KCA UNIVERSITY

TENDER DOCUMENT

PROCUREMENT OF ICT INFRUSTRUCTURE

TENDER NO. KCAU/ICT INFRASTRUC/01/2022

KCA University
Thika Road, Ruaraka
P.O. Box 56808, 00200 Nairobi.

Tel: (+254 2) 8070408-9
Cell: (+254) 734888022/0710888022

2ND DECEMBER, 2022

CONTENTS

Page

SECTION I – INVITATION TO TENDER

TENDER NAME: PROCUREMENT OF ICT INFRASTRUCTURE

TENDER NO. KCAU/ICT NFRASTR/01/2022

KCA University invites sealed tenders from eligible suppliers for supply, delivery, installation and commissioning of ICT infrastructure **at** the Main Campus in Ruaraka,
Interested eligible Suppliers may get further details from the Procurement Office, KCA University main campus in TPC Building in Thika Road, Ruaraka during normal office working hours i.e. **Monday to Friday between 8.00 a.m. to 1.00 p.m.** and **2.00 p.m. to 5.00 p.m.**

Completed tender documents are to be enclosed in plain sealed envelopes, marked "**Tender for ICT INFRASTRUCTURE**" and deposited in the tender box provided at the reception of KCA University and be addressed as follows: -

The Vice Chancellor & CEO, KCA
University,
Thika Road, Ruaraka P.O.
Box 56808- 00200,
NAIROBI

To be received on or before **12th December 2022 at 11.30am**
Tenders will be opened immediately thereafter in the presence of the tenderers representatives who choose to attend the opening at **KCA University SOB Boardroom at 11.45am** local time.

Dr. Rebecca Mutia, PhD.

MANAGER, PROCUREMENT & STORES

TEL: 0722790837

SECTION II – INSTRUCTIONS TO TENDERERS

TABLE OF CONTENTS. **Page**

SECTION II INSTRUCTIONS TO TENDERERS

2.1 Contents of tender documents

2.1.1. The tender document comprises of the documents listed: -

i) Instructions to tenderers
ii) General Conditions of Contract
iii) Special Conditions of Contract
iv) Schedule of Requirements
v) Details of service
vi) Contract form
vii) Confidential business questionnaire form

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.

2.2 Tender Prices

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

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

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

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

2.2.5 Where contract price variation is allowed, the variation shall not exceed 10% of the original contract price. However, in the event that the provider considers doing so he must initiate a discussion with the University before such variations are effected.

2.2.6 Price variation requests shall be processed by the KCA University within 30 days of receiving the request

2.3 Tenderers Eligibility and Qualifications.

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

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

2.4 Validity of Tenders

2.4.1 Tenders shall remain valid for 60 days or as specified in the invitation to tender after date of tender opening prescribed by the KCA University. A tender valid for a shorter period shall be rejected by the KCA University as nonresponsive.

2.4.2 In exceptional circumstances, the KCA University 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. A tenderer granting the request will not be required nor permitted to modify its tender.

2.5 Sealing and Marking of Tenders

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

(a) be addressed to the KCA University at the address given in the invitation to tender in page 3

(b) bear, tender number and name in the invitation to tender and the words:
"DO NOT OPEN BEFORE **12th December 2022 at 11.30am**"

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

2.5.3 If the outer envelope is not sealed and marked as required by paragraph 2.5.2, the KCA University will assume no responsibility for the tender's misplacement or premature opening.

2.6 Deadline for Submission of Tenders

2.6.1 Tenders must be received by the KCA University at the address specified on page 3 not later than**12th December 2022 at 11.30am.**

2.6.2 The KCA University may, at its discretion, extend this deadline for the submission of tenders by amending the tender documents in accordance with paragraph 2.4.2, in which case all rights and obligations of the KCA University and candidates previously subject to the deadline will thereafter be subject to the deadline as extended.

2.6.3 Bulky tenders which will not fit in the tender box shall be received by the KCA University as provided for in the appendix.

2.7 Opening of Tenders

2.7.1 The KCA University will open all tenders in the presence of tenderers' representatives who choose to attend, **on 12th December 2022 at 11.30am** and in the location specified in the invitation to tender. The tenderers' representatives who are present shall sign a register evidencing their attendance.

2.7.3 The tenderers' names, tender modifications or withdrawals, tender prices, discounts and such other details as the KCA University, at its discretion, may consider appropriate, will be announced at the opening.

2.7.4 The KCA University will prepare minutes of the tender opening which will be submitted to the tenderers that signed the tender opening register and will have made the request.

2.8 Clarification of tenders

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

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

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

2.9. Contacting the KCA University

2.9.1 Subject to paragraph 2.9, no tenderer shall contact the KCA University on any matter relating to its tender, from the time of the tender opening to the time the contract is awarded.

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

2.10 Award of Contract

a) Post qualification

2.10.1 In the absence of pre-qualification, the KCA University 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.

2.10.2 The determination will consider the tenderer's financial and technical capabilities. It will be based upon an examination of the documentary evidence of the tenderer's qualifications submitted by the tenderer, pursuant to paragraph 2.1.2, as well as such other information as the KCA University deems necessary and appropriate.

2.10.3 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 KCA University will proceed to the next lowest evaluated tender to make a similar determination of that tenderer's capabilities to perform satisfactorily.

b) Award Criteria

2.10.4 Subject to paragraph 2.20 the KCA University will award the contract to the successful tenderer whose tender has been determined to be substantially responsive and has been determined to be the lowest evaluated tender, provided further that the tenderer is determined to be qualified to perform the contract satisfactorily.

2.10.5 The KCA University 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 KCA University's action. If the KCA University determines that none of the tenderers is responsive; the KCA University shall notify each tenderer who submitted a tender.

2.10.6 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.

2.11 Notification of award

2.11.1 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.

2.11.2 The notification of award will signify the formation of the Contract subject to the signing of the contract between the tenderer and the KCA University pursuant to clause 2.22 simultaneously the other tenderers shall be notified that their tenders have not been successful.

