THE TECHNICAL UNIVERSITY OF KENYA

TENDER DOCUMENT

TENDER FOR SUPPLY, INSTALLATION, CONFIGURATION & COMMISSIONING OF UNIFIED THREAT MANAGEMENT (UTM) NETWORK SECURITY APPLIANCE

TUK/T/09/2016-17

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

Information contained in this document is provided strictly to assist prospective bidders in their bid preparation. Any other use or disclosure to a third party is restricted and requires prior permission from The Technical University of Kenya

The Technical University of Kenya

P.O.BOX 502428-00200,

NAIROBI-KENYA.

TEL:+254(020) 338232/338755/219690

JANUARY, 2017

TABLE OF CONTENTS

SECTION I - INVITATION TO TENDER

TENDER NOTICE

The Technical University of Kenya (TU-K) now invites tenders from interested, eligible and capable firms as follows:-

TENDER REFERENCE NUMBER	TENDER NAME	ELIGIBILITY	TENDER SECURITY AMOUNT (Kshs)	COST PER SET OF TENDER DOCUMENT (Kshs)
TUK/T/09/2016/17	Supply, Installation, Configuration & Commissioning of Unified Threat Management (UTM) Network Security Appliance	Open	50,000.00	Kshs.1000.00

Interested eligible tenderers may obtain further information and inspect the tender documents from the office of the Director Supply Chain Operations, N-Block, the Technical University of Kenya (TU-K) Headquarters, Haile Selassie Avenue, P. O Box 52428 – 00200, **Nairobi-Kenya**. Tel. +254 20343672, 2249974, 2251300: Fax +254 20 2219689 during normal working hours i.e. Monday to Friday between 8.00a.m to 1.00pm and 2.00pm to 5.00p.m **with effect from Thursday January 12, 2017** and at the TUK website http://www.tukenya.ac.ke. A complete set of tender documents may be obtained at a cost of Kshs.1000/= per set payable at the cashier's office situated on the ground floor of Administration Block of the Technical University of Kenya. All tender documents downloaded through the website should be duly registered at the office of the Director Supply Chain Operations.

Completed tender documents enclosed in plain sealed envelopes, marked **"Tender Reference No……," & "Category description"**…… should be deposited in the Tender Box situated on the first floor, Administration Block of The Technical University of Kenya Headquarters or be addressed and posted to:-

The Vice Chancellor
The Technical University of Kenya
P.O. Box 52428 – 00200
Nairobi.
http://www.tukenya.ac.ke

so as to reach on or before Thursday January 26, 2017, at 10.00 a.m. The closing/opening process will be conducted immediately thereafter in the presence of firms' representatives who choose to attend at the conference room situated on the 1st floor, Administration Block, the Technical University of Kenya.

Late bids will be returned unopened.

THE VICE CHANCELLOR

SECTION II - INSTRUCTIONS TO TENDERERS

Table of Clauses

SECTION II - INSTRUCTIONS TO TENDERERS

2.1 Eligible Tenderers

2.1.1 This Invitation for Tenders is open to all tenderers eligible as described in the Invitation to Tender. Successful tenderers shall complete the supply of goods by the intended completion date specified in the Schedule of Requirements Section VI.

2.1.2 The procuring entity's employees, committee members, board members and their relative (spouse and children) are not eligible to participate in the tender.

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

2.1.4 Tenderers shall not be under a declaration of ineligibility for corrupt and fraudulent practices.

2.2 Eligible Goods

2.2.1 All goods to be supplied under the contract shall have their origin in eligible source countries.

2.2.2 For purposes of this clause, "origin" means the place where the goods are mined, grown, or produced. Goods are produced when, through manufacturing, processing, or substantial and major assembly of components, a commercially-recognized product results that is substantially different in basic characteristics or in purpose or utility from its components

2.2.3 The origin of goods is distinct from the nationality of the tenderer.

2.3 Cost of Tendering

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

2.3.2 The price to be charged for the tender document shall not exceed Kshs.2,000/=

2.4. The Tender Document

2.4.1 The tender document comprises the documents listed below and addenda issued in accordance with clause 2.6 of these instructions to Tenderers

(i) Invitation to Tender
(ii) Instructions to tenderers
(iii) General Conditions of Contract
(iv) Special Conditions of Contract
(v) Schedule of requirements
(vi) Technical Specifications
(vii) Tender Form and Price Schedules
(viii) Tender Security Form
(ix) Contract Form
(x) Performance Security Form
(xi) Bank Guarantee for Advance Payment Form
(xii) Manufacturer's Authorization Form
(xiii) Confidential Business Questionnaire

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

2.5 Clarification of Documents

2.5.1 A prospective tenderer requiring any clarification of the tender document may notify the Procuring Entity in writing or by post at the entity's address indicated in the Invitation to Tender. The Procuring Entity 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 the Procuring Entity. Written copies of the Procuring Entity's response (including an explanation of the question but without identifying the source of inquiry) will be sent to all prospective tenderers that have

received the tender document.

2.5.2 The Procuring Entity shall reply to any clarifications sought by the tenderer within three (3) days of receiving the request to enable the tenderer to make timely submission of its tender.

2.6 Amendment of Documents

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

2.6.2 All prospective tenderers that have received the tender documents will be notified of the amendment in writing or by post and will be binding on them.

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

2.7 Language of Tender

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

2.8 Documents Comprising of Tender

2.8.1 The tender prepared by the tenderers shall comprise the following components

(a) a Tender Form and a Price Schedule completed in accordance with paragraph 2.9, 2.10 and 2.11 below

(b) documentary evidence established in accordance with paragraph 2.1.2 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 2.2.1 that the goods and ancillary services to be supplied by the tenderer are eligible goods and services and conform to the tender documents; and

(d) tender security furnished in accordance with paragraph 2.14

2.9 **Tender Forms**

2.9.1 The tenderer shall complete the Tender Form and the appropriate Price Schedule furnished in the tender documents, indicating the goods to be supplied, a brief description of the goods, their country of origin, quantity, and prices.

2.10 **Tender Prices**

2.10.1 The tenderer shall indicate on the appropriate Price Schedule the unit prices and total tender price of the goods it proposes to supply under the contract

2.10.2 Prices indicated on the Price Schedule shall include all costs including taxes, insurances and delivery to the premises of the entity.

2.10.3 Prices quoted by the tenderer shall be fixed during the Tenderer's performance of the contract and not subject to variation on any account. A tender submitted with an adjustable price quotation will be treated as non-responsive and will be rejected, pursuant to paragraph 2.22

2.10.4 The validity period of the tender shall be 90 days from the date of opening of the tender.

2.11 **Tender Currencies**

2.11.1 Prices shall be quoted in Kenya Shillings unless otherwise specified in the Appendix to Instructions to Tenderers.

2.12 **Tenderers Eligibility and Qualifications**

2.12.1 Pursuant to paragraph 2.1. 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.

2.12.2The documentary evidence of the tenderer's eligibility to tender shall establish to the Procuring entity's satisfaction that the tenderer, at the time of submission of its tender, is from an eligible source country as defined under paragraph 2.1

2.12.3The documentary evidence of the tenderer's qualifications to perform the contract if its tender is accepted shall be established to the Procuring Entity's satisfaction;

(a) that, in the case of a tenderer offering to supply goods under the contract which the tenderer did not manufacture or otherwise produce, the tenderer has been duly authorized by the goods' manufacturer or producer to supply the goods.

(b) that the tenderer has the financial, technical, and production capability necessary to perform the contract;

(c) 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, and spare parts stocking obligations prescribed in the Conditions of Contract and/or Technical Specifications.

2.13 Goods Eligibility and Conformity to Tender Documents

2.13.1 Pursuant to paragraph 2.2 of this section, the tenderer shall furnish, as part of its tender documents establishing the eligibility and conformity to the tender documents of all goods which the tenderer proposes to supply under the contract

2.13.2 The documentary evidence of the eligibility of the goods shall consist of a statement in the Price Schedule of the country of origin of the goods and services offered which shall be confirmed by a certificate of origin issued at the time of shipment.

2.13.3 The documentary evidence of conformity of the goods to the tender documents may be in the form of literature, drawings, data and shall consist of:

(a) a detailed description of the essential technical and performance characteristic of the goods;

(b) a list giving full particulars, including available source and current prices of spare parts, special tools, etc., necessary for the proper and continuing functioning of the goods for a period of one (1) year, following commencement of the use of the goods by the Procuring Entity; and

(c) a clause-by-clause commentary on the Procuring entity's technical specifications demonstrating substantial responsiveness of the goods and service to those specifications, or a statement of deviations and exceptions to the provisions of the technical specifications.

2.13.4 For purposes of the documentary evidence to be furnished pursuant to paragraph 2.13.3(c) above, the tenderer shall note that standards for workmanship, material, and equipment, as well as references to brand names or catalogue numbers designated by the Procurement Entity in its technical specifications, are intended to be descriptive only and not restrictive. The tenderer may substitute alternative standards, brand names, and/or catalogue numbers in its tender, provided that it demonstrates to the Procurement Entity's satisfaction that the substitutions ensure substantial equivalence to those designated in the technical specifications.

2.14 Tender Security

2.14.1 The tenderer shall furnish, as part of its tender, a tender security for the amount specified in the Appendix to Invitation to Tenderers.

2.14.2 The tender security shall be in the amount of 0.5 – 2 per cent of the tender price.

2.14.3 The tender security is required to protect the Procuring Entity against the risk of the tenderer's conduct which would warrant the security's forfeiture, pursuant to paragraph 2.14.7

2.14.4 The tender security shall be denominated in Kenya Shillings or in another freely convertible currency, and shall be in the form of a bank guarantee or a bank draft issued by a reputable bank located in Kenya or abroad, or a guarantee issued by a reputable insurance company in the form provided in the tender documents or another form acceptable to the Procuring Entity and valid for thirty (30) days beyond the validity of the tender.

