TENDER DOCUMENT

PROCUREMENT OF NEXT GENERATION FIREWALL / UTM / CYBERSECURITY SOLUTION

UNIVERSITY OF KARACHI

Opening date: 13-09-2023

UNIVERSITY OF KARACHI
KARACHI

Ref: P.O./13114-2023

Cost of Form
 Rs. 3,000/= (Non refundable)

TENDER DOCUMENT

PROCUREMENT OF NEXT GENERATION FIREWALL / UTM / CYBERSECURITY SOLUTION

S. #	TECHNICAL SPECIFICATIONS	COMPLY / NON-COMPLY
	Hardware Specifications	
	Processor : Multi-core Processing Technology	
	Form Factor : 1U Rackmount (sliding rails included)	
	Memory : Min 12 GB	
	HDD Storage : Min 180 GB SSD	
	Ethernet Ports (Minimum) : 8x 1GbE built-in Copper Ports (Incl. 2 bypass pairs), 2x GigEth SFP, 2x GigEth SFP+ Ports with additional 1x Module Slots for extension supports the combination of 8x GbE Copper / 4x GbE Copper PoE / 8x GbE Copper PoE / 8x GbE SFP / 2x GbE SFP+ / 4x GbE SFP+ / 2x 40GbE QSFP	
	I/O Ports(Minimum) : 2 USB 3.0, 1 Micro USB, 1x COM (RJ45) Front & 1x Rear, HDMI	
	Display : Multi-function LCD module for showing status and etc,.	
	Power Supply : Internal auto-ranging 110-240VAC, 50-60 Hz Redundant Power Supply (External) Hot Standby	
	Product Certifications (Safety, EMC) : CB, CE, FCC Class A, VCCI, UL, CCC, ISED	
	Security Performance	
	Firewall Throughput : Minimum 33 Gbps	
	IPS throughput : Minimum 8.5 Gbps	
	VPN throughput : Minimum 3.2 Gbps	

	Antivirus throughput (proxy) : Minimum 6 Gbps	
	Concurrent connections : Min. 17,500,000	
	New connections/sec : Min. 200,000	
	Maximum licensed users : Unrestricted	
	General Management	
	Purpose-built streamlined user interface	
	3-clicks-to-anywhere navigation	
	Self-documenting menu system	
	Advanced trouble-shooting tools in GUI (e.g. Packet Capture)	
	Full command-line-interface (CLI) accessible from GUI	
	Two-factor authentication (One-time-password) support for administrator access, self service user portal, IPSec and SSL VPN	
	Role-based administration	
	High Availability (HA) Support in Active / Active and Active / Passive mode	
	Automated firmware update notification with easy automated update process and roll-back features	
	Firmware can be directly upgraded to latest version dispite having multiple major releases in between the OLD and Latest version.	
	Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers	
	Self-service User Portal	
	Configuration change tracking	
	Flexible device access control for services by zones	
	Email or SNMP trap notification options	
	SNMP and Netflow support	
	Central managment support from Firewall Manager (Cloud or appliances) (upto 5 devices should be Free)	
	Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly	

	API for 3rd party integration	
	Remote access support from OEM directly	
	Firewall, Networking & Routing	
	Stateful deep packet inspection firewall	
	FastPath Packet Optimization	
	User, group, time, or network based policies	
	Access time polices per user/group	
	Enforce policy across zones, networks, or by service type	
	Zone isolation and zone-based policy support	
	Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi	
	Custom zones on LAN or DMZ	
	Pre-defined IPS, Web, App & Traffic Shaping (QoS Policies)	
	Firewall rule templates for common business applications like Microsoft Exchange, SharePoint, Lync and much more defined in XML enabling customization and sharing.	
	User Threat Quotient for identifying risky users based on recent browsing behavior and ATP triggers	
	Application Risk Meter provides and overall risk factor based on the risk level of applications on the network	
	SPAN support for Security Audit Reporting	
	Customizable NAT policies with IP masquerading	
	Flood protection: DoS, DDoS and portscan blocking	
	Country blocking by Geo-IP	
	Routing: static, multicast (PIM-SM) and dynamic (BGP, OSPF)	
	Upstream proxy support	
	Protocol independent multicast routing with IGMP snooping	
	Bridging with STP support and ARP broadcast forwarding	