2.12 Signing of Contract

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

2.12.2 Within fourteen (14) days of receipt of the Contract Form, the successful tenderer shall sign and date the contract and return it to the KCA University.

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

2.13 Corrupt or Fraudulent Practices

2.13.1 The KCA University requires that tenderers observe the highest standard of ethics during the procurement process and execution of contracts.

The KCA University 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;

2.13.2 Further, a tenderer who is found to have indulged in corrupt or fraudulent practices risks being debarred from participating in KCAU Procurement.

APPENDIX TO INSTRUCTIONS TO THE TENDERERS

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

Instructions to tenderers	**Particulars of appendix to instructions to tenderers**
2.3	Eligibility – **Not barred from participating in public tenders**
2.3.1	Particulars of eligibility and qualifications documents of evidence required - see **confidential Business questionnaire and special conditions plus Financial and technical capacity.**

SECTION III GENERAL CONDITIONS OF CONTRACT

3.1 Definitions

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

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

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

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

d) "The KCA University" means the organization sourcing for the services under this Contract.

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

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

g) "SCC" means the special conditions of contract

h) "Day" means calendar day

3.2 Application

These General Conditions shall apply to the extent that they are not superceded by provisions of other part of contract.

3.3 Standards

3.3.1 The services provided under this Contract shall conform to the 9 standards mentioned in the Schedule of requirements on page 15-16.

3.4 Inspections and Tests

3.4.1 The KCA University or its representative shall have the right to inspect and/or to test the services to confirm their conformity to the Contract specifications. The KCA University shall notify the tenderer in writing, in a

timely manner, of the identity of any representatives retained for these purposes.

3.4.2 The inspections and tests may be conducted on the premises of the tenderer or its subcontractor(s). If conducted on the premises of the tenderer or its subcontractor(s), all reasonable facilities and assistance, shall be furnished to the inspectors at no charge to the KCA University.

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

3.5 Payment

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

3.6 Prices

Prices charged by the contractor for services performed under the Contract shall not, with the exception of any Price adjustments authorized in SCC, vary from the prices by the tenderer in its tender or in the KCA University's request for tender validity extension as the case may be. No variation in or modification to the terms of the contract shall be made except by written amendment signed by the parties.

3.7 Assignment

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

3.8 Termination for Default

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

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

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

c) if the tenderer, in the judgment of the KCA University has engaged in corrupt or fraudulent practices in competing for
or in executing the Contract.

In the event the KCA University terminates the Contract in whole or in part, it may procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered.

3.9 Termination for Insolvency

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

3.10 Termination for Convenience

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

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

3.14 Resolution of Disputes

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

If after thirty (30) days from the commencement of such informal negotiations both parties have been unable to resolve amicably a

contract dispute either party may require that the dispute be referred for resolution to the formal mechanisms specified in the SCC.

3.15 Force Majeure

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

3.16 Applicable Law

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

3.17 Notices

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

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

SECTION IV SPECIAL CONDITIONS OF CONTRACT

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

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

General conditions of contract reference	Special conditions of contract
3.5	Specify method and conditions of payment – **30 days after presentation of an invoice and all other relevant documents.**
3.6	Specify price adjustments allowed - only **under written agreement**
3.14	Specify resolution of disputes - through **Chartered Institute of Arbitration Kenya Chapter**
3.16	Specify applicable law – **The laws of Kenya**
3.17	Indicate addresses of both parties - KCAU **physical address is as given on the top page**

SECTION V – SCHEDULE OF REQUIREMENTS FOR TENDER FOR SUPPLY, DELIVERY, INSTALLATION AND COMMISSIONING OF ICT INFRASTRUCTURE

1. Supply, Delivery, Installation, Testing, User Training, and Commissioning of Huawei Fusion Module 800 Smart Small Data Center (6 Cabinets, 16 port KVM Switch with Rack mount monitor) -**1 piece**
   - Fully loaded Huawei Smart Data Center with all accessories including but not limited to – batteries, precision cooling system, environmental control monitors, cameras, cable management, grounding and bonding, civil works, etc.
   - Attach a technical data sheet for the specified data canter.
   - Mandatory site visit on **Tuesday 6th December 2022 at 10.00 am**.

2. Supply, Delivery, Installation/ Mounting, Configuration, Testing, Training of Users and Commissioning of Huawei Ideahub Smart Screens -**5 pieces**

   Distributed as follows:
   i. Main Campus in Ruaraka- 2 pieces
   ii. Town campus- 1 piece
   iii. Kitengela Campus- 1 piece
   iv. Western Campus is Kisumu- 1 piece

Huawei Ideahub Technical Specifications

Category	Specification Requirement	Quantity	Compliance (Y/N)	Bidders Response
General Requirements	**The All-in-one terminal should include the following features:** ➢ **Interactive Panel;** ➢ **Video conference codec;** ➢ **Built-in Speaker;** ➢ **Built-in microphone;** ➢ **Built-in camera.** ➢ **OPS module**			
	System configuration: the terminal should be equipped with at least 8 core CPU, 8 GB RAM, 64GB Flash			
	The terminal should be provided with wall-mount bracket or a movable stand.			

