIII – SPECIAL CONDITIONS OF CONTRACT

The Special Conditions of Contract *hereinafter abbreviated as SCC* shall form part of the Conditions of Contract. They are made in accordance with the law and KPLC's guidelines, practices, procedures and working circumstances. They shall amend, add to and vary the GCC. The clauses in this section need not therefore, be completed but must be completed by KPLC if any changes to the GCC provisions are deemed necessary. Whenever there is a conflict between the GCC and SCC, the provisions of the SCC shall prevail over those in the GCC.

No.	GCC Reference Clause	Particulars of SCC
1.	**7.26.2 Period of Warranty**	*One Year*
2.	**7.18.1 Payment Period**	Payments shall be made promptly by KPLC thirty (30) days from delivery and submission of invoice together with other required and related documents or as otherwise prescribed in the contract.
3.	**Delivery**	Delivery will be within the date stipulated in the bids. Deliveries may be subjected to Customer Delivery Inspection. Delivery of goods within 8 weeks of LPO issue is preferred.
4	**Service Level Agreement**	The Maintenance support (SLA) contract shall be renewed for three years.

Director's Signature: ……. Date…….

Official Stamp…….....

SECTION IX - TENDER FORM

Date:
Tender No.

To:
The Kenya Power & Lighting Company Limited,
Stima Plaza,
Kolobot Road, Parklands,
P.O Box 30099 – 00100,
Nairobi, Kenya.

Ladies and Gentlemen,

1. Having read, examined and understood the Tender Document including all Addenda, the receipt of which is hereby duly acknowledged, we, the undersigned Tenderer, offer to perform, deliver, install and commission *(the latter two where applicable)* ……. *(insert services description)* in accordance and conformity with the said tender document and in particular the Schedule of Prices that are made part of this Tender.

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

3. If our Tender is accepted, we will obtain the guarantee of a bank in a sum of equivalent to ten percent (10%) of the contract price for the due performance of the contract, in the form(s) prescribed by The Kenya Power & Lighting Company Limited.

4. We agree to abide by this Tender for a period of……days **(Tenderer please indicate validity of your Tender)** from the date fixed for tender opening as per the Tender Document, and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

5. This Tender, together with your written acceptance thereof and your notification of award, shall not constitute a contract, between us. The contract shall be formed between us when both parties duly sign the written contract.

6. We understand that you are not bound to accept any Tender you may receive.

Yours sincerely,

_____

Name of Tenderer

_____

Signature of duly authorised person signing the Tender

_____

Name and Designation of duly authorised person signing the Tender

_____

Stamp or Seal of Tenderer

***NOTES:**

1. KPLC requires a validity period of at least one hundred and twenty(120) days.
2. This form must be duly signed, stamped and/or sealed.

SECTION X - CONFIDENTIAL BUSINESS QUESTIONNAIRE FORM

All Tenderers are requested to give the particulars indicated in Part 1 and either Part 2 (a), 2 (b) or 2 (c), whichever applies 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 …….. Postal Code …….

Tel No……..

Facsimile..……..

Mobile and/ or CDMA No…….

E-mail:……

Nature of your business ……..
Registration Certificate No.……

Maximum value of business which you can handle at any time KSh…….

Name of your Bankers ……..Branch… ……

*Names of Tenderer's contact person(s) …….

Designation of the Tenderer's contact person(s) ……

Address, Tel, Fax and E-mail of the Tenderer's contact person(s) …….
……...
……

Part 2 (a) Sole Proprietor

Your name in full …….

Nationality ……Country of origin ……..

*Citizenship details…….

Part 2 (b) Partnership

Give details of partners as follows: -

Names	Nationality	*Citizenship Details	Shares
1……			
2……			
3……			
4……			
5……			

Part 2 (c) Registered Company

Private or Public …….

State the nominal and issued capital of company-

Nominal KSh.……

Issued KSh……

Give details of all directors as follows

Name	Nationality	*Citizenship Details	Shares
1…….			
2…….			
3……..			
4……..			
5……..			

Name of duly authorized person to sign for and on behalf of the Tenderer

……..……..

Designation of the duly authorized person……

Signature of the duly authorized person……..

***NOTES TO THE TENDERERS ON THE QUESTIONNAIRE**

1. *The address and contact person of the Tenderer provided above shall at all times be used for purposes of this tender.*
2. *If a Kenyan citizen, please indicate under "Citizenship Details" whether by birth, naturalization or registration.*
3. *The details on this Form are essential and compulsory for all Tenderers.* **Failure to provide all the information requested shall lead to the Tenderer's disqualification**.
4. *For foreign Tenderers please give the details of nominal and issued share capital in the currency of the country of origin of the Tenderer.*

SECTION XI A - TENDER SECURITY FORM – (BANK GUARANTEE)

(To Be Submitted On Bank's Letterhead) **Date:**

To:
The Kenya Power & Lighting Company Limited,
Stima Plaza,
Kolobot Road, Parklands,
P.O Box 30099 – 00100,
Nairobi, Kenya.

WHEREAS …… (*name of the Tenderer*) (*hereinafter called "the Tenderer")* has submitted its Tender dated …… for the supply, installation and commissioning of…… *(please insert KPLC tender no. and name*) *(hereinafter called "the Tender");*

KNOW ALL PEOPLE by these presents that **WE**…….of …….having our registered office at…….*(hereinafter called "the Bank")*, are bound unto The Kenya Power and Lighting Company Limited (*hereinafter called "KPLC" which expression shall where the context so admits include its successors-in-title and assigns*) in the sum of ……. for which payment well and truly to be made to the said KPLC, the Bank binds itself, its successors, and assignees by these presents.

We undertake to pay you, upon your first written demand declaring the Tenderer to be in breach of the tender requirements and without cavil or argument, the entire sum of this guarantee being …….. (*amount of guarantee*) as aforesaid, without you needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This tender 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 date below.

This guarantee is valid until the …..…day of……20……

EITHER

SEALED with the)
COMMON SEAL)

of the said **BANK**) _____
this ……day) BANK SEAL
of ……20….)

)
in the presence of :-)
)
_____)
)
and in the presence of:-)
)
_____)

OR

SIGNED by the **DULY AUTHORISED REPRESENTATIVE(S)/ ATTORNEY(S)** of the **BANK**

_____
Name(s) and Designation of duly authorised representative(s)/ attorney(s) of the Bank

_____
Signature(s) of the duly authorised person(s)

NOTES TO TENDERERS AND BANKS

1. *Please note that no material additions, deletions or alterations regarding the contents of this Form shall be made to the Tender Security to be furnished by the Tenderer. If any are made, the Tender Security shall not be accepted and shall be rejected by KPLC. For the avoidance of doubt, such rejection will be treated as non-submission of the Tender Security where such Security is required in the tender.*

2. *It is the responsibility of the Tenderer to sensitize its issuing bank on the need to respond directly and expeditiously to queries from KPLC. The period for response shall not exceed three (3) days from the date of KPLC's query. Should there be no conclusive response by the Bank within this period, such Tenderer's Tender Security shall be deemed as invalid and the bid rejected.*

3. ***The issuing bank should address its response or communication regarding the bond to KPLC at the following e-mail address – "guarantees@ kplc.co.ke"***

4. *The Tender validity period is one twenty (120) days as set out in the Invitation to Tender (at Section I of the Tender document) or as otherwise may be extended by KPLC. Therefore the Tender Security must at all times be valid for at least 30 days beyond the tender validity period.*

SECTION XI B - TENDER SECURITY FORM (SACCO SOCIETY, DEPOSIT TAKING MICRO FINANCE INSTITUTIONS, WOMEN ENTERPRISE FUND & YOUTH ENTERPRISE FUND)

(To Be Submitted On Institutions Letterhead) **Date:**

To:
The Kenya Power & Lighting Company Limited,
Stima Plaza,
Kolobot Road, Parklands,
P.O Box 30099 – 00100,
Nairobi, Kenya.

WHEREAS……(hereinafter called "the Contractor") has undertaken, in pursuance of your Tender Number……..(*reference number of the Tender)* and its Tender dated ……*(insert Contractor's date of Tender taken from the Tender Form)* to supply ……(*description of the Works*) (hereinafter called "the Contract);

AND WHEREAS it has been stipulated by you in the said Contract that the Contractor shall furnish you with an Institution's guarantee by an acceptable Institution for the sum specified therein as security for compliance of the Contractor's performance obligations in accordance with the Contract;

AND WHEREAS we have agreed to give the Contractor a Guarantee;

THEREFORE WE HEREBY AFFIRM that we are Guarantors and responsible to you, on behalf of the Contractor, 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 Contractor 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 you 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….

EITHER
SEALED with the)
COMMON SEAL)
of the said **INSTITUTION**)

)

this ……day)
)
of ……20….)
in the presence of :-)
)
_____)
)
and in the presence of:-)
)
_____)

_____
INSTITUTION SEAL

OR

SIGNED by the **DULY AUTHORISED REPRESENTATIVE(S)/ ATTORNEY(S)** of the **INSTITUTION**

_____
Name(s) and Designation of duly authorised representative(s)/ attorney(s) of the **Institution**.

_____
Signature(s) of the duly authorised person(s)

NOTES TO SUPPLIERS AND INSTITUTIONS

1. *Please note that no material additions, deletions or alterations regarding the contents of this Form shall be made to the Tender Security to be furnished by the Tenderer. If any are made, the Tender Security shall not be accepted and shall be rejected by KPLC. For the avoidance of doubt, such rejection will be treated as non-submission of the Tender Security where such Security is required in the tender.*

2. *It is the responsibility of the Tenderer to sensitize its issuing institution on the need to respond directly and expeditiously to queries from KPLC. The period for response shall not exceed three (3) days from the date of KPLC's query. Should there be no conclusive response by the institution within this period, such Tenderer's Tender Security shall be deemed as invalid and the bid rejected.*

3. ***The issuing institution should address its response or communication regarding the Tender Security to KPLC at the following e-mail address** – "guarantees@ kplc.co.ke"*

4. *The Tender validity period is one twenty (120) days as set out in the Invitation to Tender (at Section I of the Tender document) or as otherwise may be extended by KPLC. Therefore the Tender Security must at all times be valid for at least 30 days beyond the tender validity period.*

SECTION XI C - TENDER SECURITY – (LETTERS OF CREDIT)

The Mandatory Conditions to be included in the Letters are in two parts, A and B.

Part A

Form of Documentary credit - "Irrevocable Standby"

Applicable rules - "Must be UCP Latest Version" i.e. UCP 600 (2007 REVISION) ICC Publication No. 600.

Place of expiry - At the counters of the advising bank.

The SBLC should be available – "By Payment"

Drafts should be payable at - "SIGHT"

Documents required -

1. Beneficiary's signed and dated statement demanding for payment under the letter of credit no…….. (*Insert LC No*.) as…….(*Name of applicant*) (hereinafter called the "Tenderer") indicating that the "Tenderer*"* has defaulted in the obligations of the Tenderer as stated by the Beneficiary.

2. The Original Letter of Credit and all amendments, if any.

Additional Conditions -

1. All charges levied by any bank that is party to this documentary credit are for the account of the applicant.

2. There should be no conditions requiring compliance with the specific regulations or a particular country's Law and regulations.

Charges - All bank charges are for the account of the applicant.

*****Confirmation instructions – (See notes below)

Part B

The proceeds of these Letters are payable to KPLC -

a) if the Tenderer withdraws its Tender after the deadline for submitting Tenders but before the expiry of the period during which the Tenders must remain valid.

b) if the Tenderer fails to enter into a written contract in accordance with the Tender Document

c) if the successful Tenderer fails to furnish the performance security in accordance with the Tender Document.

d) if the Tenderer fails to extend the validity of the tender security where KPLC has extended the tender validity period in accordance with the Tender Document.