	WAN link load balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rule	
	Wireless WAN support	
	802.3ad interface link aggregation	
	Full configuration of DNS, DHCP and NTP	
	Dynamic DNS	
	Protocol independent multicast routing with IGMP snooping	
	Bridging with STP support and ARP broadcast forwarding	
	IPv6 support with tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec	
	VLAN DHCP support and tagging	
	Multiple bridge support	
	Traffic Shaping & Quotas	
	Network or user based traffic shaping (QoS)	
	Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical	
	Real-time VoiP optimization	
	DSCP marking	
	Wireless Protection & Control	
	Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center (no additional hardware required)	
	Central monitor and manage all APs and wireless clients through the built-in wireless controller	
	Bridge APs to LAN, VLAN, or a separate zone with client isolation options	
	Multiple SSID support per radio including hidden SSIDs	
	Support for the latest security and encryption including WPA2 Personal and Enterprise	
	Support for IEEE 802.1X (RADIUS authentication)	
	Support for 802.11r (fast transition)	

	Hotspot support for (custom) vouchers, Password of the day, or T&C acceptance	
	Wireless guest Internet access with walled garden options	
	Time-based wireless network access	
	Wireless repeating and bridging meshed network mode with supported APs	
	Automatic channel selection background optimization	
	Support for HTTPS login	
	Rogue AP detection	
	Authentication	
	Transparent, proxy authentication (NTLM/ Kerberos) or client authentication	
	Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+	
	Client authentication agents for Windows, Mac OSX, Linux 32/64	
	Authentication certificates for iOS and Android	
	Single sign-on: Active directory, eDirectory	
	Authentication services for IPSec, L2TP, PPTP, SSL	
	Captive Portal with customized logo	
	User Self-Service Portal	
	Download the Authentication Client	
	Download SSL remote access client (Windows) and configuration files (other OS)	
	Hotspot access information	
	Change user name and password	
	View personal internet usage	
	Base VPN Options	
	Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, Pre-shared key	
	L2TP and PPTP	

	Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client support	
	SSL client for Windows & configuration download via User portal	
	IPSec Client Options	
	Authentication: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token and XAUTH	
	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	
	Intelligent split-tunneling for optimum traffic routing	
	NAT-traversal support	
	Client-monitor for graphical overview of connection status	
	Multilingual: German, English and French	
	Intrusion Prevention Systems (IPS)	
	High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection	
	Must have the capability to instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise	
	Must limit access to network resources or completely isolate compromised systems / workstations even in the same broadcast domain until they are cleaned up	
	Top rated by NSS Labs	
	Support for custom IPS signatures	
	IPS Policy Smart Filters that enable dynamic policies which automatically update as the new patterns are added	
	Advance Threat Protection and Synchronized Security	
	Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)	
	Branch Extension Support VPN	
	Central Management of all Branch devices	
	No configuration necessary: Automatically connects through a cloud-based provisioning service	
	Secure encrypted tunnel using digital X.509 certificates and AES256- encryption	
	Virtual Ethernet for reliable transfer of all traffic between locations	

	IP address management with centrally defined DHCP and DNS Server configuration	
	Remotely de-authorize Branch devices after a select period of inactivity	
	Compression of tunnel traffic	
	VLAN port configuration options	
	Clientless VPN	
	Unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet and VNC	
	Web Protection and Control	
	Fully transparent Proxy for Anti-Malware and Web-filtering	
	Enhanced Advanced Threat Protection (ATP)	
	URL Filter database with millions of sites across 92 categories backed by OEM SecurityLabs	
	Surfing quota time policies per user/group	
	Access time polices per user/group	
	Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/ HTTPS, FTP and web-based email	
	Advanced web malware protection with JavaScript emulation	
	Live Protection real-time in-the-cloud lookups for the latest threat intelligence	
	Second independent malware detection engine for dual-scanning (Dual AV)	
	Real-time or batch mode scanning	
	Pharming Protection	
	HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions	
	SSL protocol tunnelling detection and enforcment	
	Certificate validation	
	High performance web content caching	
	File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)	