Touch Screen Requirements	**The terminal should have a minimum of *86-inch* DLED touch screen, of 4K60 resolution, with Zerogap bonding**			
	The terminal should support automatic adjusting of screen brightness based on light sensing with antiglare (AG).			
	The terminal should support optical anti-blue light, protects eyes and doesn't change color with the corresponding authentication certificate must be provided.			
	The terminal should have screen protection up to physical toughened Mohs 7			
	The terminal should have a minimum screen response time of 8ms			
	The terminal should have a minimum touch accuracy of ±1mm			
	The terminal should have a minimum of 20 touch points.			
Camera Requirements	**The terminal should have a 4K30 built-in camera with a horizontal viewing angle of 80° and vertical viewing angle of 50°.**			
	The terminal should support a built-in privacy cover to physically close the camera.			
	The terminal should support auto-framing feature			
	The terminal should support speaker tracking feature			

Microphone Requirements	**The terminal should support at minimum of 6 built-in microphone arrays, with a sound pickup radius of minimum12 meters, and a sound pickup angle of 180°.**			
	The terminal should support the following features; acoustic echo cancellation (AEC), automatic gain control (AGC) and automatic noise reduction (ANR)			
Speaker Requirements	**The terminal should support at least two built-in speakers**			

Interface Requirements	**The terminal should be equipped with: Video In: 1 x HDMI 2.0 (4K60) and Video Out: 1 x HDMI 2.0 (4K60)**			
	The terminal should be equipped with; Audio In: 1 x 3.5mm and Audio Out: 1 x 3.5mm			
	The terminal should be equipped with: 3 x USB Type-A 3.0, supports USB flash drive; mouse, keyboard, microphone, speaker, remote control and wireless dongle for projection.			
	The terminal should be equipped with: a USB Type-C, supports USB flash device; wireless dongle for projection.			
	The terminal should be equipped with: 1 x 10/100/1000M RJ45 port			
	The terminal should be equipped with: 1 x COM port (RJ45)			
	The terminal should be equipped with 1 x OPS slot for PC module.			
	The terminal should support Wi-Fi 5 and Wi-Fi 6, IEEE802.11a/b/g/n/ac/ax network protocol			
	The terminal should be equipped with dual-band WiFi supporting both 2.4 GHz and 5 GHz.			
OPS Module Requirements	**The terminal should be equipped with a minimum Core I7-10700 processor, 16G DDR4 RAM, and 512G SSD.**			
	The terminal should support the following interfaces: Video out: 1 x HDMI 1.4, 1 x DP 1.2. Audio in: 1 x 3.5mm. Audio out: 1 x 3.5mm. USB: 3 x USB Type-A 3.0, 3 x USB Type-A 2.0.			
	The terminal should be equipped with Windows 10 enterprise OS.			
Remote controller Requirements	**The terminal should support a remote control that controls the volume, speaker on/off, microphone mute/unmute, camera open/close, previous/next page**			

Whiteboard Requirements	**The terminal should support a writing latency no more than 18ms.**			
	The terminal should have a built-in whiteboard that supports handwriting, drawing, erasing, marking, saving, zooming, and locking the whiteboard, background color can also be changed.			

	The terminal should support full-screen annotation: You can take a screenshot of any screen to enter the whiteboard annotation.			
	The terminal should support several modes for saving whiteboard document.			
	The terminal Whiteboard should have smart text and smart graphics recognition feature.			
	The terminal should support Wired projection through USB Type-C cable and HDMI cable with reverse control feature.			
	The terminal should support wireless projection through wireless dongle for one-click projection for PC and through projection App with reverse control feature.			
	The terminal should support Wi-Fi Direct projection with reverse control feature.			
	The terminal should support DLNA projection.			
	The terminal should allow users to use the same projection APP to project screens to OPS Windows.			
Third-party Video Conference Requirements	**The terminal should support third-party video conference APP.**			
	The terminal should support camera, microphone and speaker to be used for third-party video conference APP.			
	The terminal should support camera auto-framing and voice tracking features to be used for third-party video conference APP			
Special Feature Requirements	**The terminal should support Multi-window feature;**			
	The terminal should support BYOM and BYOD feature.			

	The terminal should support a welcome page without OPS module, the welcome page should contain text and pictures. The font of the text can be edited and the pictures can be customized.			
	The terminal should support user's quick customization of applications on the home page. Common applications can be placed on the home page for quick search. At least six applications can be configured on the home page.			
	The terminal should support dynamic wallpapers and static wallpapers. Wallpapers can be changed and imported.			
	The terminal should support cloning screen content to another screen via HDMI cable			
	The terminal should support OTA (over the air) technology.			
Security Requirements	**The terminal should support a web portal which must comply with complexity. It must contain at least three types of the following characters: letters, digits, and special characters. And the password must contain at least eight characters.**			
	The terminal should support 802.11a/b/g/n/ac/ax protocols and WPA2 authentication and also support the following protocols, TCP/IP, RTP, RTCP, DHCP, DNS, SMTP, SNTP, SSH, HTTP, HTTPS, and TR069			
Certificate Requirements	**The terminal should have a CE certificate**			
Registration with Huawei	**The bidder must be a registered partner, with Huawei Kenya**			
	ADDITIONAL ACCESSORIES	**Qty**		
1	**Ideahub Controller Pointer**	**10pcs**		
2	**Stylus pens**	**10pcs**		
3	**Ideashare Key**	**10pcs**		

3. Supply, Delivery, License Activation and Testing of Network Security Unified Threat Management System- Firewall - **2pcs**

SN	Component	Required specification/Feature /Applicable standards	Compliance (Full/Not Complied)	Detailed Response with Evidence
1.	General Requirements	**The firewall must be a hardware appliance**		
		The firewall must preferably be from a vendor ranked in the Leaders Magic Quadrant for the 2021 & 2022 Gartner Network Firewall report		
		The firewall must have ICSA Labs Certifications for Antivirus, Corporate Firewall, IPsec, NIPS, SSL-TLS.		
		The firewalls must have the following minimum features:		
		Must support at least 8 x 1GE RJ45 ports		
		Must support at least 8 x GE SFP slots with 4 x 1GE SFP SX transceiver module per appliance.		
		Must support at least 2 x 10 GE SFP+ Slots with 2 x 10GE SFP+ transceiver module short range per appliance		
		Must support at least 2x GE RJ45 MGMT/HA Ports		
		Must support a firewall throughput of at least 35Gbps		
		Must support an Enterprise NGFW throughput of at least 19 Gbps		
		Must support an Enterprise Threat Protection throughput of at least 17 Gbps		
		Must support an IPS Inspection Throughput of at least 24 Gbps		
		Must support at least 420,000 New Sessions/Second		
		Must support at least 1 Million / 2 Million Maximum Concurrent Sessions		
		Must support a IPSec VPN throughput of at least 55 Gbps		
		Must be supplied with at least 500 SSL VPN licenses and able to scale to 1500 when required		
		Must support 2* 1 TB SSD		
		Must support redundant AC power supplies		