NOTES TO TENDERERS AND BANKS.

1. *Please note that should the Tender Security (LC) omit any of the above conditions the LC shall not be accepted and shall be rejected by KPLC. For the avoidance of doubt, such rejection will be treated as non-submission of the LC where such LC is required in the Tender.*

2. *It is the responsibility of the Tenderer to sensitize its issuing bank on the need to respond directly and expeditiously to any queries from KPLC. The period for response shall not three (3) days from the date of KPLC's query. Should there be no conclusive response by the Bank within this period, such Tenderer's Tender Security shall be deemed as invalid and the bid rejected.*

3. ***The issuing bank should address its response or communication regarding the bond to KPLC at the following e-mail address – "guarantees@ kplc.co.ke"***

4. *The Tender validity period is one twenty (120) days as set out in the Invitation to Tender (at Section I of the Tender document) or as otherwise may be extended by KPLC. Therefore the Tender Security must at all times be valid for at least 30 days beyond the tender validity period.*

5. *All Guarantees issued by foreign banks must be confirmed by a local bank in Kenya.*

SECTION XII - MANUFACTURER'S/ PRINCIPAL'S AUTHORIZATION FORM

(To Be Submitted On Manufacturer's/ Principal's/ Producer's Letterhead)

To:
The Kenya Power & Lighting Company Limited,
Stima Plaza,
Kolobot Road, Parklands,
P.O Box 30099 – 00100,
Nairobi, Kenya.

WHEREAS WE ……(*name of the manufacturer/ principal*) who are established and reputable manufacturers/ principal of ……
(*name and description of the services*) having offices or factories at ……*(full address and physical location of offices or factory(ies)* do hereby confirm that ……
(*name and address of Contractor*) is authorized by us to transact in the services required against your Tender …… (*insert reference number and name of the Tender*) in respect of the above services.

WE HEREBY extend our full guarantee and warranty as per the Conditions of Contract for the services offered for provision by the above firm against the Invitation to Tender.

DATED THIS…….. DAY OF…….20……

_____
Signature of duly authorised person for and on behalf of the Manufacturer/ Principal.

_____
Name and Designation of duly authorised person signing on behalf of the Manufacturer/ Principal.

NOTES TO TENDERERS & MANUFACTURERS/ PRINCIPALS/ PRODUCERS

Only a competent person in the service of the Manufacturer/ Principal should sign this letter of authority.

SECTION XIII - DECLARATION FORM

Date _____

To:

The Kenya Power & Lighting Company Limited,
P.O Box 30099 – 00100,
Stima Plaza, Kolobot Road, Parklands,
Nairobi,
KENYA.

Ladies and Gentlemen,

The Tenderer i.e. (full name and complete physical and postal address)_____
_____declare the following: -

a) That I/ We have not been debarred from participating in public procurement by anybody, institution or person.
b) That I/ We have not been involved in and will not be involved in corrupt and fraudulent practices regarding public procurement anywhere.
c) That I/We or any director of the firm or company is not a person within the meaning of paragraph 3.2 of ITT (Eligible Tenderers) of the Instruction to Tenderers.
d) That I/ We are not insolvent, in receivership, bankrupt or in the process of being wound up and is not the subject of legal proceedings relating to the foregoing.
e) That I/We do hereby confirm that all the information given in this tender is accurate, factual and true to the best of our knowledge.
f) That I/ We are not associated with any other Tenderer participating in this tender.

Yours sincerely,

_____
Name of Tenderer

_____
Signature of duly authorised person signing the Tender

_____
Name and Designation of duly authorised person signing the Tender

_____
Stamp or Seal of Tenderer

SECTION XIV – DRAFT LETTER OF NOTIFICATION OF AWARD

To:
(Name and full address of the Successful Tenderer)……..

Dear Sirs/ Madams,

RE: NOTIFICATION OF AWARD OF TENDER NO. ……

We refer to your Tender dated…… and are pleased to inform you that following evaluation, your Tender has been accepted as follows: -

……
……

This notification does not constitute a contract. The formal Contract Agreement, which is enclosed herewith shall be entered into upon expiry of fourteen (14) days from the date hereof pursuant to the provisions of the Public Procurement and Asset Disposal Act, 2015 *(or as may be amended from time to time or replaced).*

Kindly sign, and seal the Contract Agreement. Further, initial and stamp on all pages of the documents forming the Contract that are forwarded to you with this letter. Thereafter return the signed and sealed Contract together with the documents to us within fourteen (14) days of the date hereof for our further action.

We take this opportunity to remind you to again note and strictly comply with the provisions as regards the Tender Security, Signing of Contract and Performance Security as stated in the Instructions to Tenderers.

We look forward to a cordial and mutually beneficial business relationship.

Yours faithfully,
FOR: THE KENYA POWER & LIGHTING COMPANY LIMITED

GENERAL MANAGER, SUPPLY CHAIN

Enclosures

SECTION XV – DRAFT LETTER OF NOTIFICATION OF REGRET

To: *(Name and full address of the Unsuccessful Tenderer)……* **Date:**

Dear Sirs/ Madams,

RE: **NOTIFICATION OF REGRET IN RESPECT OF TENDER NO. ……**

We refer to your Tender dated…… and regret to inform you that following evaluation, your Tender is unsuccessful. It is therefore not accepted. The brief reasons are as follows:-

1. ……
2. ……
3. …… etc…

The successful bidder was _____.

However, this notification does not reduce the validity period of your Tender Security. In this regard, we request you to relook at the provisions regarding the Tender Security, Signing of Contract and Performance Security as stated in the Instructions to Tenderers.

You may collect the tender security from our *Legal Department (Guarantees Section), on the 2nd Floor, Stima Plaza, Kolobot Road, Parklands, Nairobi* only after expiry of twenty five (25) days from the date hereof on Mondays and Wednesdays ONLY between 9.00 a.m to 12.30 pm and 2.00p.m to 4.00p.m.
It is expected that by that time KPLC and the successful bidder will have entered into a contract pursuant to the Public Procurement and Asset Disposal Act, 2015 *(or as may be amended from time to time or replaced).* When collecting the Security, you will be required to produce the original or certified copy of this letter.

We thank you for the interest shown in participating in this tender and wish you well in all your future endeavours.

Yours faithfully,
FOR: THE KENYA POWER & LIGHTING COMPANY LIMITED

GENERAL MANAGER, SUPPLY CHAIN

SECTION XVI - CONTRACT AGREEMENT FORM

THIS AGREEMENT made this**……**day of**…….20…. BETWEEN THE KENYA POWER & LIGHTING COMPANY LIMITED**, a limited liability company duly incorporated under the Companies Act, Chapter 486 of the Laws of Kenya, with its registered office situated at Stima Plaza, Kolobot Road, Parklands, Nairobi in the Republic of Kenya and of Post Office Box Number 30099-00100, Nairobi in the Republic aforesaid *(hereinafter referred to as the "KPLC")* of the one part,

AND

…….. (*Contractor's full name and principal place of business*) a duly registered entity according to the laws of**…… *(state country)*** and of Post Office Box Number/Physical Address **…….*(full address physical and postal of Contractor)*** in the Republic aforesaid, *(hereinafter referred to as the "Contractor"* of the other part;

WHEREAS KPLC invited tenders for certain services, that is to say for **…… (*KPLC Supply Chain – Procurement Department insert description of services*)** under Tender Number**…….. (*KPLC Supply Chain – Procurement Department insert tender number*)**

AND WHEREAS KPLC has accepted the Tender by the Contractor for the services in the sum of **……**(***KPLC Supply Chain – Procurement Department specify the total amount in words which should include any payable taxes, duties and insurance where applicable e.g. Value Added Tax)*** (*hereinafter called "the Contract Price"*).

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 and the Tender Document.

2. Unless the context or express provision otherwise requires: -
   a) reference to "this Agreement" includes its recitals, any schedules and documents mentioned hereunder and any reference to this Agreement or to any other document includes a reference to the other document as varied supplemented and or replaced in any manner from time to time.
   b) any reference to any Act shall include any statutory extension, amendment, modification, re-amendment or replacement of such Act and any rule, regulation or order made thereunder.
   c) words importing the masculine gender only, include the feminine gender or (as the case may be) the neutral gender.
   d) words importing the singular number only include the plural number and

vice-versa and where there are two or more persons included in the expression the *"Contractor"* the covenants, agreements obligations expressed to be made or performed by the Contractor shall be deemed to be made or performed by such persons jointly and severally.

e) where there are two or more persons included in the expression the *"Contractor"* any act default or omission by the Contractor shall be deemed to be an act default or omission by any one or more of such persons.

3. In consideration of the payment to be made by KPLC to the Contractor as hereinbefore mentioned, the Contractor hereby covenants with KPLC to perform and provide the services and remedy any defects thereon in conformity in all respects with the provisions of the Contract.

4. KPLC hereby covenants to pay the Contractor in consideration of the proper performance and provision of the services 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.

5. The following documents shall constitute the Contract between KPLC and the Contractor and each shall be read and construed as an integral part of the Contract: -

a) this Contract Agreement
b) the Special Conditions of Contract as per the Tender Document
c) the General Conditions of Contract as per the Tender Document
d) the Price Schedules submitted by the Contractor and agreed upon with KPLC.
e) the Details of Service as per KPLC's Tender Document
f) the Schedule of Requirements
g) KPLC's Notification of Award dated……
h) the Tender Form signed by the Contractor
i) the Declaration Form signed by the Contractor/ successful Tenderer
j) the Warranty
h) project implementation schedule

6. In the event of any ambiguity or conflict between the contract documents listed above, the order of precedence shall be the order in which the contract documents are listed in 5 above except where otherwise mutually agreed in writing.

7. The Commencement Date shall be the working day immediately following the fulfillment of all the following: -

a) Execution of this Contract Agreement by KPLC and the Contractor.
b) Issuance of the Performance Bond by the Contractor and confirmation of its authenticity by KPLC.
c) Issuance of the Official Order by KPLC to the Contractor.

d) Where applicable, Opening of the Letter of Credit by KPLC.

8. The period of contract validity shall begin from the Commencement date and end on either -

a) sixty (60) days after the last date of the agreed performance schedule, or,
b) where a Letter of Credit is adopted as a method of payment, sixty (60) days after the expiry date of the Letter of Credit or the expiry date of the last of any such opened Letter of Credit whichever is later.

Provided that the expiry period of the Warranty shall be as prescribed and further provided that the Warranty shall survive the expiry of the contract.

9. It shall be the responsibility of the Contractor to ensure that its Performance Security is valid at all times during the period of contract validity and further is in the full amount as contracted.

10. Any amendment, change, addition, deletion or variation howsoever to this Contract shall only be valid and effective where expressed in writing and signed by both parties.

11. No failure or delay to exercise any power, right or remedy by KPLC shall operate as a waiver of that right, power or remedy and no single or partial exercise of any other right, power or remedy.

12. Notwithstanding proper completion of performance or parts thereof, all the provisions of this Contract shall continue in full force and effect to the extent that

any of them remain to be implemented or performed unless otherwise expressly agreed upon by both parties.

13. Any notice required to be given in writing to any Party herein shall be deemed to have been sufficiently served, if where delivered personally, one day after such delivery; notices by electronic mail shall be deemed to be served one day after the date of such transmission and delivery respectively, notices sent by post shall be deemed served seven (7) days after posting by registered post (*and proof of posting shall be proof of service*), notices sent by courier shall be

deemed served two (2) days after such receipt by the courier service for Local Suppliers and five (5) days for Foreign Suppliers.