2.14.5 Any tender not secured in accordance with paragraph 2.14.1 and 2.14.3 will be rejected by the Procuring entity as non responsive, pursuant to paragraph 2.22

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

2.14.7 The successful Tenderer's tender security will be discharged upon the tenderer signing the contract, pursuant to paragraph 2.27 and furnishing the performance security, pursuant to paragraph 2.28

2.14.8 The tender security may be forfeited:

(a) if a tenderer withdraws its tender during the period of tender validity specified by the procuring entity on the Tender Form; or
(b) in the case of a successful tenderer, if the tenderer fails:
    (i) to sign the contract in accordance with paragraph 2.27
    Or
    (ii) to furnish performance security in accordance with paragraph 2.28

2.15 Validity of Tenders

2.15.1 Tenders shall remain valid for 90 days or as specified in the Invitation to tender after the date of tender opening prescribed by the Procuring Entity, pursuant to paragraph 2.18. A tender valid for a shorter period shall be rejected by the Procuring Entity as non responsive.

2.15.2 In exceptional circumstances, the Procuring Entity may solicit the tenderer's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The tender security provided under paragraph 2.14 shall also be suitably extended. A tenderer may refuse the request without forfeiting its tender security. A tenderer granting the request will not be required nor permitted to modify its tender.

2.16 **Format and Signing of Tender**

2.16.1 The Procuring Entity shall prepare one copy of the tender.

2.16.2 The original of the tender shall be typed or written in indelible ink and shall be signed by the tenderer or a person or persons duly authorized to bind the tenderer to the contract. The latter authorization shall be indicated by written power-of-attorney accompanying the tender. All pages of the tender, except for unamended printed literature, shall be initialed by the person or persons signing the tender.

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

2.17 Sealing and Marking of Tenders

2.17.1 The Tenderer shall seal the seal the envelope.

2.17.2 The envelopes shall:

(a) Be addressed to the Procuring Entity at the address given in the Invitation to Tender:

1.1 (b) Bear, tender number and name in the Invitation for Tenders and the words, "**DO NOT OPEN BEFORE," January 26, 2017 at 10.00a.m.**

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

2.17.4 If the envelope is not sealed and marked as required by paragraph 2.17.2, the Procuring Entity will assume no responsibility for the tender's misplacement or premature opening.

2.18 Deadline for Submission of Tenders

Tenders must be received by the Procuring entity at the address specified under paragraph 2.17.2 not later than **January 26, 2017 at 10.00a.m.**

2.18.1 The Procuring Entity may, at its discretion, extend this deadline for the submission of tenders by amending the tender documents in accordance with paragraph 2.6, in which case all rights and obligations of the Procuring Entity and tenderers previously subject to the deadline will therefore be subject to the deadline as extended

2.19 Modification and Withdrawal of Tenders

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

2.19.2 The Tenderer's modification or withdrawal notice shall be prepared, sealed, marked, and dispatched in accordance with the provisions of paragraph 2.17. A withdrawal notice may also be sent by cable or telex but followed by a signed confirmation copy, postmarked not later than the deadline for submission of tenders.

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

2.19.4 No tender may be withdrawn in the interval between the deadline for submission of tenders and the expiration of the period of tender validity specified by the tenderer on the Tender Form. Withdrawal of a tender during this interval may result in the tenderer's forfeiture of its tender security, pursuant to paragraph 2.14.7

2.19.5 The Procuring Entity may at any time terminate procurement proceedings before contract award and shall not be liable to any person for the termination.

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

2.20 Opening of Tenders

The Procuring entity will open all tenders in the presence of the tenderers' representatives who choose to attend, on **January 26, 2017 at 10.00a.m** and in the location specified in the Invitation to Tender.
The tenderers' representatives who will be presence shall sign a register evidencing their attendance.

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

2.20.2 The Procuring Entity will prepare minutes of the tender opening.

2.21 Clarification of Tenders

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

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

2.22 Preliminary Examination

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

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

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

2.22.4 Prior to the detailed evaluation, pursuant to paragraph 2.23 the Procuring Entity will determine the substantial responsiveness of each tenderer to the tender documents. For purposes of these paragraphs, a substantially responsive tender is one, which conforms to all the terms and conditions of the tender documents without material deviations. The Procuring Entity's determination of a tender's responsiveness is to be based on the contents of the tender itself without recourse to extrinsic evidence.

2.22.5 If a tender is not substantially responsive, it will be rejected by the Procuring Entity and may not subsequently be made responsive by the tenderer by correction of the non conformity.

2.23 Conversion to Single Currency

2.23.1 Where other currencies are used, the procuring entity will convert these currencies to Kenya Shillings using the selling exchange rate on the rate of tender closing provided by the Central Bank of Kenya.

2.24 Evaluation and Comparison of Tenders

2.24.1 The Procuring Entity will evaluate and compare the tenders which have been determined to be substantially responsive, pursuant to paragraph 2.22

2.24.2 The tender evaluation committee shall evaluate the tender within 30 days of the validity period from the date of opening the tender.

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

2.25 Preference

2.25.1 Preference where allowed in the evaluation of tenders shall not exceed 15% of the tender value.

2.26 Contacting the Procuring Entity

2.26.1 Subject to paragraph 2.21 no tenderer shall contact the Procuring Entity on any matter related to its tender, from the time of the tender opening to the time the contract is awarded.

2.26.2 Any effort by a tenderer to influence the Procuring Entity in its decisions on tender, evaluation, tender comparison, or contract award may result in the rejection of the Tenderer's tender.

2.27 Award of Contract

(a) **Post-qualification**

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

2.27.2 The determination will take into account the tenderer financial, technical, and production capabilities. It will be based upon an examination of the documentary evidence of the tenderers qualifications submitted by the tenderer, pursuant to paragraph 2.12.3 as well as such other information as the Procuring entity deems necessary and appropriate.

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

(b) **Award Criteria**

2.27.4 The Procuring Entity will award the contract to the successful tenderer(s) whose tender has been determined to be substantially responsive and has been determined to be the lowest evaluated tender, provided further that the tenderer is determined to be qualified to perform the contract satisfactorily.

(c) **Procuring Entity's Right to Vary quantities**

2.27.5 The Procuring Entity reserves the right at the time of contract award to increase or decrease the quantity of goods originally specified in the Schedule of requirements without any change in unit price or other terms and conditions

(d) **Procuring entity's Right to accept or Reject any or All Tenders**

2.27.6 The Procuring Entity reserves the right to accept or reject any tender, and to annul the tendering process and reject all tenders at any time prior to contract award, without thereby incurring any liability to the affected tenderer or tenderers or any obligation to inform the affected tenderer or tenderers of the grounds for the Procuring Entity's action

2.28 Notification of Award

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

2.28.2 The notification of award will constitute the formation of the Contract but will have to wait until the contract is finally signed by both parties

2.28.3 Upon the successful tenderer's furnishing of the performance security pursuant to paragraph 2.28, the Procuring Entity will promptly notify each unsuccessful tenderer and will discharge its tender security, pursuant to paragraph 2.14

2.29 Signing of Contract

2.29.1 At the same time as the Procuring Entity notifies the successful tenderer that its tender has been accepted, the Procuring Entity will send the tenderer the Contract Form provided in the tender documents, incorporating all agreements between the parties.

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

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

2.30 Performance Security

2.30.1 Within thirty (30) days of the receipt of notification of award from the Procuring entity, the successful tenderer shall furnish the performance security in accordance with the Conditions of Contract, in the Performance Security Form provided in the tender documents, or in another form acceptable to the Procuring Entity.

2.30.2 Failure of the successful tenderer to comply with the requirements of paragraph 2.27 or paragraph 2.28 shall constitute sufficient grounds for the annulment of the award and forfeiture of the tender security, in which event the Procuring entity may make the award to the next lowest evaluated tenderer or call for new tenders.

2.31 Corrupt or Fraudulent Practices

2.31.1 The Procuring Entity 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;

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

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, 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 the Procuring Entity of the benefits of free and open competition.

2.31.2 The Procuring Entity will reject a proposal for award if it determines that the tenderer recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

2.31.3 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

Notes on the Appendix to the Instruction to Tenderers

1. The Appendix to instructions to tenderers is intended to assist the Procuring Entity in providing specific information in relation to the corresponding clause in the instructions to tenderers included in Section II and has to be prepared for each specific procurement.

2. The Procuring Entity should specify in the Appendix information and requirements specific to the circumstances of the Procuring Entity, the goods to be procured and the tender evaluation criteria that will apply to the tenders.

3. In preparing the Appendix the following aspects should be taken into consideration;

(a) The information that specifies and complements provisions of Section II to be incorporated

(b) Amendments and/or supplements if any, to provisions of Section II as necessitated by the circumstances of the goods to be procured to be also incorporated

4. Section II should remain unchanged and can only be amended through the Appendix.

5. Clauses to be included in this part must be consistent with the public procurement law and the regulations.

Appendix to Instructions to Tenderers

The following information regarding the particulars of the tender shall complement supplement or amend the provisions of the instructions to tenderers. Wherever there is a conflict between the provision of the instructions to tenderers and the provisions of the Appendix, the provisions of the Appendix herein shall prevail over those of the instructions to tenderers

INSTRUCTIONS TO TENDERERS REFERENCE	**PARTICULARS OF APPENDIX TO INSTRUCTIONS TO TENDERS**
2.1.1	*All Tenderers are eligible as it is a public tender*
2.14.1	*Tender Security shall be Kshs 50,000.00*
	Terms and Conditions of Payment: ***30 days credit period***
2.18.1	*Closing Date of the Tender shall be* **January 26, 2017 at 10.00a.m.**
2.27.2	*Award will be on the basis of overall lowest evaluated and most responsive bidder.*
2.9.1	**IMPORTANT**: Please note that your technical bid should not contain the form of tender and the price schedule form otherwise you will be automatically disqualified. **SUBMISSION OF FINANCIAL BID (THIS SHOULD BE SEPERATE FROM THE TECHNICAL BID)** 1. Fill, sign and rubberstamp the form of tender. 2. Fill, sign and rubberstamp the price schedule form. **Note: The** technical bid containing the bid security should be in its own envelope and the financial bid (form of tender and price schedule form) should be in its own envelope. The technical bid envelope and the financial bid envelope should be sealed in one big envelope during submission of the tender.