		Must support load balancing of internet bandwidth supplied by two or more ISPs		
		Must support use of four (4) or more DNS IP addresses from ISPs		
		Must be able to provide DHCP services for different subnets when configured		
SN	Component	Required specification/Feature /Applicable standards	Compliance (Full/Not Complied)	Detailed Response with Evidence
2.	License Features	The firewall must support and licensed for:		
		Application Control		
		Web Filtering		
		DNS Security		
		Intrusion Prevention System		
		Content Disarm & Reconstruction		
		Antivirus		
		Virus Outbreak Protection		
		Anti-Botnet		
		Cloud Sandbox		
		Full SD-WAN features		
3.	Stateful Firewall Features	**The Firewall Must be ICSA Labs certified for Enterprise Firewall or EAL 4 certified, if not the same model**		
		It Must be possible to operate the firewall in "bridge mode" or "transparent mode" apart from the standard NAT mode		
		The Firewall must provide NAT functionality, including PAT.		
		Must support "Policy-based NAT"		
		The Firewall Must provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP		
		Firewall Must support Voice based protocols like H.323, SIP, SCCP, MGCP etc. and RTP Pinholing.		
		The Firewall Must support User-Group based Authentication (Identity based Firewalling) & Scheduling		

		IPv6 support for both NAT and Transparent Mode		
4.	Explicit & Transparent Proxy	**The proposed system must provide explicit web proxy capabilities for proxying IPv4 and IPv6 HTTP and HTTPS traffic with the following capabilities:**		
		Support for the use of multiple ports and port range for proxying		
		Definition of a FQDN, to be entered into browsers		
		Security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself		
		Create URL match list with URL patterns forward to forwarding servers and/or create a list of URLs that are exempt from web caching		
		The proxy must support ZTNA telemetry, tags, and policy enforcement		
		The ZTNA proxy must be able to act as a reverse proxy for HTTP servers		
		The ZTNA proxy must be able to support TCP forwarding for non-HTTP applications.		
		The proposed system must be capable of hosting Proxy Auto-Configuration (PAC) file		
		The proposed system must support proxy chaining when deployed as an explicit web proxy		
		The proposed system must support transparent web proxy whereby the user's client software, such as a browser, is unaware that it is communicating with a proxy.		
		The proposed system must support explicit FTP Proxy		
5.	High Availability	**The proposed system must support high availability with industry-standard VRRP with the following characteristics:**		

		Be able to function as a primary (master) or backup Virtual Router Redundancy Protocol (VRRP) device and can be quickly and easily integrated into a network that has already deployed VRRP		
		Be able integrated into a VRRP group with any third-party VRRP devices		
		Supports IPv4 and IPv6 VRRP		
		The proposed system must support high availability by setting up a cluster with the following characteristics:		
		Supports up to 4 cluster members		
		Supports 2 HA modes; active-passive (failover HA) and active-active (load balancing HA)		
		Cluster units communicate with each other through their heartbeat interfaces		
		Provides device failover in the event of hardware or software failure		
		Provides link failover when a direct link is not available on one/more monitored interface(s)		
		Provides remote link failover when connectivity with IP addresses of remote network devices, for example, a downstream router is not available		
		In the event of a failover, log messages about the event and can be configured to send log messages to a syslog server. The cluster can also send SNMP traps and alert email messages		
		Supports the option to automatically failback in the event the original unit recovers		
		Supports widely separated cluster units installed in different physical locations		

		The proposed system must support active-passive virtual clustering that uses virtual unit partitioning to send traffic for some virtual units to the primary cluster unit and traffic for other virtual units to the backup cluster units. If a failure occurs and only one cluster member continues to operate, all traffic fails over to that physical unit, similar to normal HA.		
		The proposed system must support the upgrade of the firmware without interrupting communication through the cluster		
		In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two to 16 units can be integrated into the load balancing configuration by operating as peers that process traffic and perform configuration synchronization; and session synchronization of connectionless sessions, expectation sessions, and NAT sessions and IPsec tunnels.		
6.	VPN Features	**The VPN Must be integrated with firewall and Must be ICSA Labs certified for both IPSec and SSL-TLS**		
		Must support the following protocols: -		
		DES & 3DES		
		MD5, SHA-1 & the more secure SHA-256 authentication		
		Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.		
		Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm		
		The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)		
		Must support Hub and Spoke VPN topology, Must also support PPTP and L2TP over IPSec VPN protocols.		

		IPSec NAT Traversal & Dead Peer Detection Must be supported		
		IPSec VPN Must support XAuth over RADIUS and RSA SecurID or similar product.		
		Must have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy		
		Must support SSL Two-factor Authentication with Digital Certificates		
		Must support Single Sign-On Bookmarks for SSL Web VPN.		
		Must support NAT within IPSec/SSL VPN tunnels		
		Must support Windows, Linux and MAC OS for SSL-VPN (Must have always-on clients for these OS apart from browser based access)		
7.	Intrusion Prevention Features	**Must have integrated Network Intrusion Prevention System (NIPS) and Must be ICSA Labs certified.**		
		Must have a built-in Signature and Anomaly based IPS engine on the same unit		
		Must have protection for 3000+ signatures		
		Able to prevent denial of service and Distributed Denial of Service attacks.		
		Must be able to exclude certain hosts from scanning of particular signatures		
		Supports CVE-cross referencing of threats where applicable.		
		Must provide the facility to configure Profile based sensors (Client/Server) for ease of deployment		
		Must support granular tuning with option to configure Overrides for individual signatures.		
		Supports automatic Attack database updates directly over the internet. (i.e. no dependency on		