14. For the purposes of Notices, the address of KPLC shall be Company Secretary, The Kenya Power & Lighting Company Limited, 7th Floor, Stima Plaza, Kolobot Road, Post Office Box Number 30099–00100, Nairobi, Kenya. The address for the Contractor shall be the

Contractor's address as stated by it in the Confidential Business Questionnaire provided in the Tender Document.

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

SIGNED for and on behalf
of **KPLC**

_____
MANAGING DIRECTOR & CEO

and in the presence of:-

_____
COMPANY SECRETARY

SEALED with the **COMMON SEAL**
of the **CONTRACTOR**
in the presence of:-

_____ _____
DIRECTOR *Affix Contractor's Seal here*

_____
DIRECTOR'S FULL NAMES

and in the presence of:-

_____
DIRECTOR/ COMPANY SECRETARY

_____
DIRECTOR/ COMPANY SECRETARY'S FULL NAMES

DRAWN BY: -
Imelda Bore,
Advocate,
C/o The Kenya Power & Lighting Company Limited,
7th Floor, Stima Plaza,
Kolobot Road, Parklands,
Post Office Box Number 30099–00100,
NAIROBI, KENYA,

Telephones: + 254-20-3201000/ 731

SECTION XVII A - PERFORMANCE SECURITY FORM (BANK GUARANTEE)

(To Be Submitted On Bank's Letterhead) **Date:**

To:
The Kenya Power & Lighting Company Limited,
Stima Plaza,
Kolobot Road, Parklands,
P.O Box 30099 – 00100,
Nairobi, Kenya.

WHEREAS……(hereinafter called "the Supplier") has undertaken, in pursuance of your Tender Number……..(*reference number of the Tender)* and its Tender dated ……*(insert Supplier's date of Tender taken from the Tender Form)* to supply ……(*description of the goods*) (hereinafter called "the Contract);

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a bank guarantee by an acceptable bank for the sum specified therein as security for compliance of the Supplier's performance obligations in accordance with the Contract;

AND WHEREAS we have agreed to give the Supplier a guarantee;

THEREFORE WE HEREBY AFFIRM that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total sum of……. (*amount of the guarantee in words and figures*) and we undertake to pay you, upon your first written demand declaring the Supplier 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 you 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….

EITHER

SEALED with the)
COMMON SEAL)
of the said **BANK**)
)

this ……day)
) _____
) BANK SEAL

of ……20….)
in the presence of :-)
)
_____)
)
and in the presence of:-)
)
_____)

OR

SIGNED by the **DULY AUTHORISED REPRESENTATIVE(S)/ ATTORNEY(S)** of the **BANK**

_____

Name(s) and Designation of duly authorised representative(s)/ attorney(s) of the Bank

_____

Signature(s) of the duly authorised person(s)

NOTES TO SUPPLIERS AND BANKS

1. *Please note that no material additions, deletions or alterations regarding the contents of this Form shall be made to the Performance Security Bond (the Bond) to be furnished by the successful Tenderer/ Supplier. If any are made, the Bond may not be accepted and shall be rejected by KPLC. For the avoidance of doubt, such rejection will be treated as non-submission of the Bond where such Bond is required in the tender and Contract.*

2. *KPLC shall seek authentication of the Performance Security from the issuing bank. It is the responsibility of the Supplier to sensitize its issuing bank on the need to respond directly and expeditiously to queries from KPLC. The period for response shall not exceed five (5) days from the date of KPLC's query. Should there be no conclusive response by the Bank within this period, such Supplier's Performance Security may be deemed as invalid and the Contract nullified.*

3. ***The issuing Bank should address its response or communication regarding the bond to KPLC at the following e-mail address – "guarantees@ kplc.co.ke"***

SECTION XVII B - PERFORMANCE SECURITY (LC)

Mandatory Conditions that should appear on the Performance Security (LC).

Form of Documentary credit - "Irrevocable Standby"

Applicable rules - "Must be UCP Latest Version" i.e. UCP 600 (2007 REVISION) ICC Publication No. 600.

Place of expiry - At the counters of the advising bank.

The SBLC should be available – "By Payment"

Drafts should be payable at - "SIGHT"

Documents required -

1. Beneficiary's signed and dated statement demanding for payment under the letter of credit no…….. (*Insert LC No*.) as…….(*Name of Applicant*) (hereinafter called the "Supplier") indicating that the "Supplier" has defaulted in the performance and adherence to and performance of the contract between the Beneficiary and the Supplier.

2. The Original Letter of Credit and all amendments, if any.

Additional Conditions -

1. All charges levied by any bank that is party to this documentary credit are for the account of the Applicant.

2. (Include) that there should be no conditions requiring compliance with the specific regulations or a particular country's laws and regulations.

Charges - All bank charges are for the account of the Applicant.

Confirmation instructions – (See notes below)

NOTES TO SUPPLIERS AND BANKS

1. Please note that should the Performance Security (LC) omit any of the above conditions the LC shall not be accepted and shall be rejected by KPLC. For the avoidance of doubt, such rejection will be treated as non-submission of the LC where such LC is required in the tender and Contract.

2. KPLC may seek authentication of the Performance Security (LC) from the issuing bank. It is the responsibility of the Supplier to sensitize its issuing bank on the need to respond directly and expeditiously to queries from KPLC. The period for

response shall not exceed three (3) days from the date of KPLC's query. Should there be no conclusive response by the Bank within this period, such Supplier's Performance Security (LC) may be deemed as invalid and the Contract nullified.

3. ***The issuing bank should address its response or communication regarding the bond to KPLC at the following e-mail address – "guarantees@ kplc.co.ke"***

4. *All Guarantees issued by foreign banks must be confirmed by a local bank in Kenya.*

SECTION XVIII – SUBCONTRACTORS

(INFORMATION TO BE PROVIDED BY THE TENDERER)

As per the requirements of Clause 7.23 of General Conditions of Contract, following is a list of subcontractors and the portions of the Work to be subcontracted:

No.	Subcontractor	Address	Brief Description of the Works to be Subcontracted	% works subcontracted

SECTION XIX - PREVIOUS EXPERIENCE WITH SIMILAR WORK

(INFORMATION TO BE PROVIDED BY THE TENDERER)

As required by Section 3.13.3(d) of the Instructions To Tenderers, following is a list of work that the Tenderer has previously performed which is similar to that described in the Request for Proposal:

No.	Description	Customer Name & Contacts	Date of Supply

SECTION XX - SUPPLIER EVALUATION FORM

(This form is for information only and <u>not</u> to be filled in by any bidder. It is for official use by KPLC to evaluate performance of Suppliers during the contract period)

Name of Firm……...Date……

Category of Product/Service (e.g. Conductors ……

Period of evaluation…….....

1. COST OF SERVICE/PRODUCT	Rating guidelines				Supplier Score	Procurement Score	User Score	Comments	Totals
	Did the vendor assist in or advice on ways of reducing the costs?	YES:4	PARTIALLY:2	NO: 0					10
	How closely did your final costs correspond to your expectation at the beginning of the project/tender?	YES:2	PARTIALLY:1	NO: 0					10.00%
	Did the company stick to the agreed transaction/contract rates?	YES:4	PARTIALLY:2	NO: 0					
2.ON TIME DELIVERY OF PRODUCT OR SERVICE									Totals
	Did the vendor perform work in compliance with contract terms and agreements?	YES:6	PARTIALLY:3	NO: 0					10
	Was the vendor prompt and effective in correction of situations and conditions?	YES:2	PARTIALLY:1	NO: 0					10.00%
	Are you able to track service level agreements and determine duration of incidents from the vendor?	YES:2	PARTIALLY:1	NO: 0					
3. FLEXIBILITY TO RESPOND TO UNEXPECTED DEMAND OF SERVICE	Rating guidelines								Totals
	Was the vendor willing to change their product/service on special needs?	YES:6	PARTIALLY:3	NO: 0					6
									6.00%
4. QUALITY	Rating guidelines								Totals
	When performing their duties, was there - rework or returns caused by non-conformance to quality?	NO:6	PARTIALLY:3	YES: 0					14
	Was the quality of service delivered equal to KPLC minimum requirements?	YES:8	PARTIALLY:4	NO:0					14.00%
5.RESPONSIVENESS	Rating guidelines								Totals
	Was the vendor well responsive to information requests, issues, or problems that arose in the course of service?	YES:2	PARTIALLY:1	NO: 0					14
	Was the vendor open to feedback on low quality of service levels and willing to act on this?	YES:6	PARTIALLY:3	NO: 0					14.00%
	Is it easy to reach staff members of suppliers in case of a request or query? (are communication channels clear?)	YES:6	PARTIALLY:3	NO: 0					
6. CUSTOMER SUPPORT	Rating guidelines								Totals
	Did the vendor offer effective customer support?	YES:10	PARTIALLY:4	NO: 0					18
	In case of reported problems/issues, were there follow ups by the vendor to ensure the problem is fully resolved during support?	YES:8	PARTIALLY:4	NO: 0					18.00%

7. COMMUNICATION SKILLS	**Rating guidelines**								**Totals**
	Are you satisfied with the attitude, courtesy, and professionalism of this vendor's staff? Written or spoken?	**YES:2**	**PARTIALLY:1**	**NO: 0**					6
	Are the vendor's staff well equipped and skilled in handling requests / issues? Are you rotated too much among staff on an issue?	**YES:4**	**PARTIALLY:2**	**NO: 0**					6.00%
8. DOCUMENTATION AND ACCOUNTING	**Rating guidelines**								**Totals**
	Are you satisfied with how the Vendor presents documentation (invoices & licenses etc) when required to do so, to necessitate finalization of contract renewals and payments?	**YES:6**	**PARTIALLY:3**	**NO: 0**					10
	Was problem documentation (incident reports) presented promptly by the vendor and was it complete?	**YES:4**	**PARTIALLY:2**	**NO: 0**					10.00%
9. VALUE ADD	**Rating guidelines**								**Totals**
	Did the vendor go over and above in optimizing service delivery process for effective services delivery?	**YES:6**	**PARTIALLY:3**	**NO: 0**					12
	Did the vendor go over and above and offer training or knowledge to assist with better systems support?	**YES:6**	**PARTIALLY:3**	**NO: 0**					12.00%
									Totals
									Score:
Totals									100.0
Maximum Score							**100.0**		100.00%
VENDOR'S TOTAL SCORE									
VENDOR'S PERCENTAGE SCORE									
ISSUES FOR FOLLOW UP -									
Evaluation Done by:	Name		Department				Date		
Checked/Validated by									

Score in Percentage % ……

PERFORMANCE LEVEL DEFINATION;

≥75% - KP1 GREEN
50% - KP2 AMBER
25% - KP3 YELLOW
≤ 25% - KP4 RED

RATING: 75% - V Good, 50% - Good, 25% - Fair, Below 25% - Poor

RECOMMENDATION

		Status	**Tick as appropriate**
1	Grant supplier preferred status	**KP1**	

2	Work with supplier or develop and improve supplier	**KP2 & KP3**	
3	Abandon / switch suppliers	**KP4**	

Name:……Sign:……..Date:……...

Name:……Sign:……..Date:……...

Name:……Sign:……..Date:……...