SECTION III: GENERAL CONDITIONS OF CONTRACT

Table of Clauses

SECTION III- GENERAL CONDITIONS OF CONTRACT

3.1 **Definitions**

3.2 **Application**

3.2.1 These General Conditions shall apply in all Contracts made by the Procuring entity for the procurement installation and commissioning of equipment

3.3 **Country of Origin**

3.3.1 For purposes of this clause, "Origin" means the place where the Goods were mined, grown or produced.

3.3.2 The origin of Goods and Services is distinct from the nationality of the tenderer

3.4 **Standards**

3.4.1 The Goods supplied under this Contract shall conform to the standards mentioned in the Technical Specifications.

3.5 **Use of Contract Documents and Information**

3.5.1 The tenderer shall not, without the Procuring entity's prior written consent, disclose the Contract, or any provision therefore, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the Procuring entity in connection therewith, to any person other than a person employed by the tenderer in the performance of the Contract.

3.5.2 The tenderer shall not, without the Procuring entity's prior written consent, make use of any document or information enumerated in paragraph 3.5.1 above

3.5.3 Any document, other than the Contract itself, enumerated in paragraph 3.5.1 shall remain the property of the Procuring entity and shall be returned (all copies) to the Procuring entity on completion of the Tenderer's performance under the Contract if so required by the Procuring entity

3.6 **Patent Rights**

3.6.1 The tenderer shall indemnify the Procuring entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof in the Procuring entity's country

3.7 **Performance Security**

3.7.1 Within thirty (30) days of receipt of the notification of Contract award, the successful tenderer shall furnish to the Procuring Entity the performance security in the amount specified in Special Conditions of Contract.

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

3.7.3 The performance security shall be denominated in the currency of the Contract, or in a freely convertible currency acceptable to the Procuring entity and shall be in the form of a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in Kenya or abroad, acceptable to the Procuring entity, in the form provided in the tender documents.

3.7.4 The performance security will be discharged by the Procuring entity and returned to the Candidate not later than thirty (30) days following the date of completion of the Tenderer's performance obligations under the Contract, including any warranty obligations, under the Contract

3.8 **Inspection and Tests**

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

3.8.2 The inspections and tests may be conducted in the premises of the tenderer or its subcontractor(s), at point of delivery, and/or at the Goods' final destination. If conducted on the premises of the tenderer or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring entity.

3.8.3 Should any inspected or tested goods fail to conform to the Specifications, the Procuring entity may reject the equipment, and the tenderer shall either replace the rejected equipment or make alternations necessary to make specification requirements free of costs to the Procuring entity.

3.8.4 The Procuring entity's right to inspect, test and where necessary, reject the goods after the Goods' arrival shall in no way be limited or waived by reason of the equipment having previously been inspected, tested and passed by the Procuring entity or its representative prior to the equipment delivery.

3.8.5 Nothing in paragraph 3.8 shall in any way release the tenderer from any warranty or other obligations under this Contract.

3.9 **Packing**

3.9.1 The tenderer shall provide such packing of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the Contract.

3.9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract

3.10 **Delivery and Documents**

3.10.1 Delivery of the Goods shall be made by the tenderer in accordance with the terms specified by Procuring entity in its Schedule of Requirements and the Special Conditions of Contract

3.11 **Insurance**

3.11.1 The Goods supplied under the Contract shall be fully insured against loss or damage incidental to manufacturer or acquisition, transportation, storage, and delivery in the manner specified in the Special conditions of contract.

3.12 **Payment**

3.12.1 The method and conditions of payment to be made to the tenderer under this Contract shall be specified in Special Conditions of Contract

3.12.2 Payments shall be made promptly by the Procuring entity as specified in the contract

3.13 Prices

3.13.1 Prices charged by the tenderer for goods delivered and services performed under the Contract shall not, with the exception of any price adjustments authorized in Special Conditions of Contract, vary from the prices by the tenderer in its tender.

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

3.13.3 Where contract price variation is allowed, the variation shall not exceed 25% of the original contract price.

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

3.14. Assignment

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

3.15 Subcontracts

3.15.1 The tenderer shall notify the Procuring entity in writing of all subcontracts awarded under this Contract if not already specified in the tender. Such notification, in the original tender or later, shall not relieve the tenderer from any liability or obligation under the Contract

3.16 Termination for default

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

(a) if the tenderer fails to deliver any or all of the goods within the periods) specified in the Contract, or within any extension thereof granted by the Procuring Entity

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

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

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

3.17 Liquidated Damages

3.17.1. If the tenderer fails to deliver any or all of the goods within the period(s) specified in the contract, the procuring entity shall, without prejudice to its other remedies under the contract, deduct from the contract prices liquidated damages sum equivalent to 1% of the delivered price of the delayed items up to a maximum deduction of 10% of the delayed goods. After this the tenderer may consider termination of the contract.

3.18 Resolution of Disputes

3.18.1 The procuring entity and the tenderer shall make every effort to resolve amicably by direct informal negotiation and disagreement or dispute arising between them under or in connection with the contract

3.18.2 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 require adjudication in an agreed national or international forum, and/or international arbitration.

3.19 Language and Law

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

3.20 Force Majeure

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

SECTION IV - SPECIAL CONDITIONS OF CONTRACT

Notes on Special Conditions of Contract

The clauses in this section are intended to assist the procuring entity in providing contract-specific information in relation to corresponding clauses in the General Conditions of Contract

The provisions of Section IV complement the General Conditions of Contract included in Section III, specifying contractual requirements linked to the special circumstances of the procuring entity and the goods being procured. In preparing Section IV, the following aspects should be taken into consideration.

(a) Information that complement provisions of Section III must be incorporated and
(b) Amendments and/or supplements to provisions of Section III, as necessitated by the circumstances of the goods being procured must also be incorporated.

SECTION IV - SPECIAL CONDITIONS OF CONTRACT

4.1. Special Conditions of Contract shall supplement the General Conditions of Contract. Whenever there is a conflict, between the GCC and the SCC, the provisions of the SCC herein shall prevail over these in the GCC.

42. Special conditions of contract as relates to the GCC

REFERENCE OF GCC	**SPECIAL CONDITIONS OF CONTRACT**
3.7.1	*Tender Security is 50,000.00* *Performance security 10% of the tender sum*
3.12.1	*Terms of payment: 30 days credit period*
3.13.1 & 3.13.2	*There Shall be no Price Variations within the period of the contract*
2.27.4	*Award of contract will be on the basis of overall lowest evaluated most responsive bidder.*
3.18.1	*Resolutions of disputes shall be through an agreed national or international forum, and/or international arbitration.*
2.9.1	***IMPORTANT**: Please note that your technical bid should not contain the form of*

	tender and the price schedule form otherwise you will be automatically disqualified. ***SUBMISSION OF FINANCIAL BID (THIS SHOULD BE SEPERATE FROM THE TECHNICAL BID)*** *1. Fill, sign and rubberstamp the form of tender.* *2. Fill, sign and rubberstamp the price schedule form.* *Note: The technical bid containing the bid security should be in its own envelope and the financial bid (form of tender and price schedule form) should be in its own envelope. The technical bid envelope and the financial bid envelope should be sealed in one big envelope during submission of the tender.*

SECTION IV – SCHEDULE OF REQUIREMNTS

TECHNICAL SPEIFICATIONS FOR THE

Introduction

Technical University of Kenya (TUK) intends to deploy an "application-aware" next generation firewall with fine-grained role-based access control, capable of providing high performance required for future enterprise networks.

The Next-Generation Network security appliance should offer inline application inspection and control, HTTPS inspection, Intrusion Prevention System, malware protection, secure remote access via VPN (IPSec and SSL) and granular bandwidth controls. The inline Layer 8 Identity-based controls with on-appliance reporting should offer complete control & real-time visibility over user and network activities. It should be deployed with minimum efforts with a high throughput speeds, offering future-ready security to the Institution.

TUK currently receives internet services from two Internet Providers and therefore the UTM should have the capability to accommodate these providers and balance the traffic load appropriately for efficient utilization of the bandwidth.

There are currently 18 physical servers running over 30 server services, some in virtualized environment. This number and virtualization schemes is set to grow in the near future. 6 of these server/services are connecting via public IP addresses.

The student and staff population currently stands at 14,500 and 1,300 respectively and figures are set to increase. The Staff and students use a variety of devices e.g. PCs, Laptops, Tablet, Smart phones etc. to access the Internet and intranet resources.

There are currently 8 VPNs and this will increase in the near future. There are currently two remote LANs which shares common resources with the main campus LAN. The remote sites shall increase to 4 in the near future.

We desire a UTM that shall provide the administrator with the ability to manage traffic to the level of individual user or device.

Background of the assignment

The Technical University of Kenya seeks to engage a reputable Networks / Data-Center /security solutions provider to supply, install and configure a Unified Threat Management to enhance its business systems. The Vendor of the gateway software must:

- have **at least 4years of experience** in the Networks / Data-Center /securitymarket
- be capable of serving the entire scope of security gateway requirements, including throughput, connection rate and next generation security application enablement for all network deployments, from small office to data center in a single hardware appliance
- be able to supply and support the solution exclusively
- provide a mechanism to constantly educate end users of the Security policy in real time.

Minimum Technical Specifications for the required Unified Threat Management System –

Table: Compliance to Technical Specifications

Item *Description*	*Fully Compliant*	*Partially Compliant*	*Does not Comply*	*Score*
1. Interfaces				**10**
1.1 Copper GBE Ports……. 8				
1.2 1GbE SFP(Mini GBIC) Ports……..…. 8				
1.3 10GbE SFP(Mini GBIC) Ports…… 2				
1.4 Configurable Internal/DMZ/WAN Ports...Yes				
1.5 Console Ports (RJ45)…….. 1				
1.6 USB Ports…….. 2				
1.7 Hardware Bypass Segments……. 2				
1.8 RAID 1 (with two disk)……..... Yes				
2. System Performance				**20**
2.1 Firewall throughput (UDP) (Mbps)… 30,000				
2.2 Firewall throughput (TCP) (Mbps)….. 28,000				
2.3 New sessions/second……. 200,000				
2.4 Concurrent sessions……. 3,500,000				
2.5 IPSec VPN throughput (Mbps)……. 8,000				
2.6 No. of IPSec Tunnels…… 3,000				
2.7 SSL VPN throughput (Mbps)…….. 1,000				
2.8 WAF throughput (Mbps)…….. 1,000				
2.9 Anti-Virus throughput (Mbps)…….. 5,000				
2.10 IPS throughput (Mbps)……... 6,000				
2.11 UTM throughput (Mbps)…….. 4,000				
3. Firewall				**20**
3.1 The solution's Firewall must be available as a Next-Generation Firewall and UTM.				