		any intermediate device)		
		Supports attack recognition inside IPv6 encapsulated packets.		
		Supports user-defined signatures (i.e. Custom Signatures) with:		
		Regular Expressions.		
		Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options		
		Must offer a variety of built-in responses including dashboard alerts, syslog / email notifications, SNMP traps and Packet Capture log. List all response options, excluding prevention responses		
		Must Identify and control over 1000+ applications (i.e. Application control feature)		
		Must perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc		
		Must control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc		
8.	Antimalware Features	**The appliance Must facilitate embedded anti-virus support which is ICSA Labs certified**		
		Must include Antispyware and Worm Prevention		
		Must have option to schedule automatic updates of the new virus pattern.		
		Gateway AV Must be supported for real-time detection of viruses and malicious code for HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP, NNTP and IM		
		Must have configurable policy options to select what traffic to scan for viruses		

		Must have option to configure to respond to virus detection at the gateway in several ways i.e. Delete the file, Alert email, Quarantine etc		
		Must have options to prevent user downloads based on file extension as well as file type		
		Must have support for "Flow-Based Antivirus Scanning Mode" for high throughput requirements		
		The solution Must be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
		Must have an ability of Antivirus scanning for IPv6 traffic		
9.	Sandboxing Features	**The solution Must be tightly integrated with the cloud threat mitigation in order to make the protection more effective and updated so as to minimize the occurrence of false positives.**		
		The solution Must have multi-layer of detection process with the malicious code emulation and execution in the VM environment.		
		The solution Must be able to inspect the web session to detect and notify the malicious web activity including malicious file downloads through the web/internet.		
		The solution Must be able to store payload and artifacts of the detected threats for further analysis and incident time lines that is with the third party as well.		

		The proposed solution Must have the ability to analyze, detect and block malware in common file formats including but not limited to executable, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks.		
		The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution Must also assign a unique identification number to each identified/detected threat for future reference.		
		The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration		
		The solution Must be part of an integrated model therefore it Must interact with other security network element in order to give full proof detection and correction model rather than having a point product.		
		The solution must be able to detect and report malware by using multiple client environments (operating systems with multiple service pack levels) supporting both x64 and x86 architectures.		
		The solution Must support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions		

		The solution Must be based on algorithm, which Must be able to detect maximum Malware or rogue elements with each signature.		
		The solution Must have ability to block all outbound call- back communication initiated by the internal clients (infected)		
10.	Web Filtering Features	**The appliance Must facilitate embedded Web Content Filtering feature**		
		Web content filtering solution Must work independently without the need to integrate with External proxy server.		
		Must have facility to block URL' based on categories. Must support HTTP and HTTPS based traffic.		
		URL database Must have more than 250 million URLs under 75+ categories.		
		Must be able to block different categories/sites based on User Authentication.		
		Must have configurable parameters to block/allow unrated sites. Must have option to locally rate sites.		
		Must have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable		
		Must have options to customize the "Blocked Webpage Message" information displayed to end users		
		Must have facility to schedule the configurations so that non-work related sites are blocked during office hours and allow access to all sites except harmful sites during non- office hours. Must also have time-based quota		
		The solution Must have options to block java applets, ActiveX as well as cookies		
		The solution Must be able to block URLs hosting spywares / adwares etc.		

		Must have capability to restrict access to Google Corporate Accounts only		
		Must support credential phishing prevention: scans user names and passwords in submission traffic to external URLs against the sensitive corporate network credentials stored in the corporate domain controller		
		Must have configurable policy options to define the URL exempt list		
11.	Traffic Optimization Features	**Must support WAN load balancing (weighted) algorithms by volume, sessions, source-destination IP, Source IP, and spillover**		
		Must support link aggregation or bandwidth aggregation and redistribution based on firewall policies and rules.		
		Must support multi-path intelligence using rules defined by:		
		Source address and/or user group		
		Destination address and/or a selection of over 3,000 applications		
		Path selection using particular link quality criteria or SLAs defined		
		Must support traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support		
		Must support an option to set up traffic shaping profile by defining the percentage of interface bandwidth for each classified traffic and then bind to interfaces		
		Must support traffic shaping policies that a signs traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL		

		category.		
		Must support DSCP match in SD-WAN rules		
		Must support inline and out-of-path WAN optimization topology, peer to peer, and remote client support		
		Must support at least CIFS, FTP, HTTP(S), MAPI and TCP WAN optimization protocols		
		Must support multiple WAN optimization sessions on the same tunnel, must support zero-touch deployment		
12.	System Integration	**The proposed system must have the ability to interconnect discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface.**		
		The proposed system must have in-built automation feature that pairs an event trigger with one or more actions to monitor the network and take the designated actions when a threat or situation change is detected. It should have the followings:		
		Triggers: configuration change, system status, HA failover, event log handler, incoming webhook and schedule		
		Actions: Cli Script, Email, iOS app notification, public cloud functions, slack notification and webhook		
		The proposed system must allow GUI configurations to external services that include:		
		Public cloud providers - AWS, Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), IBM Cloud and AliCloud		

		SDN platforms and private cloud hypervisors - Kubernates, VMware NSX, VMware ESXi, OpenStack, Cisco ACI, Nutanix and Nuage VSP		
		Identity Systems - Active Directory service, RADIUS, NAC system, endpoint management system and Microsoft Exchange		
		External threat feeds: URL list, IP list, domain name list, and malware file hash		
13.	SSL Inspection	**The proposed system must provide Secure sockets layer (SSL) content scanning and inspection abilities that allow organizations to apply antivirus scanning, application control, web filtering, and email filtering to encrypted traffic**		
		The proposed system must support certificate inspection on port 443, all ports or a specific non-standard port. In addition, the system should:		
		Must have an option block session with invalid certificates		
		Must have an option allow sessions with untrusted certificates		
		Must support HTTP/2 in proxy mode SSL inspection		
		Must leverage on dedicated hardware for hardware-accelerated SSL Inspection		
		The proposed system must provide the ability to exempt web sites from SSL inspection by site reputation, address, category, or using a white list.		
14.	Logging, Analytics, Automated Response, & Reporting Appliance (Quantity 1)	**Must be a virtual appliance**		
		Must support at least 5 GB/Day of logs		
		Must support Indicators of Compromise License for malicious IPs, URLs, and file Hashes		
		Must support an Outbreak Alert service for new malware campaigns.		