SECTION XXVII - THE TECHNICAL SPECIFICATIONS

Technical specifications describe the basic requirements for goods. In addition to the information and documentation in the Tender Document regarding the technical aspects of this tender, all Tenderers shall comply with the following -

PART A - GENERAL REQUIREMENTS

1. Technical documentation shall be in English language.
2. The specific items on offer shall be marked clearly for the goods they intend to supply. The type reference or model number(s) of the item(s) on offer must be clearly indicated in the bid.
3. The Tenderer shall submit the Schedule of Guaranteed Technical Particulars (GTP) completed and signed by the Manufacturer. In submitting the GTP, cross-references should be made to the documents submitted.
4. Deviations from the tender specifications, if any, shall be explained in detail in writing, with supporting data including calculation sheets, detailed drawings and certified test reports and submitted together with the Tender. In submitting the deviations, cross- references should be made to the documents submitted. KPLC reserves the right to reject the goods if such deviations shall be found critical to the use and operation of the goods.
5. Detailed contact information including title, e-mail, facsimile, telephone or any other form of acceptable communication of the testing and standards body used shall be provided.
6. Where Type Test Certificates and their Reports and or Test Certificates and their Reports are translated into English, all pages of the translations must be signed and stamped by the testing authority.
7. A Copy of the manufacturer's valid quality management system certification i.e. ISO 9001:2015 shall be submitted for evaluation. For locally manufactured goods, valid KEBS Mark of Quality Certificate or KEBS Standardisation Mark Certificate will also be accepted.
8. In all cases where the level of galvanizing and painting is not specifically stated in the detailed Technical Specifications, the general requirement shall be for a uniform coating of thickness not less than 80 microns.
9. Tenderers are required to provide information on proper representative(s) and or workshop for back-up service and or repair and maintenance including their names, telephone, facsimile, e-mail, physical and postal addresses, along with their offers.
10. Improvement process

10.1 The Tenderer shall provide a description of the continuous improvement process that it has in place to improve quality, delivery, service, administrative or other processes used that would enhance the proposed contract.

10.2 The Tenderer may suggest and where suggested shall provide a description of the suggested improvements to the technical aspects of the goods that would enhance value to the proposed contract.

10.3 The Tenderer may list any alternative methods, procedures, features, terms, etc., that may be of interest to KPLC.

11. **Amendments to the detailed technical specifications**

The Tenderer shall provide its proposed method of accommodating future amendments to the Technical Requirements and the sharing of any resulting benefits with KPLC.

12. **Standards**

Notwithstanding anything contained in the tender document and proposed contract, at all times every item shall be manufactured to comply with the standards specified in the tender document. This shall mean the current or prevailing standards of those specified as at the date of manufacture. For the avoidance of doubt, the standards used must be current at the date of manufacture.

PART B – DETAILED TECHNICAL SPECIFICATIONS (DTS)

The Detailed Technical Specifications are as attached on the next page.

Table 2.1 **Advanced Endpoint Protection**

Index	Advanced Endpoint Protection (3000 Endpoints)	Compliance (Full, Partial, Not Complied)	Respons e
1.1	***Advanced Endpoint Threat Protection Requirements:***		
1	The proposed solution must support Windows, Mac OS and Linux Operating Systems		
2	Must support Antimalware and Web Reputation		
3	The proposed solution must have a recommendation on the NSS Labs 2018 Advanced Endpoint Protection (AEP) test and ICSA 2018 Advanced Threat Defense certification		
4	Deliver the systems with latest Antimalware protection technology to meet its existing and future requirements.		
5	Delivers an anti-malware agent to extend protection to the endpoint clients		
6	Must support real-time scanning capabilities, on-demand and scheduled scan capabilities		
7	Must protect against sophisticated attacks in endpoints by isolating malware from critical operating system and security components		
8	Must integrate with global threat intelligence network for web reputation capabilities that strengthen protection for endpoints from a single console		
9	Must provide real-time and On-Demand Scanning of the endpoints		
10	Must provide Exploit Prevention to all endpoints		
11	Must support behavioral Monitoring, Process Memory Scanning and Registry Scan for Windows Servers and endpoints		
12	Must support behavioral analysis to detect unknown malware like ransom ware		
13	Must support the detection for Viruses, Spywares, Trojans		
14	The detection must rely not only conventional signatures, rather on reputation and multiple detections technologies as well		
15	The solution must support sandbox integration with Deep Discovery Custom Sandbox		
16	The proposed sandbox solution must allow for custom VMs.		
17	The sandboxing solution must support pre-Execution & Run-time Predictive Machine Learning		
18	The solution must support scans on computers/Servers to identify known vulnerabilities (Scheduled or On-Demand)		
19	The solution must provide increased visibility and control over applications accessing the network		
20	The solution must have a built-in reporting and logging capabilities		

21	The system manager (Management Console) must support deployment in a Microsoft Windows environment providing an Interactive dashboard		
22	The solution must support the ability to automate the scanning for all protection layers		
23	The solution must support zero-day ransomware detection and prevention		
24	The system must generate events when application control detects new or changed software on the file system, and each time that software tries to execute		
25	The solution must progressively filter out threats using the most efficient techniques for maximum detection without false positives.		
26	The solution must blend signature-less techniques including machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking.		
27	The solution must be lightweight and optimized security that uses the right detection technique at the right time to ensure minimal impact on devices and networks.		
28	The solution must have a comprehensive central view of user security that lets user quickly and efficiently analyze data and threats across the whole solution.		
29	The solution must have user-centric visibility to allow easy understanding of how threats are affecting a particular user across multiple systems.		
30	The solution must allow automatic sharing of threat intelligence across security layers so as to enable protection from emerging threats across the whole organization.		
31	The solution must block zero-day malware with signature-less techniques		
32	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.		
33	The proposed sandboxing 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 and .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip to prevent advanced Malware and Zero-day attacks.		

34	The sandbox must be deployed in high availability i.e. load balance file submissions and analysis between two appliances		
35	The sandbox must support on-demand file submission		
36	The sandbox must support Windows client and server, MacOS and Android Oses		
37	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.		
38	The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration		
39	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.		
40	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.		
41	The solution Must support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions		
42	The solution Must be based on algorithm, which Must be able to detect maximum Malware or rogue elements with each signature.		
43	The solution Must have ability to block all outbound call- back communication initiated by the internal clients (infected)		

Table 2.2 **Email Security Gateway**

Index	Email Security Gateway (2 Units)	Compliance (Full, Partial, Not Complied)	Response
1.1	***General Requirements:***		
1	The solution Must Enforce email and security policies at a granular level		
2	Must be VBSpam+, NSS Labs and ICSA Labs Certified		
3	The solution Must support three modes of operations Gateway, Transparent and server modes		
4	The solution must be with no per user/mailbox license		
5	The solution must integrate with the proposed internet perimeter firewall as part of a security fabric to share security intelligence including dynamic blacklists		
1.2	***Technical Requirements:***		
1	Must support a minimum of 4xGE RJ45 ports		
2	Must support at least RAID 1, 5, 10 options		
3	Must support at least 800 configurable Email domains		
4	The solution must support unlimited mailboxes in gateway mode		
5	The solution must support at least 2x 2 TB storage		
6	The solution must at least 1 Million message per hour as a mail relay(Email routing) [Without queuing based on 100 KB message size].		
7	The solution must support dual power supplies		
1.3	***Mail Gateway Features Requirement:***		
1	The proposed system must support high availability (HA) features:		
a	Active-Passive Mode		
b	Configuration Synchronization Mode (Configuration Master and Slave Mode)		
c	Quarantine and Mail Queue Synchronization		
d	Device Failure Detection and Notification		
e	Link Status, Failover and Redundant Interface Support		
2	The proposed systems shall provide the following denial-of-service protection:		

a	Inbound and Outbound Message Rate Limiting		
b	Recipient Address Attack		
c	Reverse DNS Check (Anti-Spoofing)		
d	Forged Sender Address		
3	The proposed system shall provide the following logging and reporting capabilities:		
a	Configuration Change and Management		
b	Event Logging		
c	Built-in Reporting module		
d	Centralized logging and reporting		
e	Centralized Quarantine		
f	SNMP Support using Standard and Private MIB with Threshold-Based Traps		
1.4	***Mail Antispam Solution***		
1	Must support the following protocols:-		
a	The solution Must support SMTP control at all stages of Email processing starting from Session initiation stage till Body transmission stage (URIs & HASH checks, heuristic rules, spam attachment, spam images, viruses, malware)		
b	The solution Must support different actions on spam detection including inserting new header, Delivering to alternate host, archiving, Quarantine, discarding the email silently		
c	The solution Must be able to scan email header, body, and attachments (including compressed files) for virus infections.		
d	The solution Must support different actions on Virus detection including inserting new header, Delivering to alternate host, Quarantine, discarding the email silently.		
e	The solution Must be able to control email based upon its subject line, message body, and attachments to be able to restrict prohibited content, such as words or phrases, file names, and file attachments that are not permitted.		
2	The solution Must support different actions for content control including inserting new header, Delivering to alternate host, Quarantine, Archiving, discarding the email silently and content disarm and neutralization		

3	The solution Must be able to locally compute a score for every source IP address Based on traffic quality observed for that IP Taking into account amount of virus, spam and harm email {Local IP reputation Must be able to work regardless of address type (Public or Private IP)}		
4	The solution Must support Grey listing for IPv4, IPv6 addresses and email accounts		
5	The solution Must support on box archiving		
6	The solution Must support Identity-Based Encryption in both push and pull methods with no additional hardware or software to install and no user provisioning, with no additional licenses		
7	The solution Must support Data Leak Prevention, and Policy-Based Encryption and Archiving enable compliance with SOX, GLBA, HIPAA, PCI DSS		
8	The solution Must Enforce email and security policies at a granular level		
1.5	**Mail Anti Malware Solution**		
1	Must support Antivirus detection		
2	Must support Virus Outbreak protection		
3	Must support Heuristic-based behavioral detection		
4	Must support Real-time malware outbreak detection		
5	Must support Cloud and On-premise sandbox integration		
6	Must support Password protected archive and PDF decryption		
7	Must support Active content detection and removal (PDF & Office Documents)		
8	Must support Email Threat Neutralization		
9	Must support Rescan for threats on quarantine release		
10	Must support URL Click Protect to rewrite URLs and rescan on access		
11	Must support Impersonation Analysis		

Table 2.3 **Network Access Control (NAC)**

Index	***NAC Solution (2 Units supporting 5000 users each))***	***Compliance (Full, Partial, Not Complied***	***Response***
1.1	***General Requirements:***		
1	Must be supplied as virtual appliances		
2	Must support agentless scanning of network for detection and classification of devices		
3	Must create an inventory of all devices on the network		
4	Must support event reporting to SIEM with detailed contextual data to reduce investigation time		
5	Must assess risk of every endpoint on the network		
6	Must support perpetual licensing model		
7	Must automate onboarding process for large number of endpoints, users and guests		
8	Must enforce dynamic network access control and enable network segmentation		
9	Must reduce containment time from days to seconds		
10	Must support multiple canned reports for network reporting, compliance, and analysis		
11	Must form a security fabric with the proposed firewalls for automated quarantine of infected hosts		

1.2	***Technical Requirements:***		
1	The solution must support major hypervisors including VMWare and Hyper-V		
2	Must be able to scale to 15,000 concurrent users per VM		
3	Must be licensed with at least 5000 concurrent user/device licenses		
4	Must support at least 12GB RAM		
5	Must support at least 1TB of attached storage		
6	The proposed VM appliances must be deployed in high availability for high availability		
7	The proposed VM appliances must be deployed centrally in the datacenter without any requirement of having different appliances across branch sites		
3	***Licensing Requirements:***		
1	Visibility:		
i	Must support Network Discovery		
ii	Must support both agentless and persistent agent deployments		

iii	Must support User and Device Domain Authorization		
iv	Must support User and Device Captive Portals		
v	Must support Rogue Endpoint Identification		
vi	Must support Device Profiling and Classification		
vii	Must support MDM Integration		
2	Automation / Control		
i	Must support Network Access Policies		
ii	Must support BYOD Onboarding		
iii	Must support Advanced Guest Management		
iv	Must support IoT Onboarding with Sponsor authorization		
v	Must support Endpoint Compliance		
vi	Must support automated Rogue Device Detection & Restriction		
vii	Must support Web & Firewall Single Sign On		
viii	Must support Firewall Segmentation		
3	Incident Response		
i	Must support Event Correlation		
ii	Must support Extensible Actions & Audit Trail		
iii	Must support Alert Criticality & Routing		
iv	Must support Guided Triage Workflows		
4	Integrations		
i	Must support Inbound Security Events		
ii	Must support Outbound Security Events		
iii	Must support REST API		
5	Reporting		
i	Must support live reporting		
ii	Must support historical analysis		
4	***System Features:***		
1	Must support Role-Based-Access-Control.		
2	The solution must support secure management protocols (e.g. HTTPS, SSH)		
3	The solution must support advanced auditing capabilities		
4	Processes running on the device or operating system		
5	The solution must provide e-mail alerting for administrative alerts		
6	The solution must support configuration backup/restore		
7	The solution must support common external authentication mechanisms for administrators (e.g. LDAP, AD, RADIUS, etc.)		