3.2 The security gateway must use Stateful and Deep packet Inspection based on granular analysis of communication and application state for network, application and user identity-based security.				
3.3 Should provide Flood protection: DoS, DDoS and portscan blocking/ prevention				
3.4 Should Enforce policy across Multiple Security zones, networks, or by service type				
3.5 Firewall with High Availability with stateful failover,				
3.6 Should support NAT-traversal and allow Customizable NAT policies with IP masquerading				
3.7 Should support Multiple Access Control Criteria (ACC) – User/ group - Identity, Source & Destination Zone, MAC and IP address, Service				
3.8 Must offer support Thin Client-Thin client authentication with session IDs,Supports Citrix – XenApp server, Microsoft Windows Server (Microsoft TSE) and Identity-based policies in thin client environment				
3.9 The solution must allow MAC&IP-MAC filtering and IP Spoof prevention				
3.10 The solution must support Time and Data Quota restriction				
3.11 The solution must support Schedule based Committed and Burstable Bandwidth				
3.12 The solution must allow Layer 7 (Application) Control & Visibility				
3.13 The solution must support Layer-8 user identity awareness across key areas of the firewall- Firewall Rules based on user or Group membership in Active Directory (AD) orLightweight Directory Access Protocol (LDAP				
3.14 The solution must offer Centralized Management				
3.15 The solution must offer Comprehensive Logging & Reporting- Layer 8 Identity-based Reporting, Firewall logs and Centralized logging and reporting				
3.16 Must have Virtual host capability				
3.17 The solution must support Multi-core technology for high-speed parallel processing				
3.18 The solution must Enable secure hosting of servers inside LAN and DMZ				
3.19 The solution must supports creation of work profile-based groups across distributed locations				
4. Intrusion Prevention System (IPS)				**15**
4.1 IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection				
4.2 IPS must provide an automated mechanism to activate or manage new signatures from updates				
4.5 IPS must support network exceptions based on source, destination, service or a combination of the three.				
4.6 IPS application must have a centralized event				

correlation and reporting mechanism.				
4.7 IPS must be able to detect and prevent the following threats: Protocol misuse, malware communications, tunneling attempts, Distributed Denial of Service (DDoS) and generic attack types without predefined signatures.				
4.8 IPS must be able to collect packet capture for specific protections				
4.9 IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP, Windows services (Microsoft Networking), SNMP……				
4.10 IPS and/or Application Control must include the ability to detect and block peer to peer traffic using evasion techniques.				
4.11 IPS must support Flexible IPS policy deployment as part of any network or user policy with full customization/ User-based policy creation				
4.12 IPS must support High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection				
4.13 IPS must support Automatic real-time updates from CR Protect networks				
4.14 IPS must support for over 5000 default and customized Signatures				
4.14 IPS must detect, block or drop intrusion attempts by detecting anomalous traffic.				
5. Identity Awareness				**5**
5.1 Must be able to acquire user identity by querying Microsoft Active Directory (AD) andLightweight Directory Access Protocol (LDAP based on security events.				
5.2 Must have a browser based User Identity authentication method for non-domain users or assets.				
5.3 Must support the use of LDAP nested groups.				
5.4 Must be able share or propagate user identities between multiple security gateways				
6. Application Protection, Control and Filtering				**25**
6.1 The solution must provide granular security control of at least 250,000 Web 2.0 widgets.				
6.2 The solution must offer complete visibility on which applications are being accessed within the organization and by which user, irrespective of their ports and protocols.				
6.3 The solution must not have any known published vulnerabilities in the last year to the existing architecture which can be exploited.				
6.4 The solution must be able to Prioritize bandwidth allocation to critical applications Eg. Salesforce, Sharepoint, CRM, ERP, etc. and Control bandwidth allocation to non-business applications				
6.5 The solution must have an easy to use, searchable interface for applications and URLs				

6.6 The solution must have Layer 8 Identity and QoS-based Application Control- Control application usage based on user, user group, source, destination and bandwidth				
6.7 The solution must provide a mechanism to inform or ask users in real time to educate them or confirm actions based on the security policy.				
6.8 The solution must support application control based on category, characteristics (e.g. bandwidth and productivity consuming), technology (e.g. P2P) and risk level				
6.9 The application control and URLF security policy must report on the rule hit count.				
6.10 Enhanced application control with signatures and Layer 7 patterns for thousands of applications.				
6.11 The solution must support dynamic application identification that utilizes the Synchronized Security Heartbeat link with the endpoint to determine apps responsible for generating unknown traffic on the network				
6.12 The solution must offer application control to TUK based on network access policies, users and their job roles, and time				
6.13 The solution must be able to create a filtering for single site being supported by multiple categories.				
6.14 The solution must have the pro-active protection model which eliminates the need for manual intervention by administrator to update policy for new applications that are being added to the list				
6.15 The solution must control usage of social applications Eg., Facebook, YouTube, iTunes, gaming, BitTorrent based on Time and Layer 8 Identity-based policies				
6.16 The solution must control P2P applications, Eg. Skype and IM applications				
6.17 The solution must support Real-time network logs and reports to allow TUK to promptly re-set network settings for maximum security and productivity.				
6.18 The solution must have Inbuilt application category database				
6.19 The solution must Prevents "Phone home" activities and keyloggers				
6.20 The solution must SUPPORT Visibility & Control over HTTPS-based Micro Apps- Should support Deep scans HTTPS-based applications- Prevents latent security threats from HTTPS based requests from entering network				
6.21 The solution must Support the creation of White (Business-Critical), Black (Non-Productive), Grey (Social, Entertainment) application categories for prioritization				
6.22 The solution must Schedule non-critical applications during non-peak hours				
6.23 The solution must Blocks anonymous proxies Eg. UItra surf				
7. Web *Application* Protection, Control				**25**

and Filtering				
7.1 The solution must support Complete Visibility & Control over HTTP & HTTPS Web Filtering, comprehensive URL databases with millions of URLs grouped into hundreds of categories				
7.2 Live Protection real-time in-the-cloud lookups for the latest threat intelligence				
7.3 Protection against SQL Injections, Cross-site Scripting (XSS), Session Hijacking, URL Tampering, Cookie Poisoning				
7.4 HTTP and HTTPS scanning and enforcement on any network and user policy with fully customizable rules and exceptions				
7.5 File type filtering by mime-type, extension and active content types (e.g. Activex, Java applets, cookies, etc.)				
7.6 The solution must support Customized Allow/Warn/Block IP ranges, messages per category (third-party proxy and tunnelling software, Google cache pages, embedded URLs in websites, malware, phishing, pharming URLs, Java Applets, Cookies, Active X				
7.7 The solution must enforce 'safe search' in search engines				
7.8 The solution must offer a wide security cover against web-based threats, including the entry of malware, phishing, pharming, intrusions and unauthorized data uploads.				
7.9 The solution must support Layer 8 Identity-based Controls –surfing policies based on user, group, work function, web category and duration or time of the day deliver high flexibility and web security and content security.				
7.10 The solution must support Bandwidth Management which ensures bandwidth availability and data transfer limit based on duration and schedule of access for specific web categories and so limit rather than block non-productive sites.				
7.11 The solution must detect and block third-party proxy and tunneling software, Google cache pages, embedded URLs and 'safe search' over search engines to prevent harmful websites from appearing in search results.				
7.12 The solution must support Data Leakage Prevention –block file uploads over HTTP, HTTPS and FTP while Instant Messaging and Application Visibility & Control block file transfers over IM and P2P applications,				
7.13 Solution must block access to harmful websites, preventing malware, phishing, pharming attacks and undesirable content that could lead to legal liability and direct financial losses.				
7.14 The solution must perform comprehensive web filtering & content filtering based on multiple options – URL, Keyword, File type, Database				
7.15 On-appliance reporting must offer visibility into user and system activity, allowing TUK to take instant and preventive action to meet compliance requirements.				

7.16 The solution must support multiple categorization - On-cloud, Customized and third party URL databases				
7.17 The solution must support HTTPS Controls such as Visibility into encrypted HTTPS Traffic, Prevention of unauthorized file upload and download over HTTP and HTTPS and Blocking unauthorized, malicious and illegal HTTPS websites				
7.18 The solution must support Layer 8 Identity-based Controls- Username, group, work-requirement based policies; Schedule-based access control; Integrates with a range of existing authentication mechanisms (ADS, RADIUS, SSO, local and thin client…..)				
7.19 The solution must support Data and bandwidth quota allocation based on web categories and time of the day				
7.20 The solution must support customized messages to user with reason for blocked website				
7.21 The solution must support Category-based bandwidth allocation and prioritization				
7.22 The solution must support Unscannable content handling				
7.23 The solution must support Automatic appending of prefix/suffix for authentication				
7.24 The solution must support Reverse authentication (offloading) for form-based and basic authentication for server access				
7.25 The solution must support SSL protocol tunnelling detection and enforcment				
8. Anti-Bot				**5**
8.1 The solution must have an integrated Anti-Bot application on the next generation firewall.				
8.2 The solution's Anti-Bot policy must be administered from a central console.				
8.3 Anti-Bot application must have a centralized event correlation and reporting mechanism.				
8.4 Anti-Bot must be have real time updates from a cloud based service				
8.5 Anti-Bot policies must be centrally managed with granular policy configuration and enforcement.				
9. Gateway Anti-Virus & Anti-Spyware				**10**
9.1 The solution must have Virus, Worm, Trojan…. Detection &Removal ability				
9.2 The solution must support Automatic and real time virus signature database update				
9.3 The solution must protect against Spyware, Malware, Phishing				
9.4 The solution must scan HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IM, VPN Tunnels etc				
9.5 The solution must support the addition of disclaimers/signatures				
9.6 The solution's Anti-Virus policies must be centrally managed with granular policy configuration and enforcement.				
9.7 The solution must support Self Service Quarantine area				