		Must support and Security Operation Center (SOC) functionality with SIEM database to store normalized logs from logging devices.		
		Must support SOAR capabilities such as creation of playbooks for automated response of incidents.		
		Must support syslog or CEF log forwarding for third-party solution integration		
		Support full Graphic summary reports, providing network wide reporting of events, activities, and trends		
		Must have Built in report templates		
		Allow Comprehensive alert builders		
		Simple and intuitive Google-like search experience and reports on network traffic, threats, network activities and trends across the network		
		ADDITIONAL ACCESSORIES	**Qty**	
	4	**Structured cabling at Main Campus – Must come for site visit**	**lot**	

4. Supply, Delivery, Installation of Structured cabling, Testing, Documentation, Training of Technical Support Staff and Commissioning of LAN at Main Campus.

Required: Mandatory site visit on Tuesday 6th December 2022, at 10.00 am. Any late bidder will NOT BE ALLOWED TO PARTICIPATE.

S/No	Scope of Work/ Required specification/Feature /Applicable standards Compliance	Medium/ Devices
1.	Installation of LAN backbone – six (6) segments, 8 core, multimode, 10 G	Fiber optic cable connecting core network segments
2.	Installation of structured cabling -in offices, library,	CAT 6 A

	Labs	
3.	Installation of structured cabling to support out-door WIFI access points	Fiber / UPT
4.	Managed cisco full PoE 48 port switches with SFP ports and modules	To be determined during site visit
5.	Delivery and deployment of network accessories e.g. trucking, face plates, modules, cable support structures, RJ 45, patch panels, patch codes, cabinets, UPS, etc.	To be determined during site visit
6.	Cable management	Entire LAN
7.	Test full functionality of the network throughput and stability	Entire LAN
8.	Documentation of the entire network	Entire LAN

5. Voice over Internet Protocol Telephone System

SUPPLY, DELIVERY, INSTALLATION, TESTING, TRAINING AND COMMISSIONING OF INTERNET PROTOCOL (IP) BASED TELEPHONE SYSTEM WITHIN EXISTING LOCAL AREA NETWORK (LAN)

(i) Supply Delivery & Installation

S/No.	Location	Scope of work ***(Inclusive of all Installation, Configuration and Activation/Licensing Costs where applicable)***	Minimum Specs	Units	Quantity
1.	Server Room	Supply & Installation of Grandstream IP-PBX	• Support for up to 2000 SIP endpoint registrations, up to 200 concurrent calls and up to 64 conference attendees • 1GHz quad-core processor • 1GB DDR3 Ram, 32GB Flash • 1 Integrated T1/E1/J1 interface, 2PSTN trunk FXO ports, 2 analog telephone/Fax FXS ports capability • Gigabit network ports which Integrates PoE, USB, SD card, integrated NAT router • Comprehensive security protection using SRTP, TLS and HTTPS with hardware encryption accelerator	PCs	1

			• Power Adapter		
2.	GSM gateway router	4 channel GMS gateway router	• Pcs	1	
3.	Operator's Desk	Grandstream Operator's console & Headset	• 12 lines, 6 SIP accounts, 5 soft keys and 5-way voice conferencing • 48 on-screen digitally customizable BLF/speed-dial keys • 4.3 inch (480x272) color-screen LCD • Dual 10/100/1000 Mbps ports, integrated PoE • HD handset and speakerphone with support for wideband audio • Supports for headset use • Headset provided • Power Adapter		1
4.	Executive offices	High End Grandstream IP Phones	• 16 lines with up to • 16 SIP accounts • Built-in 1 mega-pixel • CMOS tiltable camera • for video calling with • privacy wheel • Dual-switched • auto-sensing • 10/100/1000Mbps • network ports • Integrated dual- • band Wi-Fi • (2.4GHz & 5GHz) • Built-in PoE/PoE+ for • power and network connections • 4-core 1.3GHz ARM • Cortex A53 processor • with 2GB RAM and • 8GB eMMC Flash • 6-way audio conferencing & • 3-way 720p 30fps HD video • conferencing capability		
5.	Offices of other senior managers	High End Grandstream IP Phones	• 8 lines, 8 dual-color line keys (with 4 SIP accounts) • 32 digitally programmable & customizable BLF/fastdial keys • HD wideband audio, fullduplex speakerphone • 5-way audio conferencing	Pcs	22

			• Dual-switched 10/100Mbps ports with integrated PoE • TLS and SRTP security encryption technology • Large phonebook capacity with at least 1,000 contacts • Call history with at least 100 records • Power Adapter		
6.	Other Offices	Basic Grandstream IP Phones	• 1 SIP account, 2 line keys, 3-way conferencing • Dual-switched 10/100 mbps ports • EHS support for headsets • At least 500 contacts • Call history with at least 100 records • Integrated PoE • Power Adapter	Pcs	173

(ii) Other Requirements (Cross-Cutting)

	Item	**Details (where applicable)**	**Unit**	**Qty**
7.	Labeling, Documentation & Telephone Directory		Lot	1
8.	Training (Users & Technical Staff)	(i) Users (Secretaries)	No	50
		(ii) Technical (ICT) Staff	No	15
9.	1 Year Warranty, Maintenance & Support Contract (accompanied with SLA)	Quarterly maintenance	Lot	1
10.	CAT 6, 3M and 1M patch codes	Patch codes for devices and patch panel	Lot	As per number of devices
11.	Other necessary hardware/software/passive devices	Any other items deemed necessary to meet specific/scope of the project	Lot	

Please note that the existing switches may NOT necessarily be POE and Power Adapters will be required for all Handsets

Mandatory Site visit is scheduled to take place at KCAU Main Campus in Rwaraka on **Tuesday 6th December 2022** at **10.00 am**. Any late bidder will NOT BE ALLOWED TO PARTICIPATE.