5	***Policy Requirements:***		
1	The solution must be able to classify assets on the network based on categories (e.g. Windows, Linux, Mobile, etc.)		
2	The solution must collect detailed asset information (e.g. MAC address, Logged on user, OS, NIC vendor, Switch Port, etc.)		
3	The solution must be able to prevent network access from unauthorized and/or non-compliant devices (eg: BYOD device, device without Anti-Virus running)		
4	The solution must provide captive portal abilities for guest device self-registration		
5	The solution must provide captive portal abilities for BYOD devices via corporate logon credentials (e.g. AD, LDAP)		
6	The solution must be able to detect/prevent ARP spoofing		
7	The solution must be able to detect/prevent device dual-homing (e.g. wired + wireless access)		
8	The solution must be able to detect/prevent malicious hosts		
9	The solution must be able to detect Windows Update compliance		
10	The solution must be able to detect Anti-Virus Update compliance		
11	The solution must be able to detect endpoint firewall compliance		
12	The solution must be able to detect/prevent external storage media & peripherals (e.g. USB flash drives, webcams, etc.)		
13	The solution must be able to detect custom attributes of devices (e.g. script output, WMI, registry, file attributes, running processes, etc.)		
14	The solution must be able to quarantine devices based on policy (e.g. Switch port block, virtual firewall)		
15	The solution must support administrative reversal of policy actions (e.g. un-quarantine device)		
16	The solution must support manual administrative actions (e.g. quarantine device, re-evaluate policies, etc.)		
6	***Mandatory Integration Requirements:***		
1	The solution must integrate with common router/switch vendors (e.g. Cisco, Brocade etc)		
2	The solution must integrate with common AV/EDR vendors (e.g. Sophos, Crowd-strike, Carbon Black etc)		
3	The solution must integrate with common firewall vendors (e.g. Palo Alto, Fortinet, Check Point etc)		

4	The solution must integrate with common Anti-malware vendors (e.g. FireEye)		
5	The solution must integrate with common WiFi vendors (e.g. Cisco, Meru Networks, Aruba)		
6	The solution must integrate with common mobile device management (MDM) vendors (e.g. Air watch, Mobile Iron, Citrix etc)		
7	The solution must integrate with common vulnerability assessment vendors (e.g. Qualys, Rapid7 etc)		
7	***Mandatory Reporting Requirements:***		
1	The solution must include pre-built report templates (e.g.: device policy compliance)		
2	The solution must support custom reports		
3	The solution must support scheduled reports		

Table 2.4 **Wireless Controller & Wireless Access Points**

Index	Wireless Access Points (40 Units)	Compliance (Full, Partial, Not Complied)	Response
1.1	***General Requirements:***		
1	Must support the latest 802.11ac (WAVE 2) technology with association rate of more than 1.5 Gbps		
2	Must leverage the proposed firewall platforms as controllers for low TCO		
3	Integration with centralized management and reporting solutions		
4	Fast Roaming for uninterrupted data access.		
5	Automatic Radio Resource Provisioning (ARRP) for optimized throughput.		
6	Layer 7 application control prioritizes business traffic.		
7	Rogue AP detection and mitigation to satisfy PCI DSS compliance		
1.2	***Technical Requirements:***		
1	Should be a high density high performance indoor access point		
2	Should support dual wireless radios		
3	Should support 8 Internal wireless and 1 Bluetooth antennas		
4	Should support 2xGE RJ45 port		
5	Should support 802.3at PoE		
6	Should support a throughput of at least 600Mbps on Radio 1 @ 2.4 GHz, b/g/n and 2000 Mbps on Radio 2 @ GHz, a/n/ac		
7	Should support 4x4 MIMO 4 spatial stream		
8	Ceiling, T-Rail and/or Wall mount kit should be included		
1.3	***Other Specifications***		
1	WiFi Alliance Certified		
2	The solution must support EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST		
3	The solution must support WPA™ and WPA2™ with 802.1x or Pre-shared key, WEP and Web Captive Portal, MAC blacklist & whitelist		

4	The solution must support max transmit power of 2.4 GHz: 28 dBm / 631 mW (4 chains combined)* 5 GHz: 26 dBm / 398mW (4 chains combined)*		
5	The solution must support 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11n, 802.1x, 802.3af, 802.11ac, 802.3at, 802.3az, 802.3ad IEEE standards		
6	The solution must support Transmit Beam Forming (TxBF)		
7	The solution must support Low-Density Parity Check (LDPC) Encoding		
8	The solution must support Maximum Likelihood Demodulation (MLD)		
9	The solution must support Maximum Ratio Combining (MRC)		
10	The solution must support A-MPDU and A-MSDU Packet Aggregation		
11	The solution must support MIMO Power Save		
12	The solution must support Short Guard Interval		
13	The solution must support WME Multimedia Extensions including 4 priority queues for voice, video, data and background traffic		

Table 2.5 **Branch Software Defined (SD) WAN Firewalls**

Index	Branch Software Defined (SD-WAN Firewalls (2 Units)	Compliance (Full, Partial, Not Complied)	Response
1.1	***General Requirements:***		
1	The solution must be appliance based and Must facilitate multi-application environment.		
2	Must be a leader in both Gartner UTM and Enterprise Firewall Quadrants		
3	The platform must use a security-hardened, purpose-built operating system, and Must support the deployment option in NGFW and UTM mode.		
4	The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
5	Licensing: Must be per device license for unlimited users for Firewall and other features. There Must not have any user/IP/host based licenses .		
6	The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
	Each Virtual Domain Must be allowed to connect to Specific 3rd Party Authentication service, AD, Radius, Tacacs or other…		
	Must support more than one ISP with automatic ISP failover		
7	Must have support for Explicit Proxy and Transparent Proxy		
8	Must form the heart of the security fabric by integrating networking and security solutions and 3rd party solutions		
9	Must have security fabric 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		
1.2	***Mandatory Requirements:***		
1	Must support a minimum of 12 x GE RJ45 PoE+ ports		
2	Must support at least 1 Million Maximum Concurrent Sessions		
3	Must support at least 30,000 New Sessions/Second		
4	Must support at least 4Gbps of firewall throughput		

5	Must support at least 450 Mbps Enterprise/Production IPS Throughput		
6	Must support at least 250 Mbps Enterprise/Production Threat Protection Throughput		
7	Must support at least 128GB SSD storage		
8	Must support at least 200 SSL VPN licenses		
9	Must support at least 900Mbps of CAPWAP throughput		
10	Must have the following licenses included Application Control, IPS, AV, Web Filtering and Sandbox		

1.3	***Firewall Features Requirement:***		
1	The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified, if not the same model		
2	It Must be possible to operate the firewall in "bridge mode" or "transparent mode" apart from the standard NAT mode		
3	The Firewall must provide NAT functionality, including PAT.		
4	Must support "Policy-based NAT"		
5	The Firewall Must provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP		
6	Firewall Must support Voice based protocols like H.323, SIP, SCCP, MGCP etc and RTP Pin holing.		
7	The Firewall Must support User-Group based Authentication (Identity based Firewalling) & Scheduling		
8	IPv6 support for both NAT and Transparent Mode		
1.4	***Authentication Requirements:***		
1	Support for authentication at the firewall policy level (Local and Remote)		
2	Support for RSA Secure ID or other Token based products		
3	Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication		
4	Support for Native Windows Active Directory		
5	Must support authentication based on LDAP Groups		
6	Must support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators		

1.5	***Encryption / VPN Requirements***		
1	The VPN Must be integrated with firewall and Must be ICSA Labs certified for both IPSec and SSL-TLS		
	Must support the following protocols:-		
a	DES & 3DES		
b	MD5, SHA-1 & the more secure SHA-256 authentication		
c	Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.		
d	Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm		
e	The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)		
2	Must support Hub and Spoke VPN topology		
3	IPSec NAT Traversal & Dead Peer Detection Must be supported		
4	IPSec VPN Must support XAuth over RADIUS and RSA SecurID or similar product.		
5	Must have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy		
6	Must support SSL Two-factor Authentication with Digital Certificates		
7	Must support Single Sign-On Bookmarks for SSL Web VPN		
8	Must support Windows, Linux and MAC OS for SSL-VPN (Must have always-on clients for these OS apart from browser based access)		
9	Must support NAT within IPSec/SSL VPN tunnels		
10	Must also support PPTP and L2TP over IPSec VPN protocols.		
1.6	***High Availability Requirements:***		
1	The device must support Active-Active as well as Active-Passive redundancy.		
2	The Firewall must support stateful failover for both Firewall and VPN sessions.		
3	The HA Architecture Must have the ability for Device Failure Detection and Notification as well as Link Status Monitor		
4	Must support VRRP and Link Failure Control		

1.7	***Data Center Optimization:***		
1	Must support Server Load Balancing with features like HTTP persistence		
2	Must support TCP Multiplexing		
3	Must support HTTPS Offloading with flexible Digital Certificate Management		
4	Must have support for WCCP and ICAP protocols		
1.8	***Administration/ Management Requirements:***		
1	The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management		
2	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)		
3	There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)		
4	The device Must have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).		
5	Provision to generate automatic notification of events via mails / syslog		
6	Provision to send alerts to multiple email recipients		
7	Support for role based administration of firewall		
8	Must support simultaneous login of Multiple Administrators.		
9	Must have provision to customize the dashboard (eg: by selecting suitable Widgets)		
10	The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP		
11	Support for Image upgrade via FTP, TFTP and WebUI		
12	Must support system software rollback to the previous version after upgrade		
1.9	***Network IPS:***		
1	Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.		
2	Must have a built-in Signature and Anomaly based IPS engine on the same unit		
3	Must have protection for 3000+ signatures		
4	Able to prevent denial of service and Distributed Denial of Service attacks.		