9.8 The solution's Anti-virus application must be able to inspect SSL encrypted traffic.				
9.9 The solution must support customized individual user scanning- Scan and deliver by file size, Block by file types				
9.10 The solution's Anti-Virus must be able to stop incoming malicious files.				
10. Gateway Anti-Spam				**10**
10.1 The solution must offer real-time spam protection over SMTP, POP3, IMAP protocols, protecting organizations from zero-hour threats and blended attacks that involve spam, malware, botnets, phishing, Trojans etc.				
10.2 The solution must have the ability to perform Inbound/Outbound Scanning				
10.3 Should support Virus Outbreak Detection (VOD)- Signature-less detection from Anti-Virus and Anti-Spyware to closes early-hour vulnerability gap of massive virus outbreaks over email and offers Comprehensive Email Security				
10.4 Must perform Spam Filtering- IP reputation-based filtering, RBL Lists, MIME header check and should be based on message header, size, sender, recipient				
10.5 The solution must support Email Management-Granular email management with message and attachment size, subject line etc.				
10.6 The solution must support Identity-based Security-Layer 8 Identity-based requirement- Copy and route mail to pre-defined mail addresses thus preventing Data Leakage Prevention DLP (Granular protection based on user work profile)				
10.7 The solution must support Email Logging and Reporting-Data archiving, Extensive Layer 8 Identity-based reporting – Top spam receivers, senders, applications of spam Real-time logs and reports				
10.8 The Anti-Spam application must include IP reputation blocking based on an online service to avoid false positives				
10.9 The solution must support Filter based on message header, size, sender, recipient				
10.10 The solution must have Recurrent pattern detection (RPD) Technology to automated antispam protection based on distribution pattern, Extracts and analyzes relevant message patterns, Blocks attachment-based spam – PDF, XL, MP3 etc. and Content agnostic, multi-language, multi-format antispam protection (Blocks foreign language, image spam)				
11. Email Protection and Control				**20**
11.1 Email security application must offer comprehensive email security, covering all email protocols – SMTP, POP3 and IMAP – and eliminating the need for investment in other email security solutions.				
11.2 Email security application must have real-time classification and protections based on detected spam outbreaks which are based on patterns and not				

content.				
11.3 The Email security application must include IP reputation blocking based on an online service to avoid false positives				
11.4 Email security application must include a Zero-hour protection mechanism for new viruses spread through email and spam without relying solely in heuristic or content inspection				
11.5 Email security application must block unwanted emails at the Gateway, significantly reducing bandwidth consumption and optimizing network performance				
11.6 Email security application must support Reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology				
11.7 Email security application must support Outbound Spam Protection –protects service providers from recurring incidents of outbound spam in their networks thus avoiding consequences of outbound spam like higher cost of providing service, wastage of operations / IT time, blacklisting of IP addresses, inability to meet SLAs and more, by protecting their server reputation				
11.8 Email security application must support Live Protection -real-time in-the-cloud lookups for the latest threat intelligence				
11.9 Email security application must support Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages				
11.10 Email security application must Prevents Email Data Leakage -blocks email attachments based on Layer 8 identity-based policies with pre-specified file extensions, e.g., .XLS, .EXE, .JPEG to prevent leakage of critical business, financial or design data./ Email Encryption and DLP engine with automatic scanning of emails and attachments for sensitive data				
11.11 Email security application must simplify email management by re-routing or copying incoming email messages containing specific keywords about a project, workgroup or topic to the manager or other specified authorities or server.				
11.12 Email security application must meet Compliance, centralized logging and reporting requirements –allows real-time visibility into email traffic with reports that include top mail users, hosts, applications, senders and recipients, in addition to simplifying audit requests through mail archival.				
11.13 Email security application must support pre-defined and user created/ customized content scanning rules based on a variety of criteria				
11.14 Email security application must support Integrated MTA (Message Transfer Agent) to store-and-forward mail in the event servers are unavailable				
11.15 Email security application must support Pre-packaged sensitive data type content control lists				

(CCLs) for PII, PCI, HIPAA, and more,				
11.16 Email security application must detects phishing URLs within e-mails				
11.17 Email security application must support appending of signature automatically to all outbound messages and Accept, reject or drop over-sized messages				
12. Networking				**15**
12.1 Failover - Automated Failover/Failback, Multi-WAN failover, 3G, Modem failover				
12.2 Solution must support gateway high availability and load sharing with state synchronization				
12.3 IP Address Assignment - Static, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP server, DHCP relay				
12.4 Policy routing based on Application and User				
12.5 Routing: static, multicast (PIM-SM) and dynamic (RIP v1& v2, OSPF, BGP, Multicast Forwarding, OSPF)				
12.6 IPv6 support with tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec				
12.7 Country blocking by geo-IP with simple country and continent selections				
12.8 Per-rule and policy based routing by source, destination, user/group or layer-4 service				
12.9 Protocol independent multicast routing with IGMP snooping				
12.10 WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rules				
12.11 Full configuration of DNS, DHCP and NTP				
12.12 Bridging with STP support and ARP broadcast forwarding				
12.13 Supports USB port, 3G, 4G/LTE and WiMAX connectivity				
13. Virtual Private Network (VPN)				**20**
13.1. The Solution must support Layer 8 Identity-based Reporting- Reporting with username and multi-reporting options (on-appliance reporting, centralized reporting….				
13.2 The Solution must offers the option of IPSec VPN, L2TP, PPTP and SSL VPN to provide secure remote access to TUK.				
13.3 The Solution must communicate with most third party VPNs, making it compatible with existing network infrastructures and providing secure access with remote workers, partners, suppliers and customers				
13.4 The Solution must Establish road warrior, Net-to-Net, Host-to-Net VPN connections				
13.5 Solution must support automatic failover of VPN connectivity for IPSec and L2TP connections across multiple ISP gateways				
13.6 The Solution must support Network				

authentication and encryption through DES, 3DES and AES				
13.7 Encryption: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (up to 2048 Bit), DH groups 1/2/5/14, MD5 and SHA-256/384/512				
13.8 The Solution must support Web, application and client-based access modes to Eliminate the need to install VPN clients over individual devices				
13.9 The Solution must support Layer 8 Identity-based VPN Access-Identity and work profile-based access policies to employees, partners, customers (Control over 'Who Accesses What')				
13.10 The Solution must have On-appliance SSL VPN				
13.11 The Solution must support Threat-Free Tunneling Technology to Scan IPSec, L2TP, PPTP, SSL VPN traffic for malware, spam, inappropriate content and intrusions				
13.12 The solution must Support multiple Authentication schemes - Active Directory, LDAP, RADIUS…				
13.13 The Solution must support at least the following Diffie-Hellman Groups: Diffie Hellman Groups - 1,2,5,14,15,16,19,20				
13.14 The Solution must support data integrity with md5, sha1 SHA-256, SHA-384 and AES-XCBC				
13.15 The Solution must support unlimited clientless SSL VPNs for remote access.				
13.16 The Solution must support Authentication: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token and XAUTH				
13.17 The Solution must support Encryption - 3DES, DES, AES, Twofish, Blowfish, Serpent				
The Solution must support IPSec NATTraversal				
13.18 Remote access: SSL, IPsec, iPhone/iPad/Cisco/Andriod VPN client support				
Support Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key				
13.19 Intelligent split-tunneling for optimum traffic routing				
13.20 Supported platforms: Windows 2012 Server 64-bit ,Windows 7 32/64-bit, Windows 10, Linux,Mac OS and newer versions				
13.21 Multi-layered Client Authentication - Certificate, Username/Password, Preshared key, Digital certificates				
13.22 Support flexible Administrative controls - Session timeout, Dead Peer Detection, Portal customization				
14. Instant Messaging (IM) Management (Archiving & Controls)				**10**
14.1 Compatible with current Messengers and Custom Alerts				
14.2 Virus Scanning for IM traffic				
14.3, identity- and group-based policies to control: File transfer, Voice chat, Video chat, one-to-				

one/group chat, Allow/Block Login				
14.4 Content-based blocking				
14.5 Support Reports based on time, users, keywords used in chat				
14.6 support IM Layer 8 Identity-based activities Log				
14.7 support Archives IM activity				
14.8 support Keyword-based chat filtering, Eg. Social Security and Credit Card Numbers, etc.				
14.9 must Control who chats with whom through whitelists and blacklists				
14.10 support Customized alerts				
15. Bandwidth Management				**10**
15.1 Application and User Identity based Bandwidth Management				
15.2 Should provide WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rules				
15.3 support granular Layer 7 and Layer 8 Bandwidth Allocation and controls - Prioritizes business-critical applications and users for bandwidth allocation; Prioritization based on source, destination, user, service, service group				
15.4 support Multiple WAN link bandwidth Logging & reporting				
15.5 Support Guaranteed & Burstable bandwidth policy				
15.6 supports bandwidth requirement for Cloud, SaaS				
15.6. Web Category-based Allocation-Bandwidth allocation based on website categories: webmail, social media, gaming, entertainment etc. including Upload/ download limits				
15.7 Layer 8 Identity-based policies with category-based allocation and bandwidth restriction				
15.8.Time-based Allocation- Bandwidth scheduling by time of the day and Committed bandwidth to business-critical applications during scheduling				
16. Virtualized Environment Security				**10**
16.1 The solution must offer Protection in virtual environments –offer inter-VM traffic scanning along with granular firewall and security policies enforcement, eliminating the blind spots created by hardware security appliances in virtual networks.				
16.2 The solution must support threat-free traffic and security from vulnerabilities in the virtualized web applications.				
16.3 The solution must support centralized management and logging and reporting				
16.4 The solution must allow role-based administration allowing separation of duties In case of collapsed DMZ.				
16.5 The solution must allow administrators to segment Hypervisor Management Console into the DMZ and route all traffic through the virtual security for security against hypervisor				

vulnerabilities.				
17. User Authentication				**10**
17.1 support local user database to allow user authentication and authorization without the need for an external device				
17.2 support Captive Portal -Automatic Windows Single Sign On				
17.3 support for External LDAP/RADIUS database integration - External Authentication for Users and Administrators				
Support Multiple Authentication servers- .Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+				
17.4 support Thin Client and RSA SecurID				
17.5 support User/MAC Binding				
17.6 support Transparent, proxy authentication (NTLM) or client authentication				
17.7 support Client authentication agents for Windows, Mac OS X, Linux 32/64				
17.8 support Two factor authentication (one-time password support) for IPSec and SSL VPN, user portal, and Webadmin				
17.9 Authentication services for IPSec, L2TP, PPTP, SSL				
17.10 Authentication certificates for iOS and Android				
18. General Administration & System Management				**15**
18.1 All security applications must be managed from the central console.				
18.2 The solution must provide the option to save the entire policy or specific part of the policy.				
18.3 The solution must have a security policy verification mechanism prior to policy installation.				
18.4 The solution must support Configuration change tracking				
18.5 The solution must support Advanced trouble-shooting tools in GUI (e.g. Packet Capture)				
18.6 The solution must include the ability to centrally distribute and apply new gateway software versions				
18.7 The solution must include a tool to centrally manage licenses of all gateways controlled by the management station				
18.8 The solution must have the capabilities for multi-domain management and support the concept of global security policy across domains.				
18.9 The Log Viewer should have the ability view all of the security logs (fw,IPS ,urlf...) in one view pane (helpful when troubleshooting connectivity problem for one IP address)				
18.10 The solution must support automated firmware update notification with easy automated update process and roll-back features				
18.11 The solution must support reusable system				