Mandatory

1. Duly signed Site visit Certificate
2. Detailed product brochures (technical data sheets) with **ACTUAL** device specifications/features

3. Manufacturer's authorization letter

SCHEDULE OF REQUIREMENTS

(i) Supply Delivery & Installation

S/No.	Location	Scope of work *(Inclusive of all Installation, Configuration and Activation/Licensing Costs)*	Minimum Specs	Units	Qty	Price	TOTAL
1.	Server Room	Supply & Installation of Grandstream IP-PBX	• Support for up to 2000 SIP endpoint registrations, up to 200 concurrent calls and up to 64 conference attendees • 1GHz quad-core processor • 1GB DDR3 Ram, 32GB Flash • 1 Integrated T1/E1/J1 interface, 2PSTN trunk FXO ports, 2 analog telephone/Fax FXS ports capability • Gigabit network ports with Integrates PoE, USB, SD card, integrated NAT router • Comprehensive security protection using SRTP, TLS and HTTPS with hardware encryption accelerator • Power Adapter	PCs	1		
2.	Server room	GSM gateway router	• 4 channel GMS gateway router	Pcs	1		
3.	Operator's Desk	Grandstream Operator's console & Headset	• 12 lines, 6 SIP accounts, 5 soft keys and 5-way voice conferencing • 48 on-screen digitally customizable BLF/speed-dial keys • 4.3 inch (480x272)		1		

			color-screen LCD • Dual 10/100/1000 Mbps ports, integrated PoE • HD handset and speakerphone with support for wideband audio • Supports for headset use • Headset provided • Power Adapter				
4.	Executive offices	High End Grandstream IP Phones	• 16 lines with up to • 16 SIP accounts • Built-in 1 mega-pixel • CMOS tiltable camera • for video calling with • privacy wheel • Dual-switched • auto-sensing • 10/100/1000Mbps • network ports • Integrated dual- • band Wi-Fi • (2.4GHz & 5GHz) • Built-in PoE/PoE+ for • power and network connections • 4-core 1.3GHz ARM • Cortex A53 processor • with 2GB RAM and • 8GB eMMC Flash • 6-way audio conferencing & • 3-way 720p 30fps HD video • conferencing capability	Pcs	4		
5.	Offices of other senior managers	Middle range Grandstream IP Phones	• 8 lines, 8 dual-color line keys (with 4 SIP accounts) • 32 digitally programmable & customizable BLF/fastdial keys • HD wideband audio, fullduplex speakerphone • 5-way audio	Pcs	20		

			conferencing • Dual-switched 10/100Mbps ports with integrated PoE • TLS and SRTP security encryption technology • Large phonebook capacity with at least 1,000 contacts • Call history with at least 100 records • Power Adapter				
6.	Other Offices	Basic Grandstream IP Phones	• 1 SIP account, 2 line keys, 3-way conferencing • Dual-switched 10/100 mbps ports • EHS support for headsets • At least 500 contacts • Call history with at least 100 records • Integrated PoE • Power Adapter	173			

(ii) Other Requirements (Cross-Cutting)

	Item	**Details (where applicable)**	**Unit**	**Qty**
12.	Labeling, Documentation & Telephone Directory		Lot	1
13.	Training (Users & Technical Staff)	(iii) Users (Secretaries)	No	50
		(iv) Technical (ICT) Staff	No	15
14.	1 Year Warranty, Maintenance & Support Contract (accompanied with SLA)	Quarterly maintenance	Lot	1
15.	CAT 6E, 3M and 1M patch codes	Patch codes for devices and patch panel	Lot	As per devices
16.	Other necessary hardware/software/passive devices	Any other items deemed necessary to meet specific/scope of the project	Lot	1

NOTES:

1. PLEASE FILL IN all quantities and their prices.
2. The existing switches are NOT necessarily POE and Power Adapters will be required for all Handsets

6. Supply, Delivery, Implementation, Integration with ERP, Testing, Training of Users and Commissioning of Portable Biometric Devices for Credit and Access Control

Technical Specifications and Requirements

Features	Description	Quantity
Portable RFID / Biometric Reader	All kinds of RFID card reader Provision to setup Start and Expiry date for cards secure fingerprint access control solution. Scratch proof QR, Barcode scanner Face Recognition (Optional)	10 pieces
3rd Party Access Controller	Any 3rd party access controller can integrate with all our turnstiles	
SDK, API Integration and documentation	Provide software development kit and the API documentation along with proposed solution.	
Access Control System (ACS)	Centralized architecture and all gate controllers should work independently.	
Failover method	Solution should make provision for primary and secondary servers to handle failure.	
Anti-pass back	Anti-pass back features.	
Custom Access Levels and Zones		
Clock/Time sync	All elements should sync time with central server. Realtime	
Custom Reports	In/out reports Login System Report Audit trail report Gate status report Readers status Error reports Hours inside the access area reports	
Integration with ERP	Integration with MS Dynamics NAV 2017	
Camera Integration	Integrate camera with system. Embedded in the reader to read face in dark or low light	
Security	Solution should be intelligent and have integrated security system based on TCP/IP protocol that provides configurable access at the gates	
Smart Card Read range	Proximity	
GPS /Wifi Enabled	Mode of connectivity	
Expected output	1. The devices should be able to read details of students from the ERP and display the following	

	details: Name, Course, Units and Students fees balance. 2. Should support the generation attendance lists by capturing such details about class attendance like: name and admission numbers of students who signed in, date, unit and the time signed in.	