5	Must be able to exclude certain hosts from scanning of particular signatures		
6	Supports CVE-cross referencing of threats where applicable.		
7	Must provide the facility to configure Profile based sensors (Client/Server) for ease of deployment		
8	Must support granular tuning with option to configure Overrides for individual signatures.		
9	Supports automatic Attack database updates directly over the internet. (i.e. no dependency on any intermediate device)		
10	Supports attack recognition inside IPv6 encapsulated packets.		
11	Supports user-defined signatures (i.e. Custom Signatures) with Regular Expressions.		
12	Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options		
13	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		
14	Must Identify and control over 1000+ applications (i.e. Application control feature)		
15	Must perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc		
16	Must control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc		
1.1	***Gateway Antivirus***		
1	The appliance Must facilitate embedded anti-virus support which is ICSA Labs certified		
2	Must include Antispyware and Worm Prevention		
3	Must have option to schedule automatic updates of the new virus pattern.		
4	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		
5	Must have configurable policy options to select what traffic to scan for viruses		
6	Must have option to configure to respond to virus detection at the gateway in several ways ie. Delete the file, Alert email, Quarantine etc		

7	Must have options to prevent user downloads based on file extension as well as file type		
8	Must have support for “Flow-Based Antivirus Scanning Mode” for high throughput requirements		
9	The solution Must be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
10	Must have an ability of Antivirus scanning for IPv6 traffic		
1.11	***Advanced Threat Protection***		
1	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.		
2	The solution must have multi-layer of detection process with the malicious code emulation and execution in the VM environment.		
3	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.		
4	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.		
5	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.		
6	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.		
7	The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration		
8	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.		
9	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.		
10	The solution Must support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions		
11	The solution Must be based on algorithm, which Must be able to detect maximum Malware or rogue elements with each signature.		
12	The solution Must have ability to block all outbound call- back communication initiated by the internal clients (infected)		
1.12	***Web Content Filtering***		
1	The appliance Must facilitate embedded Web Content Filtering feature		
2	Web content filtering solution Must work independently without the need to integrate with External proxy server.		
3	Must have facility to block URL' based on categories. Must support HTTP and HTTPS based traffic.		
4	URL database Must have more than 2 billion URLs under 70+ categories.		
5	Must be able to block different categories/sites based on User Authentication.		
6	Must have configurable parameters to block/allow unrated sites. Must have option to locally rate sites.		
7	Must have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable		
8	Must have options to customize the “Blocked Webpage Message” information displayed to end users		
9	Must have facility to schedule the configurations so that non-work related sites are blocked during office hrs and allow access to all sites except harmful sites during non office hrs. Must also have time-based quota		
10	The solution Must have options to block java applets, ActiveX as well as cookies		

11	The solution Must be able to block URLs hosting spywares / adwares etc.		
12	Must have configurable policy options to define the URL exempt list		
1.13	***Anti-Spam***		
1	Must have integrated support for Anti-Spam for the following protocols: SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS		
2	Anti-Spam database Must have updates for Real-Time Blacklist and Open Relay Database Servers		
3	Automatic Real-Time Updates of Anti-Spam database		
4	Must perform MIME Header Check		
5	Must have facility for Keyword/Phrase Filtering		
6	Must be configurable for IP Address Blacklist and Exempt List		
1.14	***SD-WAN***		
1	Must support WAN load balancing (weighted) algorithms by volume, sessions, source-destination IP, Source IP, and spillover		
2	Must support multi-path intelligence using rules defined by:		
	Source address and/or user group		
	Destination address and/or a selection of over 3,000 applications		
	Path selection using particular link quality criteria or SLAs defined		
3	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		
4	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		
5	Must support traffic shaping policies that assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.		
6	Must support DSCP match in SD-WAN rules		
7	Must support inline and out-of-path WAN optimization topology, peer to peer, and remote client support		

8	Must support at least CIFS, FTP, HTTP(S), MAPI and TCP WAN optimization protocols		
9	Must support multiple WAN optimization sessions on the same tunnel		
10	Must support zero-touch deployment		
1.15	***Certifications***		
1	Must have support for the following certifications:		
a	FIPS-140-2 for Client VPN software		
b	OS Must be “IPv6 Phase II Ready” certified		

Table 2.6 **Central Logging & Reporting Appliance /Server**

Index	Central Logging & Reporting Appliance/Server (1)	Compliance (Full, Partial, Not Complied)	Response
1.1	*General Requirements:*		
1	Must support integrated logging, and tighter integration & correlation of events & policies		
2	Must support automated Indicators of Compromise (IOC)		
3	Must Support role based administrator		
4	Must support Network Operation Center (NOC) and Security Operation Center (SOC) functionality		
5	Must support syslog or CEF log forwarding for third-party solution integration		
6	Support full Graphic summary reports, providing network wide reporting of events, activities, and trends		
7	Must have Built in report templates		
8	Allow Comprehensive alert builders		
9	Simple and intuitive Google-like search experience and reports on network traffic, threats, network activities and trends across the network.		
1.2	*Mandatory Requirements:*		
1	Must be a hardware appliance or One Server with Virtual Machines capability.		
2	Must support at least 25,000 Maximum Indexed/Analysed Logs/Sec		
3	Must support at least 400GB/Day of Logs		
5	Must support at least 16 TB of storage capacity configurable in at least RAID 5/10 levels		
1.3	*Use of Virtual Machines & Virtual Servers for Multiple Logging Incidences of Dissimilar Equipment*		
1	Where more than one manufacture of devices is to be logged or used in the tender, the server shall have the necessary software to receive logs from different manufacturers. In this case a virtual machine or virtual server can be created per each logged entity for compatibility purposes where necessary.		
2	All logging shall be available in a common final format as in templates in part 1.1 of this table. A common navigator such as web tool will be used to show how and where logs from different manufacturers are accessed.		
3	The number of Virtual Machines to be created for purposes of interoperability shall be known in this tender.		

Table 2.7 **Central Management Appliance**

Index	Central Management Appliance/Server (1 Unit)	Compliance (Full, Partial, Not Complied)	Response
1.1	*General Requirements:*		
1a	Must be a hardware appliance or One Server with Virtual Machines capability.		
1b	Must support centralized management of the proposed firewall appliances		
2	Must support centralized software upgrades and security updates for the managed devices		
3	Must support Hierarchical Objects Database, reuse of common configurations		
4	Must support automated device discovery support and maintain policies on same device types		
5	Must support granular device and role based administration for large enterprises and multi-tenancy deployments		
6	Must support workflow integration for change control management		
7	Must support detailed revision tracking, and thorough auditing capabilities		
8	Must support centralized SD-WAN provisioning and monitoring		
9	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		
1.2	*Mandatory Requirements:*		
1	Must be able to support at least 10 devices with the provision of device scaling with additional licenses		
1.3	*Use of Virtual Machines & Virtual Servers for Multiple Network Management Incidences of Dissimilar Equipment*		
1	Where more than one manufacture of dissimilar devices is to be managed or used in the tender, the server shall have the necessary software to manage devices from more than one manufacturers. In this case a virtual machine or virtual server can be created		

	per each managed entity for compatibility purposes where necessary.		
2	All managed instances shall be available in a common final webpage as in part 1.1 of this table. A common navigator such as web tool will be used to show how devices from different manufacturers are accessed and managed..		
3	The number of Virtual Machines to be created for purposes of interoperability shall be known in this tender.		

Table 2.8 **Application and Global Load Balancers**

Index	Application and Global Load Balancers (2 Units)	Compliance (Full, Partial, Not Complied)	Response
1.1	***General Requirements:***		
1	The Must be appliance based		
2	Must support comprehensive server load balancing for 99.999% application uptime		
3	The platform must use a security-hardened, purpose-built operating system, and Must support NAT, Transparent, proxy, Active/Active and Active/Passive deployment modes		
4	The platform should use hardware acceleration for SSL offloading and Forward Proxy		
5	Licensing: The appliances should include Global Server Load Balancing, Link Load Balancing and L4 & L7 load balancing without additional licenses		
1.2	***Technical Requirements:***		
1	Must support at least 8x GE RJ45 interfaces		
2	Must support at least 8xGE SFP interfaces		
3	Must support at least 4x10G BASE-SR SFP+ slots with 2 10GE SR SFP+ modules		
4	Must support an ASIC based SSL Acceleration Technology		
5	Must support L4 Throughput of at least 20Gbps		
6	Must support L7 Throughput of at least 15Gbps		
7	Must support at least 500,000 L7 RPS		
8	Must support at least 2,500,000 DNS QPS		
9	Must support a Compression Throughput of at least 12Gbps		
10	Must support at least 20,000 SSL CPS 2048 Key		
11	Must support at least 45 Virtual Instances		
12	Must support Dual Power Supplies		
1.3	***System Features Requirement:***		
1	Must support simple management access i.e. without the need for local management clients (HTTPS preferred)		
2	Must support high availability		

3	Must support CLI Interface for configuration and monitoring		
4	Must support secure SSH remote network management		
5	Must support secure Web UI access		
6	Must support RESTful API		
7	Must support SNMP with private MIBs with threshold-based traps		
8	Must support Real-time Data Analytics		
9	Must support Syslog support		
10	Must support role-based administration		
11	Must support in-build diagnostic utilities		
12	Must support real-time monitoring graphs		
13	Must support built-in reporting		
14	Must support getting Started wizard for first-time login		
15	Must support Virtual Domains (VDOMs)		
16	Must support BGP and OSPF Support		
17	Must support IPv6 Support		
18	Must support IPv6 routing		
19	Must support IPv6 firewall rules		
1.4	***L4 and L7 Application Load Balancing Requirement:***		
1	Must support virtual service definition with inherited persistence, load balancing method and pool members		
2	Must support static, default and backup policies and groups		
3	Must support Layer 4/7 application routing policy		
4	Must support Layer 4/7 server persistence		
5	Must support Application load balancing based on round robin, weighted round robin, least connections, shortest response		
6	Must support granular real server control including warm up rate limiting and maintenance mode with session ramp down		
7	Must support custom Scripting for SLB and Content Rewriting		
8	Must support Application Templates for Microsoft Applications including SharePoint, Exchange and Windows Remote Desktop		
9	Must support L4 dynamic load balancing based on server parameters(CPU, Memory and disk)		
10	Must support L4 Persistent IP, has IP/port, hash header, persistent cookie, hash cookie, destination IP hash, URI hash, full URI hash, host hash, host domain hash		

11	Must support Layer 7 Application Load Balancing		
12	Must support HTTP, HTTPS, HTTP 2.0 GW, FTP, SIP, RDP, RADIUS, MySQL, RTMP, RTSP		
13	Must support L7 content switching		
14	HTTP Host, HTTP Request URL, HTTP Referrer		
15	Source IP Address		
16	Must support URL Redirect, HTTP request/response rewrite (includes HTTP body)		
17	Must support Layer 7 DNS load balancing, security, and caching		
18	Must support 403 Forbidden Rewrite		
19	Must support Content rewriting		
1.6	***Global Server Load Balancing Requirement:***		
1	Must support load balancing of servers between different Data Centres, at Primary and DR sites		
2	Must support dynamic proximity		
3	Must support inbound Link Load Balancing		
4	Must support Global data center DNS-based failover of web applications		
5	Must deliver local and global load balancing between multi-site SSL VPN deployments		
6	Must support DNSSEC		
7	Must support DNS Access Control Lists		
1.7	***High Availability Requirement:***		
1	Solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Stateful session failover with Active-active & active standby unit redundancy mode.		
2	Must support communication link for real-time configuration synchronization		
3	Must support built in failover decision/health check conditions		
4	Must support configuration synchronization at boot time and during run time to keep consistence configuration on both units.		
1.8	***Application Acceleration Requirement:***		
1	Must support HTTPS and TCPS processing offload		
2	Must support full certificate management features		

3	Must support SSL Forward Proxy for secure traffic inspection		
4	Must support HTTP/S Mirroring for traffic analysis and reporting		
5	Must support 100x acceleration by off-loading TCP processing		
6	Must support connection pooling and multiplexing for HTTP and HTTPS		
7	Must support HTTP Page Speed-UP for Web Server Optimization and Acceleration		
8	Must support TCP buffering		
9	Must support HTTP Compression and Decompression		
10	Must support HTTP Caching (static and dynamic objects)		
11	Support bandwidth allocation with Quality of Service (QoS)		
12	Must support HTTP and Layer 4 Rate Limiting		
13	Must support the following authentication offloading methods:		
	Local		
	LDAP		
	RADIUS		
	Kerberos		
	SAML 2.0 (SP & Idp)		