object definitions for networks, services, hosts, time periods, users and groups, clients and servers				
18.12 The solution must offer support for SNMP and Netflow, NTP, SNMP(v1, v2c, v3)				
18.13 The solution must support backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly				
18.14 The solution must offer High Availability (HA) support clustering 2 devices in active-active or active-passive with State Synchronization mode.				
18.15 The solution must support role-based access control and administration				
18.16 The solution must support Email or SNMP trap notification options				
19. Logging & Monitoring				**20**
19.1 The central logging must be part of the management system.				
19.2 The solution must have the ability to log all integrated security applications on the gateway and including Firewall, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti–Spam, User Identity, Data Loss Prevention, Mobile Access, System and Admin Events……				
19.3 The solution must include an automatic packet capture mechanism for IPS events to provide better forensic analysis				
19.4 The solution must have the ability to log all rules (+30k logs/sec)				
19.5 Log viewer must have an indexed search capability				
19.6 The solution must provide different logs for regular user activity and management related logs				
19.7 The solution must include the option to dynamically block an active connection from the log graphical interface without the need to modify the rule base				
19.8 The solution must support exporting logs in database format				
19.9 The solution must include a graphical monitoring interface that provides an easy way to monitor gateways status				
19. The solution must support automatic switch of the log file, based on a scheduled time or file size				
19.11 The solution must support adding exceptions to IPS enforcement from the log record				
19.12 The solution must be able to associate a username and machine name to each log record.				
19.13 For each match rule or type of event Solution must provide at least the following event options: Log, alert, SNMP trap, email and execute a user defined script				
19.14 The solution must provide the following system information for each gateway: OS, CPU usage, memory usage, all disk partitions and % of free hard disk space.				
19.15 The solution must be able to recognize malfunctions and connectivity problems, between two points connected through a VPN, and log and alert when the VPN tunnel is down.				

19.16 The solution must include the status of all VPN tunnels, site-to-site and client-to-site				
19.17 The solution must include customizable threshold setting to take actions when a certain threshold is reached on a gateway. Actions must include: Log, alert, send an SNMP trap, send an email and execute a user defined alert.				
19.18 The solution must include preconfigured graphs to monitor the evolution in time of traffic and system counters: top security rules, top P2P users, vpn tunnels, network traffic and other useful information. Solution must provide the option to generate new customized graphs with different chart types				
19.19 The solution must include the option to record traffic and system views to a file for later viewing at any time.				
19.20 The solution must support Graphical real-time and historical monitoring Email notification of reports, gateway status, viruses and attacks				
20. Logging and Reporting				**10**
20.1 Hundreds of on-box drilldown and compliance reports with custom report options: Multiple Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Search Engines, Web Servers, FTP), Network & Threats (IPS, ATP, Wireless, Security Heartbeat), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)				
20.2 Automated Report scheduling to multiple recipients by report group with flexible frequency options and Multi-format reports				
20.3 Export reports as HTML, PDF, Excel (XLS)				
20.4 Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks				
20.5 Customized log viewer refresh period and color coded log lines for easy trouble-shooting*				
20.6 Log retention customization by category				
20.7 Report anonymization and bookmarks				
20.8 Historical and Real-time Reports - Security, Virus, Spam, Traffic, Policy violations, VPN, Search Engine keywords				
21. Event Correlation and Reporting				**20**
21.1 Solution must include a tool to correlate events from all the gateway features and third party devices				
21.2 Solution must allow the creation of filters based on any characteristic of the event such as security application, source and destination IP, service, event type, event severity, attack name, country of origin and destination, etc.				
21.3 The application must have a mechanism to assign these filters to different graph lines that are updated in regular intervals showing all events that matches that filter. Allowing the operator to focus on the most important events.				

21.4 The event correlation application must supply a graphical view events based on time.				
21.5 Solution must show the distribution of events per country on a map.				
21.6 Solution must allow the administrator to group events based on any of it characteristics, including many nesting levels and export to PDF.				
21.7 Solution must include the option to search inside the list of events, drill down into details for research and forensics.				
21.8 In the event list view Solution must include the option to automatically generate small graphs or tables with the event, source and destination distribution.				
21.9 Solution must detect Denial of Service attacks correlating events from all sources.				
21.10 Solution must detect an administrator login at irregular hour				
21.11 Solution must support credential guessing attacks detect				
21.12 Solution must report on all security policy installations.				
21.13 Solution must include predefined hourly, daily, weekly and monthly reports. Including at least Top events, Top sources, Top destinations, Top services, Top sources and their top events, Top destinations and their top events and Top services and their top events.				
21.14 The reporting tool must support at least 25 filters that allow to customize a predefined report to be closest to administrator's needs				
21.15 Solution must support automatic reports scheduling for information that need to extract on regular basis (daily, weekly, and monthly). Solution must also allow the administrator to define the date and time that reporting system begins to generate the scheduled report.				
21.16 Solution must support the following reports formats: HTML, CSV and MHT				
21.17 Solution must support automatic report distribution by email, upload to FTP/Web server and an external custom report distribution script				
22. Data Loss Prevention (DLP)/ Data Leakage Prevention (DLP)				**10**
22.1 Vendor should have an option of a fully integrated Data Loss Prevention application				
22.2 DLP policies should have the option of being central managed with all other security applications				
22.3 DLP application should have the mechanism for end user self-incident handling				
22.4 DLP application should have the option to manage over 500 pre-defined data types.				
22.5 Email Leakage Prevention –enables TUK to implement Identity-based policies to block attachments and forward email copies of departing and pre-specified users to their managers and IT security.				
22.6 Web Leakage Prevention – prevents file				

upload over HTTP, Web mail, FTP, P2P and other file sharing applications based on username and work profile.				
22.7 Instant Messenger Leakage Prevention –blocks chat conversations based on pre-specified keywords and file transfer over IM in accordance with Human Layer 8 Identity-based policies.				
22.8 Encrypted HTTPS/SSL Protocol Leakage Prevention –controls file upload over HTTPS/SSL websites, preventing misuse of this encrypted medium in the form of unauthorized transfer of sensitive data.				
22.9 Logging and Reporting – Human Layer 8 Identity-based logging and reporting includes chat logs which help in monitoring and taking corrective action. The extensive logs and reports support CIPA, HIPAA, PCI DSS regulatory compliance.				
22.10 must offer centralized reporting.				
23. Multiple Link Management				**5**
23.1 The solution must supports WAN redundancy and delivers assured WAN availability and reliable connectivity.				
23.2 The solution must supports Automated Load Balancing by Automatically distributing traffic over multiple links, Weighted round robin load balancing of links and supporting the routing of traffic based on speed and cost of WAN link				
23.3 The solution must supports Layer 8 Identity-based Routing- Defines routing path based on User, Source, IP, Protocol				
23.4 The solution must supports Automatic Link Failover by Automatic detection of failed WAN link and routing to working link and performing Multiple test methods to detect failure to reach applications, Eg. Inventory Management, ERP, CRM				
23.5 The solution must supports configuration of 3G and WiMAX as back-up or primary links for WAN redundancy and Elimination of the risk of wireline outages				
24. Regulatory Compliance				**10**
24.1 Vendor must have a fully integrated Compliance appliance				
24.2 Vendor must have an option for Real Time Compliance Monitoring across all security services in the product				
24.3 Vendor must have an option for Instant notification on policy changes impacting compliance				
24.4 Vendor must have an option to recommend Security Best Practices				
24.5 Vendor must have an option to Translate regulatory requirements into actionable security best practices				
24.6 Vendor must have an option to Monitor constantly gateway configuration with the security best practices				
24.7 Vendor must have an option to Generate automated assessment reports for compliance rating				

with top regulations CE / FCC / UL				
24.8 The Children's Internet Protection Act (CIPA) Compliant				
24.9 The Health Insurance Portability and Accountability (HIPAA)				
24.10 Payment Card Industry Data Security Standard (PCI DSS)				
25. Certification				**5**
25.1 ICSA Labs Firewall – Corporate				
25.2 Checkmark UTM Level 5 Certification				
25.3 VPNC- Basic and AES interoperability				
25.4 IPv6 Ready				
26. Provisioning and Monitoring				**10**
26.1 The solution must provide centralized administration and security provisioning of the devices.				
26.2 The solution must provide an intuitive and easy-to-use security management console to centrally manage device configurations such as operating system and network settings.				
26.3 The administrators should be able to automate device configuration and easily roll out changes to settings to multiple, geographically distributed devices, via a single security management console				
26..4 The Administrators should manage security provisioning by defining profiles for common security policies and device settings, which can then be used to manage hundreds and thousands of devices using the same policies				
26.5 The solution should present a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events				
26.6 The solution should generate detailed or summary graphs and charts for analysis of traffic patterns, audit and estimate costs of network use, identify departments and users that generate the most traffic, and detect and monitor suspicious activity.				
27. Installation				**3**
The appliance should be able to fit into any make or type of cabinet, indicate how.				
28. Hardware Specifications				**5**
28.1 Memory 6GB				
28.2 HDD (HOT Swappable) 250GB				
29. Power				**5**
Input Voltage ……. 100–240V AC, …… 60–50 Hz				
Redundant Power Supply…… Yes				
30. Support				**7**
Comprehensive Support Plan (3 Years)				

SUMMARY OF REQUIREMENTS

System Components

	Technical Specifications	*Cost (Ksh)*
1	**Security Appliances (UTM) Qty:1** *Should be able to support at least* 8x1 GbE Copper interfaces 8x1 GbE SFP(Mini GBIC) Ports 2x10 GbE SFP(Mini GBIC) Ports Minimum 6 GB RAM on appliance AC or DC hot-swappable power supplies Hot-swappable 250GB HDD 30 Gbps firewall throughput	
2	**Centralized Security Management Server/Platform Qty:1** Network Policy Management Endpoint Policy Management Logging and Status Monitoring User Directory Compliance Event Report	
3	**Training of at least TWO Network Security administrators**	
4	**3 year Licenses and Direct manufacturer warranty**	
	Note: Any further clarifications regarding the technical aspects of this tender should be made in writing to director.dicts@tukenya.ac.ke	

SECTION V – PRICE SCHEDULE OF REQUIREMNTS

IMPORTANT: Please note that your technical bid should not contain the form of tender and the price schedule form otherwise you will be automatically disqualified.