FIRM REPRESENTATIVE
NAME: ……. **DATE: ……**

TITLE: …….

SIGNED: ……..

NAME OF ORGANIZATION: ……STAMP……

SECTION VI – EVALUATION CRITERIA

The evaluation shall be carried out in three Stages namely:

a. **Mandatory requirement**
b. **Technical evaluation**
c. **Financial evaluation**

a) Mandatory Requirements

The Mandatory requirements shall be as follows:

1. Must be a registered Company, licensed to provide the services tendered for. (Certificate of Incorporation must be attached)
2. Must have been in existence for a minimum of Five (5) Years as a registered Company.
3. Must have carried out similar assignments. (Evidence must be attached)
1. Authorized vendors of the products/ devices/ appliances/ software if different from the bidder. (Attach copy of vendor License/ authorization certificate)
4. Duly filled Business Questionnaire
5. Bid Bond (2% of the Bid amount) valid for 120 days from the date of Tender Opening
6. PIN/VAT Certificate
7. Certificate of Tax Compliance
8. Audited Accounts for the last 3 Years.
9. Any other requirement stipulated in the Tender document

b) Technical Evaluation

The Technical Evaluation shall be carried out as follows:-

ITEM	DESCRIPTION	Max Points
A	**Proven experience of the firm in implementation of relevant projects.**	**15 Points**
	A1. Experience in the implementation of the project -especially in a University (1 point for each project up to a maximum of 5 projects):	*5*
	A2. For each of the above five (5) projects, state whether it has been deployed: • Nationally- in Kenya (1 point per project) • Internationally (0.5 points per project)	*5*

	A3. Firms years of Experience in Similar Works • 5-10 years (3 points) • 10-15 Years (4 Points) • Above 15 Years (5 Points)	*5*
B	**Staff qualifications and experience in implementation of similar projects especially the proposed solution** ***(Attach CV's of Team lead and at least four (4) key project implementation members.)***	**45 Points**
	B1. Project/ Team Leaders experience in managing projects of Similar size and magnitude. • Below 5 Years (5 Points) • 5 to 10 Years (7 Points) • Above 10 Years (10 Points)	*10*
	B2. Staff, (Other 3 proposed staff) experience in implementing similar project is institutions of higher learning. **Scores per staff** • Below 5 Years (2 Points) • 5 to 10 Years (3 Points) Above 10 Years (5 Points)	*15*
	B3. Project/ Team Leader Academic Qualifications • Relevant Degree and Above (5 Points) **or** • Relevant Higher Diploma (3 Points) • Other relevant Certifications (2 points)	*5*
	B4. Other proposed **three** (3) staff academic Qualifications **Scores per staff**: • Relevant Degree and Above (5 Points) **or** • Relevant Higher Diploma (3 Points) • Other relevant Certifications (2 Point)	*15*
C	**Compliance with the provided technical specifications including provision of technical data sheets (where applicable), licensing (where applicable), detailed description of system and components (e.g. for structured cabling, etc.)**	**40 points or 25 Points (see details below)**
	NB: Since this evaluation checklist will be used to evaluate bidders for each of the six (6) projects listed in section V, bidders for tenders number 2, 3, 5 and 6 are advised to used the checklists provided in section V above and attach technical datasheets where applicable. For tenders number 1 and 4, evaluation will be based on site survey report and compliance with the provided specifications and scope of work. **For tender number 3, section C will provide 40 points, for tenders 1, 2, 4,5 and 6, section C will constitute 25 points.**	40 points for tender 3 25 Points for tenders 1,2,4,5 & 6

D	**D1. Work plan Presentation**: To include time frames, deliverables, milestones, manpower requirements e.t.c. (only tender number 3 is exempted)	*3*
	D2. Proposed completion dates being within the timelines provided in the bid document (only tender number 3 is exempted)	*2*
	D3. Methodology/Design D3.1 Description of implementation methodology/ approach (only tender number 3 is exempted)	*5*
	D3.2. Technical Drawing/Design All relevant Technical Drawings and Designs must be provided	*5*
	TOTAL	**100 Points**

The Cut off points for the Technical Score is 75%. Only the bidders who shall score above 75% in the Technical score shall proceed for Financial Evaluation.

SECTION VII- STANDARD FORMS

a) CONTRACT FORM

THIS AGREEMENT made the day of 20 between…… [Name of procurement entity] of..... [Country of Procurement entity](Hereinafter called "the KCA University") of the one part and …… [Name of tenderer] of ……. [City and country of tenderer](Hereinafter called "the tenderer") of the other part.

WHEREAS the KCA University invited tenders for certain materials and spares. Viz…….. [Brief description of materials and spares] and has accepted a tender by the tenderer for the supply of those materials and spares in the spares in the sum of …… [Contract price in words and figures]

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

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

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

   (a) the Tender Form and the Price Schedule submitted by the tenderer;
   (b) the Schedule of Requirements;
   (c) the Technical Specifications;
   (d) the General Conditions of Contract;
   (e) the Special Conditions of Contract; and

(f) the KCA University's Notification of Award.

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

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

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

delivered by_____the_____(for the KCA University)

Signed, sealed, delivered by_____the_____(for the tenderer)

in the presence of_____.

b) 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 ..... (**Attach Copy**)

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

……

Name of your bankers ……..

Branch ……

KRA Tax Compliance Certificate… .....(**Attach copy)**

Business Permit No..... (**Attach copy**)

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.

c) LETTER OF NOTIFICATION OF AWARD

Address of KCA University

_____

_____

To:_____

_____

_____

_____

RE: Tender No._____

Tender Name_____

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

_____

_____

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

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

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

Dr. Rebecca Mutia, PhD.

MANAGER, PROCUREMENT & STORES

(rmutia@kcau.ac.ke)