Table 2.9 **Internet Edge Firewalls**

Index	Internet Edge Firewalls (Pri & DR sites) (4 Units)	Compliance (Full, Partial, Not Complied)	Response
1.1	***General Requirements:***		
1	The solution must be appliance based and Must facilitate multi-application environment.		
2	Must be a leader in Enterprise Firewall Quadrant		
3	The platform must use a security-hardened, purpose-built operating system, and Must support the deployment option in NGFW mode.		
4	The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
5	Licensing: Must be per device license for unlimited users for Firewall and other features. There Must not have any user/IP/host based licenses .		
6	The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
	Each Virtual Domain Must be allowed to connect to Specific 3rd Party Authentication service, AD, Radius, Tacacs or other…		
	Must support more than one ISP with automatic ISP failover		
7	Must have support for Explicit Proxy and Transparent Proxy		
8	Must form the heart of the security fabric by integrating networking and security solutions and 3rd party solutions		
9	Must have security fabric 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		
1.2	***Mandatory Requirements:***		
1	Must support a minimum of 8 x 10GE SFP+ Slots populated with at least 6 10G SFP+ SR modules		
2	Must support at least 10 Million Maximum Concurrent Sessions		
3	Must support at least 300,000 New Sessions/Second		
4	Must support at least 50Gbps of firewall throughput		

5	Must support at least 12 Gbps Enterprise/Production IPS Throughput		
6	Must support at least 5 Gbps Enterprise/Production Threat Protection Throughput		
7	Must support at least 480GB SSD storage		
8	Must support at least 1000 SSL VPN licenses		
9	Must support at least 20Gbps of CAPWAP throughput		
10	Must have the following licenses included Application Control, IPS, AV, Web Filtering and Sandbox		

1.3	***Firewall Features Requirement:***		
1	The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified, if not the same model		
2	It Must be possible to operate the firewall in "bridge mode" or "transparent mode" apart from the standard NAT mode		
3	The Firewall must provide NAT functionality, including PAT.		
4	Must support "Policy-based NAT"		
5	The Firewall Must provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP		
6	Firewall Must support Voice based protocols like H.323, SIP, SCCP, MGCP etc and RTP Pin holing.		
7	The Firewall Must support User-Group based Authentication (Identity based Firewalling) & Scheduling		
8	IPv6 support for both NAT and Transparent Mode		
1.4	***Authentication Requirements:***		
1	Support for authentication at the firewall policy level (Local and Remote)		
2	Support for RSA SecureID or other Token based products		
3	Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication		
4	Support for Native Windows Active Directory		
5	Must support authentication based on LDAP Groups		
6	Must support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators		

1.5	***Encryption / VPN Requirements***		
1	The VPN Must be integrated with firewall and Must be ICSA Labs certified for both IPSec and SSL-TLS		
	Must support the following protocols:-		
a	DES & 3DES		
b	MD5, SHA-1 & the more secure SHA-256 authentication		
c	Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.		
d	Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm		
e	The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)		
2	Must support Hub and Spoke VPN topology		
3	IPSec NAT Traversal & Dead Peer Detection Must be supported		
4	IPSec VPN Must support XAuth over RADIUS and RSA SecurID or similar product.		
5	Must have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy		
6	Must support SSL Two-factor Authentication with Digital Certificates		
7	Must support Single Sign-On Bookmarks for SSL Web VPN		
8	Must support Windows, Linux and MAC OS for SSL-VPN (Must have always-on clients for these OS apart from browser based access)		
9	Must support NAT within IPSec/SSL VPN tunnels		
10	Must also support PPTP and L2TP over IPSec VPN protocols.		

1.6	***High Availability Requirements:***		
1	The device must support Active-Active as well as Active-Passive redundancy.		
2	The Firewall must support stateful failover for both Firewall and VPN sessions.		
3	The HA Architecture Must have the ability for Device Failure Detection and Notification as well as Link Status Monitor		
4	Must support VRRP and Link Failure Control		
1.7	***DataCenter Optimization:***		

1	Must support Server Load Balancing with features like HTTP persistence		
2	Must support TCP Multiplexing		
3	Must support HTTPS Offloading with flexible Digital Certificate Management		
4	Must have support for WCCP and ICAP protocols		
1.8	***Administration/ Management Requirements:***		
1	The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management		
2	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)		
3	There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)		
4	The device Must have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).		
5	Provision to generate automatic notification of events via mails / syslog		
6	Provision to send alerts to multiple email recipients		
7	Support for role based administration of firewall		
8	Must support simultaneous login of Multiple Administrators.		
9	Must have provision to customize the dashboard (eg: by selecting suitable Widgets)		
10	The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP		
11	Support for Image upgrade via FTP, TFTP and WebUI		
12	Must support system software rollback to the previous version after upgrade		
1.9	***Network IPS:***		
1	Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.		
2	Must have a built-in Signature and Anomaly based IPS engine on the same unit		
3	Must have protection for 3000+ signatures		
4	Able to prevent denial of service and Distributed Denial of Service attacks.		
5	Must be able to exclude certain hosts from scanning of particular signatures		

6	Supports CVE-cross referencing of threats where applicable.		
7	Must provide the facility to configure Profile based sensors (Client/Server) for ease of deployment		
8	Must support granular tuning with option to configure Overrides for individual signatures.		
9	Supports automatic Attack database updates directly over the internet. (i.e. no dependency on any intermediate device)		
10	Supports attack recognition inside IPv6 encapsulated packets.		
11	Supports user-defined signatures (i.e. Custom Signatures) with Regular Expressions.		
12	Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options		
13	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		
14	Must Identify and control over 1000+ applications (i.e. Application control feature)		
15	Must perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc		
16	Must control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc		
1.10	***Gateway Antivirus***		
1	The appliance Must facilitate embedded anti virus support which is ICSA Labs certified		
2	Must include Antispyware and Worm Prevention		
3	Must have option to schedule automatic updates of the new virus pattern.		
4	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		
5	Must have configurable policy options to select what traffic to scan for viruses		
6	Must have option to configure to respond to virus detection at the gateway in several ways ie. Delete the file, Alert email, Quarantine etc		
7	Must have options to prevent user downloads based on file extension as well as file type		

8	Must have support for “Flow-Based Antivirus Scanning Mode” for high throughput requirements		
9	The solution Must be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
10	Must have an ability of Antivirus scanning for IPv6 traffic		

1.11	***Advanced Threat Protection***		
1	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.		
2	The solution Must have multi-layer of detection process with the malicious code emulation and execution in the VM environment.		
3	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.		
4	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.		
5	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.		
6	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.		
7	The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration		
8	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.		

9	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.		
10	The solution Must support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions		
11	The solution Must be based on algorithm, which Must be able to detect maximum Malware or rogue elements with each signature.		
12	The solution Must have ability to block all outbound call- back communication initiated by the internal clients (infected)		
1.12	***Web Content Filtering***		
1	The appliance Must facilitate embedded Web Content Filtering feature		
2	Web content filtering solution Must work independently without the need to integrate with External proxy server.		
3	Must have facility to block URL' based on categories. Must support HTTP and HTTPS based traffic.		
4	URL database Must have more than 2 billion URLs under 70+ categories.		
5	Must be able to block different categories/sites based on User Authentication.		
6	Must have configurable parameters to block/allow unrated sites. Must have option to locally rate sites.		
7	Must have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable		
8	Must have options to customize the “Blocked Webpage Message” information displayed to end users		
9	Must have facility to schedule the configurations so that non-work related sites are blocked during office hrs and allow access to all sites except harmful sites during non-office hrs. Must also have time-based quota		
10	The solution Must have options to block java applets, ActiveX as well as cookies		
11	The solution Must be able to block URLs hosting spywares / adwares etc.		
12	Must have configurable policy options to define the URL exempt list		

1.13	***Anti-Spam***		
1	Must have integrated support for Anti-Spam for the following protocols: SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS		
2	Anti-Spam database Must have updates for Real-Time Blacklist and Open Relay Database Servers		
3	Automatic Real-Time Updates of Anti-Spam database		
4	Must perform MIME Header Check		
5	Must have facility for Keyword/Phrase Filtering		
6	Must be configurable for IP Address Blacklist and Exempt List		
1.14	***SD-WAN***		
1	Must support WAN load balancing (weighted) algorithms by volume, sessions, source-destination IP, Source IP, and spillover		
2	Must support multi-path intelligence using rules defined by:		
	Source address and/or user group		
	Destination address and/or a slection of over 3,000 applications		
	Path selection using particular link quality criteria or SLAs defined		
3	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		
4	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		
5	Must support traffic shaping policies that assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.		
6	Must support DSCP match in SD-WAN rules		
7	Must support inline and out-of-path WAN optimization topology, peer to peer, and remote client support		
8	Must support at least CIFS, FTP, HTTP(S), MAPI and TCP WAN optimization protocols		
9	Must support multiple WAN optimization sessions on the same tunnel		
10	Must support zero-touch deployment		

1.15	***Certifications***		
1	Must have support for the following certifications:		
a	FIPS-140-2 for Client VPN software		
b	OS Must be “IPv6 Phase II Ready” certified		

Table 2.10 **Data Centre Firewalls**

Index	Data Centre Firewalls (4 Units)	Compliance (Full, Partial, Not Complied)	Response
1.1	***General Requirements:***		
1	The solution must be appliance based and Must facilitate multi-application environment.		
2	Must be a leader in Gartner 2018 Enterprise Firewall Quadrant, recommended NSS Labs 2018 NGFW test and ICSA 2018 Firewall certification		
3	The platform must use a security-hardened, purpose-built operating system, and Must support the deployment option in NGFW mode		
4	The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
5	Licensing: Must be per device license for unlimited users for Firewall and other features. There Must not have any user/IP/host based licenses .		
6	The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
	Each Virtual Domain Must be allowed to connect to Specific 3rd Party Authentication service, AD, Radius, Tacacs or other…		
	Must support more than one ISP with automatic ISP failover		
7	Must have support for Explicit Proxy and Transparent Proxy		
8	Must form the heart of the security fabric by integrating networking and security solutions and 3rd party solutions		
9	Must have security fabric 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		
1.2	***Mandatory Requirements:***		
1	Must support a minimum of 8 x 10GE SFP+ Slots populated with at least 6 10G SFP+ SR modules		
2	Must support at least 8 Million Maximum Concurrent Sessions		
3	Must support at least 300,000 New Sessions/Second		

4	Must support at least 5 Gbps Enterprise/Production Threat Protection Throughput		
5	Must support at least 240GB SSD storage		
6	Must have the following licenses included Application Control, IPS, AV and Sandbox		
1.3	***Firewall Features Requirement:***		
1	The Firewall Must be ICSA Labs certified for Enterprise Firewall		
2	It Must be possible to operate the firewall in "bridge mode" or "transparent mode" apart from the standard NAT mode		
3	The Firewall must provide NAT functionality, including PAT.		
4	Must support "Policy-based NAT"		
5	The Firewall Must provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP		
6	Firewall Must support Voice based protocols like H.323, SIP, SCCP, MGCP etc and RTP Pinholing.		
7	The Firewall Must support User-Group based Authentication (Identity based Firewalling) & Scheduling		
8	IPv6 support for both NAT and Transparent Mode		
1.4	***Authentication Requirements:***		
1	Support for authentication at the firewall policy level (Local and Remote)		
2	Support for RSA Secure ID or other Token based products		
3	Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication		
4	Support for Native Windows Active Directory		
5	Must support authentication based on LDAP Groups		
6	Must support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators		
1.5	***Encryption / VPN Requirements***		
1	The VPN Must be integrated with firewall		
	Must support the following protocols:-		
a	DES & 3DES		

b	MD5, SHA-1 & the more secure SHA-256 authentication		
c	Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.		
d	Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm		
e	The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)		
2	Must support Hub and Spoke VPN topology		
3	IPSec NAT Traversal & Dead Peer Detection Must be supported		
4	IPSec VPN Must support XAuth over RADIUS and RSA SecurID or similar product.		
5	Must have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy		
6	Must support SSL Two-factor Authentication with Digital Certificates		
7	Must support Single Sign-On Bookmarks for SSL Web VPN		
8	Must support Windows, Linux and MAC OS for SSL-VPN (Must have always-on clients for these OS apart from browser based access)		
9	Must support NAT within IPSec/SSL VPN tunnels		
10	Must also support PPTP and L2TP over IPSec VPN protocols.		
1.6	***High Availability Requirements:***		
1	The device must support Active-Active as well as Active-Passive redundancy.		
2	The Firewall must support stateful failover for both Firewall and VPN sessions.		
3	The HA Architecture Must have the ability for Device Failure Detection and Notification as well as Link Status Monitor		
4	Must support VRRP and Link Failure Control		
1.7	***Data Center Optimization:***		
1	Must support Server Load Balancing with features like HTTP persistence		
2	Must support TCP Multiplexing		
3	Must support HTTPS Offloading with flexible Digital Certificate Management		
4	Must have support for WCCP protocol		