SUBMISSION OF FINANCIAL BID (THIS SHOULD BE SEPERATE FROM THE TECHNICAL BID)

1. Fill, sign and rubberstamp the form of tender.
2. Fill, sign and rubberstamp the price schedule form.

Note: The technical bid containing the bid security should be in its own envelope and the financial bid (form of tender and price schedule form) should be in its own envelope. The technical bid envelope and the financial bid envelope should be sealed in one big envelope during submission of the tender.

S/No	Description	Total Cost VAT Inclusive (Kshs)	Delivery Period in Days
1.	**TENDER FOR SUPPLY, INSTALLATION, CONFIGURATION & COMMISSIONING OF UNIFIED THREAT MANAGEMENT (UTM) NETWORK SECURITY APPLIANCE**		

Bidder's Signature ---------- Official Stamp ----------

Date ----------

Note:

1. In case of discrepancy between unit price and total, the unit price shall prevail.

Date:

Tender Number and Name:

To:

The Technical University of Kenya

P.O.BOX 502428-00200,

NAIROBI-KENYA.

TEL:+254(020) 338232/338755/219690

Dear Sirs and Madams,

Having read, examined and understood the Tender Document including all Addenda, receipt of which we hereby acknowledge, we, the undersigned Tenderer, offer to provide ……*(insert services description*) for the sum of……(*total tender price in words and figures*) or such other sums as may be ascertained in accordance with the schedule of prices inserted by me/ us above.

Name of Tenderer

_____

Name and Capacity of authorised person signing the Tender

_____

Signature of authorised person signing the Tender

_____

Stamp of Tenderer

_____

SECTION VI - SUMMARY OF EVALUATION PROCESS

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

a. MANDATORY REQUIREMENTS EVALUATION CRITERIA (must provide all the mandatory requirements)
b. TECHNICAL REQUIREMENTS EVALUATION CRITERIA and Visitation(site) evaluation
c. FINANCIAL EVALUATION
d. COMBINED SCORE EVALUATION

6.1 MANDATORY REQUIREMENTS: *The mandatory information below MUST be provided. Any failure to provide ANY of the information under Mandatory requirements will lead to disqualification from further evaluation.*

No.	MANDATORY EVALUATION CRITERIA	Yes/No
1	Tender Security – Bank Guarantee or from an Insurance Company (All from acceptable and approved locally based Kenyan institutions)	
2	Copy of Company or Firm's Registration Certificate	
3	Copy of Valid Tax Compliance Certificate	
4	Copy of Receipt for purchase of tender document (Free download)	
5	Audited Financial Accounts for the year 2015 OR 2016 duly signed by your Auditing firm and Stamped	
6	Show evidence that your Company has an experience of at least 4 years in the provision of networks/data center security solutions in the market	
7	Submit the specific product brochure/proposed technical solution specifications for our confirmation that it conforms to all the outlined technical specifications	
8	Submit a minimum of **2 reference sites** where you have implemented network or Data center security solutions. Provide the names of the organizations, contact persons and their telephone numbers and the nature of the job undertaken for that organization	
9	Submit at least 2 recommendation letters from companies for which you have undertaken for them similar data security and network	

	solutions- Mandatory.	
10	Submit the company's Manufacturers/dealership authorization letter	
11	Submit their valid network certifications (Attach their professional certifications) and product certification for the proposed 2 implementation team members - This is Mandatory.	

NOTE: THE ABOVE MANDATORY REQUIREMENTS MUST BE PROVIDED

6.2 TECHNICAL EVALUATION

S/NO.	TECHNICAL EVALUATION CRITERIA	MARKS ALLOCATED
1	Written confirmation on Terms Of Payment Of 30 Days Credit Period on the Firms Letterhead	**2**
2	Duly completed Form of Tender stamped and signed & Schedule of requirements duly filled indicating items offered and their prices.	**2**
3	Duly completed Declaration Form stamped and signed	**2**
4	Confidential Business Questionnaire (CBQ) duly filled stamped and signed	**2**
5	Three Recommendation Letters and Three Copies of LPOs or Contracts from different Corporate organizations where you have supplied a similar product	**2**
6	Submit your company profile.	**2**
7	Submit the technical qualifications / professional experience of at least 2 proposed technical implementation team as proof of competency in undertaking the assignment if awarded the tender.	**2**
8	The proposed technical implementation team must have a minimum of 3 years' experience in similar assignments	**2**

	related to the product (Submit their respective CV's and respective academic qualifications).	
9	Provide your project implementation plan (Indicate your delivery period and submit your installation schedule.	**2**
10	Indicate your support services on Installation on the network environment for a period of 3 years and also you're after sales support charges if applicable	**2**
11	Submit your project methodology for carrying out the assignment if awarded the tender.	**2**
	Subtotal Marks	**22 MARKS**

	SPECIFICATIONS TECHNICAL REQUIREMENTS	**MARKS ALLOCATED**
1	**Interfaces**	**10**
2	**System Performance**	**20**
3	**Firewall**	**20**
4	**Intrusion Prevention System (IPS)**	**15**
5	**Identity Awareness**	**5**
6	**Application Protection, Control and Filtering**	**25**
7	**Web Application Protection, Control and Filtering**	**25**
8	**Anti-Bot**	**5**
9	**Gateway Anti-Virus & Anti-Spyware**	**10**
10	**Gateway Anti-Spam**	**10**
11	**Email Protection and Control**	**20**
12	**Networking**	**15**
13	**Virtual Private Network (VPN)**	**20**
14	**Instant Messaging (IM) Management (Archiving & Controls**	**10**
15	**Bandwidth Management**	**10**
16	**Virtualized Environment Security**	**10**
17	**User Authentication**	**10**

18	**General Administration & System Management**	**15**
19	**Logging & Monitoring**	**20**
20	**Logging and Reporting**	**10**
21	**Event Correlation and Reporting**	**20**
22	**Data Loss Prevention (DLP)/ Data Leakage Prevention (DLP)**	**10**
23	**Multiple Link Management**	**5**
24	**Regulatory Compliance**	**10**
25	**Certification**	**5**
26	**Provisioning and Monitoring**	**10**
27	**Installation**	**3**
28	**Hardware Specifications**	**5**
29	**Power**	**5**
30	**Support**	**7**
		387

Minimum technical specifications of the system which should be at 90%

THE TECHNICAL EVALUATION TOTAL MARKS: 90%

NOTE: ***PASS MARK BEFORE PROCEEDING TO THE FINANCIAL EVALUATION = 90%***

The maximum score under technical evaluation is 100%. Bidders must score at least 90% under technical evaluation to proceed to the next stage *(Due Diligence/Post qualification).*

Bidders **MUST** score at **least 90%** in the compliance to technical specifications section to proceed to the next stage. 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. The "boxes" in the compliance table shall be checked, "√", as appropriate and each row shall be awarded scores.**

Technical evaluation has several aspects and below is the criteria to be used:

5.5.3 DUE DILIGENCE/POST QUALIFICATION.

The maximum score under this stage of evaluation is 20%. Bidders **MUST** score at least 18% to proceed to the next stage, (*Financials).*

Due diligence will be undertaken through site visits to the bidders' reference sites in order to confirm the authenticity of the sites and the scope of work done in relation to this project amongst other criteria stipulated below. At **least two sites** will be visited (for each site 10 marks). The scores will be spread out as follows:

No.	Criteria	Maximum Score
1	Authenticity of the site provided. **If authenticity for any provided site is established to be false, the bidder will score zero for Due Diligence/ Post Qualification section.**	2
2.	Proof of the scope of work carried out in relation to this tender.	2
3.	Proof of completion of work on site.	2
4.	Team involved in the implementation.	2
5.	Client satisfaction on the deployment and post implementation support. Issue to do with project timelines, deliverables, support and general performance of the contractor will be examined.	2
	TOTAL	**10**

Bidders **MUST** score at least 18% to proceed to the next stage, *Financials.*

6.3 PART III – FINANCIAL EVALUATION

This will include the following: -

A) CONFIRMATION OF AND CONSIDERING PRICE SCHEDULE DULY COMPLETED AND SIGNED
B) CHECKING THAT THE TENDERER HAS QUOTED PRICES BASED ON VAT INCLUSIVE.
c) CORRECTION OF ARITHMETICAL ERRORS,

After all the above have been confirmed,

D) CONDUCTING A FINANCIAL COMPARISON.

E) **COMBINED SCORE**

The Successful Tenderer shall be the lowest evaluated bidder.

NOTES: -

1. For purposes of evaluation, the exchange rate to be used for currency conversion shall be the selling exchange rate ruling 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 goods it offers to supply.

SUBMISSION OF FINANCIAL BID (THIS SHOULD BE SEPERATE FROM THE TECHNICAL BID)

IMPORTANT: Please note that your technical bid should not contain the form of tender and the price schedule form otherwise you will be automatically disqualified.

1. Fill, sign and rubberstamp the form of tender.

2. Fill, sign and rubberstamp the price schedule form.

Note: The technical bid containing the bid security should be in its own envelope and the financial bid (form of tender and price schedule form) should be in its own envelope. The technical bid envelope and the financial bid envelope should be sealed in one big envelope during submission of the tender.

SECTION VII- FORM OF TENDER

Date
Tender No.

To: The Vice Chancellor
The Technical University of Kenya
P. O Box 52428 – 000200
NAIROBI.

Gentlemen and/or Ladies:

1. Having examined the tender documents including Addenda Nos. ……. *[Insert numbers]*.the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver (…… (*insert equipment description*) in conformity with the said tender documents for the sum of …… (*total tender amount in words and figures*) or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Tender.

2. We undertake, if our Tender is accepted, to deliver install and commission the equipment in accordance with the delivery schedule specified in the Schedule of Requirements.

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

4. We agree to abide by this Tender for a period of …… [*number]* days from the date fixed for tender opening of the Instructions to tenderers, 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 constitute a Contract, between us. Subject to signing of the Contract by the parties.

6. We understand that you are not bound to accept the lowest or any tender you may receive.

Dated this day of 20

[Signature] [In the capacity of]

Duly authorized to sign tender for an on behalf of

SECTION VIII-CONFIDENTIAL BUSINESS QUESTIONNAIRE FORM

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

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

Part 1 – General:

Business Name ……..

Location of business premises. ……..

Plot No…… Street/Road ……..

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

Nature of Business ,……..

Registration Certificate No. ……

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

Name of your bankers …….. Branch ……

	Part 2 (a) – Sole Proprietor Your name in full …….. Age …….. Nationality …… Country of origin ……. • Citizenship details …… . •
	Part 2 (b) Partnership Given details of partners as follows: Name Nationality Citizenship Details Shares 1. …… 2. …… 3. …… 4. ……
	Part 2 (c) – Registered Company Private or Public ……. State the nominal and issued capital of company- Nominal Kshs. …… Issued Kshs. …… Given details of all directors as follows Name Nationality Citizenship Details Shares 1

	…… 2. …… 3. …… 4. …… 5 ……
Date …….. Signature of Candidate ……..	

- If a Kenya Citizen, indicate under "Citizenship Details" whether by Birth, Naturalization or registration.

SECTION IX-TENDER SECURITY FORM

Whereas ……. [*name of the tenderer]*

(hereinafter called "the tenderer") has submitted its tender dated ……. [*date of submission of tender]* for the supply, delivery installation and commissioning of ……*[name and/or description of the equipment]*

(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 …….. [*name of Procuring entity}* (hereinafter called "the Procuring entity") in the sum of …….. for which payment well and truly to be made to the said Procuring entity, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Common Seal of the said Bank this day of 20 .

THE CONDITIONS of this obligation are:-

1. If the tenderer withdraws its Tender during the period of tender validity specified by the tenderer on the Tender Form; or

2. If the tenderer, having been notified of the acceptance of its Tender by the Procuring entity during the period of tender validity:

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

We undertake to pay to the Procuring entity up to the above amount upon receipt of its first written demand, without the Procuring entity having to substantiate its demand, provided that in its demand the Procuring entity will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This 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 above date.

[Signature of the bank]

(Amend accordingly if provided by Insurance Company)

SECTION X- PERFORMANCE SECURITY FORM

To: The Vice Chancellor
The Technical University of Kenya
P. O Box 52428 – 000200
NAIROBI.

WHEREAS …… [*name of tenderer*] (hereinafter called "the tenderer") has undertaken , in pursuance of Contract No. _____ [*reference number of the contract]* dated _____ 20 _____ to supply …… [*description of goods]* (hereinafter called "the Contract").

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

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

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the tenderer, up to a total of ……. [*amount of the guarantee in words and figure]* and we undertake to pay you, upon your first written demand declaring the tenderer to be in default under the Contract and without cavil or argument, any sum or sums within the limits of …….. [*amount of guarantee]* as aforesaid, without 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 _____

Signed and seal of the Guarantors

_____

[Name of bank or financial institution]

_____

[Address]

_____

[Date]

SECTION XI-BANK GUARANTEE FOR ADVANCE PAYMENT FORM

To: The Vice Chancellor
The Technical University of Kenya
P. O Box 52428 – 000200
NAIROBI.

[Name of tender] ……..

Gentlemen and/or Ladies:

In accordance with the payment provision included in the Special Conditions of Contract, which amends the General Conditions of Contract to provide for advance payment, ……. [*Name and address of tenderer]*(hereinafter called "the tenderer") shall deposit with the Procuring entity a bank guarantee to guarantee its proper and faithful performance under the said Clause of the Contract in an amount of …… ……. [*amount of guarantee in figures and words]*.

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

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

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

Yours truly,

Signature and seal of the Guarantors

[Name of bank or financial institution]

[Address]

[Date]

SECTION XII- DECLARATION FORM

Date _____

To:

The Technical University of Kenya

P.O.BOX 502428-00200,

Nairobi-Kenya.

TEL:+254(020) 338232/338755/219690

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 any body, 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 Bidders.

e) That I/ We are not associated with any other Tenderer participating in this Tender.

f) 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.

Yours sincerely,

_____

Name of Tenderer

_____

Signature of duly authorised person signing the Tender

_____

Name and Capacity of duly authorised person signing the Tender

_____

Stamp or Seal of Tenderer

_____

Stamp or Seal of Tenderer

SECTION III-DRAFT LETTER OF NOTIFICATION OF AWARD

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

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 but not later than thirty (30) days after expiry of tender validity pursuant to the provisions of the Public Procurement and Disposal Act, 2005 *(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 TECHNICAL UNIVERSITY OF KENYA

DIRECTOR SUPPLY CHAIN OPERATIONS.

Enclosures

SECTION XIV-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 Procurement *Department , The Technical University of Kenya, Nairobi* only after expiry of twenty five (25) days from the date hereof. It is expected that by that time TUK and the successful bidder will have entered into a contract pursuant to the Public Procurement and Disposal Act, 2005 *(or as may be amended from time to time or replaced).* When collecting the Security, you will be required to produce the original 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 TECHNICAL UNIVERSITY OF KENYA

DIRECTOR SUPPLY CHAIN OPERATIONS.

SECTION XV-CONTRACT AGREEMENT FORM

THIS AGREEMENT made this**……**day of**…….**20**….BETWEENTHE TECHNICAL UNIVERSITY OF KENYA** of Post Office Box Number 52428, -00200, Nairobi in the Republic aforesaid *(hereinafter referred to as the "TUK")* of the one part,

AND

…….. (*Supplier'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**…….*(full address of Supplier)***in the Republic aforesaid, *(hereinafter referred to as the "Supplier")* of the other part;

WHEREAS TUK invited tenders for certain goods, that is to say for **……(TUK *insert description of goods*)** under Tender Number**…….. (*insert tender number*)**

AND WHEREAS TUK has accepted the Tender by the Supplier for the goods in the sum of **……(TUK *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 there-under.

   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 *"Supplier"* the covenants, agreements obligations expressed to be made or performed by the Supplier 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 *"Supplier"* any act default or omission by the Supplier 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 TUK to the Supplier as hereinafter mentioned, the Supplier hereby covenants with TUK to supply the goods and remedy any defects thereon in conformity in all respects with the provisions of the Contract.

4. TUK hereby covenants to pay the Supplier in consideration of the proper supply of the goods 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 TUK and the Supplier 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 Supplier and agreed upon with TUK
e) the Technical Specifications as per TUK's Tender Document
f) the Schedule of Requirements
g) TUK's Notification of Award dated……
h) the Tender Form signed by the Supplier
i) the Declaration Form signed by the Supplier/ successful Tenderer
j) the Warranty

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 TUK and the Supplier.
b) Issuance of the Performance Bond by the Supplier and confirmation of its Authenticity by TUK.
c) Issuance of the Official Order by TUK to the Supplier.
d) Where applicable, Opening of the Letter of Credit by TUK.

8. The period of contract validity shall begin from the Commencement date and end on -
a) sixty (60) days after the last date of the agreed delivery 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 Supplier 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 TUK shall operate as a waiver of that right, power or remedy and no single or partial exercise of any other right, power or remedy shall operate as a complete waiver of that other right, power or remedy.

12. Notwithstanding proper completion of delivery 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 and facsimile shall be deemed to be served one day after the date of such transmission and delivery respectively (*and proof of service shallbe by way of confirmation report of such transmission and or delivery*), 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 (Kenyan) Suppliers and five (5) days for Foreign Suppliers.

14. For the purposes of Notices, the address of TUK shall be **The Vice Chancellor, the Technical University of Kenya, P. O Box 52428 – 00200, NAIROBI.** The address for the Supplier shall be the Supplier'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 **TUK**

_____
COMPANY SECRETARY

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

_____ _____
DIRECTOR *Affix Supplier's Seal here*

_____
DIRECTOR'S FULL NAMES

and in the presence of:-

_____
DIRECTOR/ COMPANY SECRETARY

_____
DIRECTOR/ COMPANY SECRETARY'S FULL NAMES

*OR

SIGNED BY and on BEHALF

of the **SUPPLIER**

_____

SIGNATURE OF THE SUPPLIER

_____

FULL NAMES OF THE SUPPLIER

***NOTES TO THE SUPPLIER**

1. *Please note that the alternative is applicable IF AND ONLY IF the Supplier is not a registered company but has tendered, and, is trading as a sole proprietor or a partnership as provided in the Confidential Business Questionnaire or is registered as a business name.*

2. *In all other cases, the Supplier is required to execute the contract as first provided.*

SECTION XVI-MANUFACTURER'S AUTHORIZATION FORM

(To Be Submitted On Manufacturer'sLetterhead)

To: The Technical University of Kenya

P.O.BOX 502428-00200,

Nairobi-Kenya.

TEL:+254(020) 338232/338755/219690

WHEREAS WE ……(*name of the manufacturer*) who are established and reputable manufacturers of ……
(*name and description of the goods*) having factories at ……*(full address and physical location of factory(ies) where goods to be supplied are manufactured)* do hereby confirm that ……
(*name and address of Supplier*) is authorized by us to transact in the goods required against your Tender …… (*insert reference number and name of the Tender*) in respect of the above goods manufactured by us.

WE HEREBY extend our full guarantee and warranty as per the Conditions of Contract for the goods offered for supply 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.

_____

Name and Capacity of duly authorised person signing on behalf of the Manufacturer

NOTES TO TENDERERS AND MANUFACTURERS

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

SECTION XVII-SUPPLIER BUSINESS PREMISE LOCATION AND MOBILE TELEPHONE CONTACT

BUSINESS NAME:	
NAME OF BUILDING AND TOWN/CITY	
STREET OR ROAD	
MOBILE TELEPHONE CONTACT NUMBER	
AREA e.g Industrial Area, Town Center, Westlands etc	