1.8	***Administration/ Management Requirements:***		
1	The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management		
2	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)		
3	There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)		
4	The device Must have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).		
5	Provision to generate automatic notification of events via mails / syslog		
6	Provision to send alerts to multiple email recipients		
7	Support for role based administration of firewall		
8	Must support simultaneous login of Multiple Administrators.		
9	Must have provision to customize the dashboard (eg: by selecting suitable Widgets)		
10	The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP		
11	Support for Image upgrade via FTP, TFTP and WebUI		
12	Must support system software rollback to the previous version after upgrade		
1.9	***Network IPS:***		
1	Must have integrated Network Intrusion Prevention System (NIPS)		
2	Must have a built-in Signature and Anomaly based IPS engine on the same unit		
3	Must have protection for 3000+ signatures		
4	Able to prevent denial of service and Distributed Denial of Service attacks.		
5	Must be able to exclude certain hosts from scanning of particular signatures		
6	Supports CVE-cross referencing of threats where applicable.		
7	Must provide the facility to configure Profile based sensors (Client/Server) for ease of deployment		
8	Must support granular tuning with option to configure Overrides for individual signatures.		

9	Supports automatic Attack database updates directly over the internet. (i.e. no dependency on any intermediate device)		
10	Supports attack recognition inside IPv6 encapsulated packets.		
11	Supports user-defined signatures (i.e. Custom Signatures) with Regular Expressions.		
12	Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options		
13	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		
14	Must Identify and control over 1000+ applications (i.e. Application control feature)		
15	Must perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc		
16	Must control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc		
1.10	***Gateway Antivirus***		
1	The appliance Must facilitate embedded anti-virus support		
2	Must include Antispyware and Worm Prevention		
3	Must have option to schedule automatic updates of the new virus pattern.		
4	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		
5	Must have configurable policy options to select what traffic to scan for viruses		
6	Must have option to configure to respond to virus detection at the gateway in several ways ie. Delete the file, Alert email, Quarantine etc		
7	Must have options to prevent user downloads based on file extension as well as file type		
8	Must have support for “Flow-Based Antivirus Scanning Mode” for high throughput requirements		
9	The solution Must be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
10	Must have an ability of Antivirus scanning for IPv6 traffic		

1.11	***Advanced Threat Protection***		
1	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.		
2	The solution Must have multi-layer of detection process with the malicious code emulation and execution in the VM environment.		
3	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.		
4	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.		
5	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.		
6	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.		
7	The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration		
8	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.		
9	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.		
10	The solution Must support logging of important parameters like Source IP, Destination IP, ports,		

	protocol, Domain, time stamp etc. of the malicious web sessions		
11	The solution Must be based on algorithm, which Must be able to detect maximum Malware or rogue elements with each signature.		
12	The solution Must have ability to block all outbound call- back communication initiated by the internal clients (infected)		
1.12	***Web Content Filtering***		
1	The appliance Must facilitate embedded Web Content Filtering feature		
2	Web content filtering solution Must work independently without the need to integrate with External proxy server.		
3	Must have facility to block URL' based on categories. Must support HTTP and HTTPS based traffic.		
4	URL database Must have more than 2 billion URLs under 70+ categories.		
5	Must be able to block different categories/sites based on User Authentication.		
6	Must have configurable parameters to block/allow unrated sites. Must have option to locally rate sites.		
7	Must have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable		
8	Must have options to customize the “Blocked Webpage Message” information displayed to end users		
9	Must have facility to schedule the configurations so that non-work related sites are blocked during office hrs and allow access to all sites except harmful sites during non-office hrs. Must also have time-based quota		
10	The solution Must have options to block java applets, ActiveX as well as cookies		
11	The solution Must be able to block URLs hosting spywares / adwares etc.		
12	Must have configurable policy options to define the URL exempt list		
1.13	***Certifications***		
1	Must have support “IPv6 Phase II Ready” certified		

Table 2.11 **Web Application Firewall**

Index	Web Application Firewall (2 Units)	Compliance (Full, Partial, Not Complied)	Response
1.1	***General Requirements:***		
1	The solution must be appliance based		
2	Should must be ICSA Certified with NSS Labs recommended WAF rating		
3	The platform must use a security-hardened, purpose-built operating system, and should support the deployment option in reverse proxy, inline transparent, true transparent proxy, offline sniffing and WCCP options		
4	The platform should use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
5	Licensing: Should be per device license for unlimited users for WAF and other features. There should not have any user/IP/host based licenses .		
6	The solution must be able to integrate with the proposed NGFW by synchronizing WAF protections and sharing of threat information to both deeply scan suspicious files and share infected internal sources.		
1.2	***Mandatory Requirements:***		
1	Must support at least 4 GE RJ-45 ports and 2x10G BASE-SR SFP+ slots		
4	Must support at least 20,000 HTTPS trans/sec		
5	Must support a WAF throughput of 1 Gbps		
6	Must support at least 700,000 HTTPS concurrent connections/sec		
8	Must support Active/Passive, Active/Active High Availability		
1.4	***WAF Security Features Requirement:***		
1	Should automatically and dynamically builds a security model of protected applications by continuously monitoring real time user activity		
2	Should be able to block Access outside the baseline		
3	Should Protect against:		
	OWASP Top 10		
	Cross Site Scripting		

	SQL Injection		
	Cross Site Request Forgery		
	Session Hijacking		
4	Must have a built-in Vulnerability Scanner		
5	Must support third-party scanner integration (virtual patching)		
6	Must support File upload scanning with AV and sandbox		
7	Must support automatic profiling (white list)		
8	Must support Web server and application signatures (black list)		
9	Must support IP Reputation		
10	Must support IP Geolocation		
11	Must support HTTP RFC compliance		
12	Must have Native support for HTTP/2		
13	Must support WWeb services signatures		
14	Must support XML and JSON protocol conformance		
15	Must support Malware detection		
16	Must support Virtual patching		
17	Must support Protocol validation		
18	Must support Brute force protection		
19	Must support Cookie signing and encryption		
20	Must support Threat scoring and weighting		
21	Must support Syntax-based SQLi detection		
22	Must support HTTP Header Security		
23	Must support Custom error message and error code handling		
24	Must support Operating system intrusion signatures		
25	Must provide Known threat and zero-day attack protection		
26	Must support L4 Stateful Network Firewall		
27	Must support DoS prevention		
28	Must support Advanced correlation protection using multiple security elements		
29	Must support Data leak prevention		
30	Must support Web Defacement Protection		
31	Must support Ongoing and automated protection against botnets and malicious sources		
32	Must support Bot dashboard help analyzing traffic from malicious robots, crawlers, scanners and search engines		

33	Must provide User behavior and web application structure analysis		
34	Must provide Geo IP analytics and security		
35	Must provide Antivirus file scanning		
36	Must support Credential Stuffing Defense		
37	Must support both cloud-based or on-premise sandboxing solution		
38	Must support machine learning to automate application and content inspection		
	Application Delivery		
1	Layer 7 server load balancing		
2	URL Rewriting		
3	Content Routing		
4	HTTPS/SSL Offloading		
5	HTTP Compression		
6	Caching		
	WAF Essential Features		
1	Must be IPv6 Ready		
2	Must support HTTP/2 to HTTP 1.1 translation		
3	Must support HSM Integration		
4	Must support Seamless PKI integration		
5	Must support a scanning for ActiveSync and OWA applications		
6	Must support Setup Wizards for common applications and databases		
7	Must support Preconfigured for common Microsoft applications; Exchange, SharePoint, OWA		
8	Must support predefined security policies for Drupal and Wordpress applications		
9	Must have Web Sockets support		
10	Must support active and passive authentication		
11	Must support Site Publishing and SSO		
12	Must support RSA Access for 2-factor authentication		
13	Must have LDAP, RADIUS, and SAML support		
14	Must have SSL client certificate support		
15	Must support CAPTCHA and Real Browser Enforcement (RBE)		

Table 2.12 **Entity and User Behavior Analytics (EUBA)**

Index	Entity and User Behavior Analytics (500 Agents)	Compliance (Full, Partial, Not Complied)	Response
1.1	***Entity and User Behavior Analytics Requirements:***		
1	The proposed solution must support continuous protective monitoring with flexible, automated auditing and monitoring process in place that oversees and scrutinizes the behaviors of the super user		
2	Must integrate easily with existing security platforms		
3	The proposed solution must instantly protect business data		
4	The proposed solution must provide 360 visibility around data flow whether users are on or off the network.		
5	The proposed solution must support and enable compliance across ISO 270001 and or EU GDPR; SOX (Sarbanes-Oxley), MiFID II, HIPAA		
6	The proposed solution can be applied to any data source - endpoint, database, cloud		
7	The proposed solution must provide fast, accurate insights with minimal human resources required		
8	The proposed solution must ensure that only the necessary data is collected and storage requirements are minimized		
9	The proposed solution must ensure that data can be stored for as long as required		
10	The proposed solution must provide visibility around permissions so you can fine-tune around global access, excessive permissions, and privilege escalations		
11	The proposed solution must be unobtrusive; doesn't impact on user privacy or productivity		
12	The proposed solution must minimize response time to threats with instant alerting		
13	The proposed solution must have minimum false-positives		
14	The proposed solution must provide clarity around shadow-IT usage i.e. how widespread it is, who's using it and what data has been shared with whom.		
15	The proposed solution's data is stored centrally so user activity can be correlated across machines into a single behavioral analysis		
16	The proposed solution must scale with organizational needs		

17	The proposed solution must be fully automated with no hand-holding required with rapid insights i.e. hours instead of days, weeks or even months.		
18	The proposed solution must provide detailed forensics that allow organizations to respond to threats rapidly, contain damage, avoid fines and mitigate financial and reputational loss		
19	The proposed solution must have no window or lag between collection and analysis of data		
20	The proposed solution must push architecture protecting data the instant it's switched on		
21	The proposed solution must unique UBA capabilities that enables one to drill down and identify risky activities quickly and intuitively		
22	The proposed solution must provide a bird's-eye view of user behaviour, rapidly prioritise relevant, high-risk anomalies		
23	The proposed solution must provide instant alerting and take immediate action and limit the amount of time your data is vulnerable		
24	The proposed solution must provide powerful analytics that automatically detects when a user's behavior changes, identify compromised user accounts		
25	The proposed solution must easily meet regulatory compliance requirements		
26	The proposed solution must robust reporting i.e. detailed, dynamic reporting capabilities, enabling critical decisions around your security strategy		
27	The proposed solution must detailed forensics i.e. full forensic history of all user behavior provided so you can quickly identify and answer questions around any incident - who/what/why		
28	The proposed solution must integrate with a SIEM for alerting		
29	The proposed solution must support user tracking / session capabilities		
30	The proposed solution must map datasets to analytics		