	YouTube for Schools enforcement/policy	
	SafeSearch enforcement (DNS-based) for major search engines	
	Web keyword monitoring and enforcement to log, report or block web content matching keyword	
	Block Potentially Unwanted Applications	
	Cloud Application Visibility	
	Display amount of data uploaded and downloaded to cloud applications	
	Application categorization as new, authorized, unauthorized or tolerated	
	Details of uses, traffic and data	
	Traffic shaping policies can enforce of cloud Apps on one-click	
	Filter cloud applications usage by category or volume	
	Detailed customizable cloud application usage report for full historical reporting	
	Application Protection and Control	
	Enhanced application control with signatures and Layer 7 patterns for thousands of applications	
	Synchronized App Control to automatically identifies hundreds of unknown, evasive, and custom Windows and MAC applications with the option to prioritze and block.	
	Application Control Smart Filters that enable dynamic policies which automatically update as the new patterns are added	
	Macro app discovery and control for granual level policy enforcement	
	Application control based on category, characteristics (e.g. bandwidth and productivity consuming), technology (e.g. P2P) and risk level	
	Per-user or network rule application control policy enforcement	
	Web & App Traffic Shaping	
	Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared	
	Built-in on-box reports with customized reporting	
	Dashboards on Traffic, Security, and User Threat Quotient,	

	Applications Report on App Risk, Blocked Apps, Web Uses, Search Engines, Web Servers, Web Keyword matching, FTP	
	Network & Threats Report on IPS, ATP, Wireless	
	VPN Reports	
	Email usage and protection Reports	
	Compliance reports i.e., PCI-DSS, HIPAA, GLBA, SOX, FISMA, NERC CIPv3, and CIPA	
	Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks	
	Report anonymization	
	Report scheduling to multiple recipients by report group with flexible frequency options	
	Export reports as HTML, PDF, Excel (XLS)	
	Report bookmarks	
	Full log viewer with retention customization by category	
	Compliance & Certifications	
	The solution must be HIPAA complaint and addressed the security requirements as a part of the customer's HIPAA compliance program:	
	Payment Card Industry Data Security Standard (PCI DSS) v3.2 compliant	
	SANS Top 20 security controls compliant	
	Must be ICSA Labs certified	
	Product must be in Leaders Quadrant in recent Gartner Magic Qadrant for UTM	
	Recommended by NSS Labs	
	Warranty and Support	
	2 Years Hardware Warranty & RMA with Exchange of box in 2 business days	
	24x7 Enhanced Plus Support by the Provider as Local and Principal as needed and as required	
	8*5 Local Support by the Provider as needed and as required (for2 year)	
	Free Security Updates & Patches, Free Software Features Updates & Upgrades	

	Security Subscriptions	
	24 months Security Subscription License Includes :	
	Next Generation Firewall with VPN, Routing, WAN Link Load Balancing, Link Aggregation, Traffic Shaping & Quota, Built-in Wireless Controller, Authentication	
	Network Protection including IPS, Branch Extension VPN, HTML5, ATP, Anti-malware, Anti-virus.	
	Web Protection including URL Filtering, App Control, Web & Application Traffic Shaping	
	Important Note:	
	Training to the staff	
	Supplying, Installing(Hardware/Software), Configuring, Provisioning, Management by the Principal with all respect as needed and as required	
	The H/W (Hardware) is required in H/A	
	The RMA applied for both of the hardware's for next 2 years	
	All the licenses should be required and subscribed for 2 years from the date of inception of this F/W	
	Local support from the local vendor for 2 years. From the excepts of providers	

TERMS & CONDITIONS

- The Procuring Agency may reject all bids at any time prior to the acceptance of a bid under SPP-Rules, 2010 amended up to date.
- 2% Bid Security should be attached with the bidding document in shape of pay-order drawn in favor of University of Karachi.
- Bids not accompanied by the Bid Security will not be considered.
- Copies of the Sales Tax Registration, Sindh Revenue Board (SRB) and NTN are to be attached with the bidding documents.
- The quoted price shall be inclusive of all applicable Govt. Taxes and Charges.
- Procurement Committee shall finalize the bids in light of SPP-Rules, 2010 clause (8).
- The bid must be submitted along with the detailed company profile.
- The method of procurement is open competitive bidding single stage one envelop procedure.
- The price to be quoted shall be filled in the bidding documents mandatory.
- The successful bidders who undertake to execute the contract shall be liable to forfeiture of their Bid Security as a penalty.
- The bid shall be evaluated on the following criterion.
  o Lowest evaluated bid in terms of Value for Money.
  o As per specifications, terms & conditions mentioned in the bidding document.
- Period of Bid Validity (days):- 90 (Ninety) Days
- Delayed Delivery: 10% liquidity damages of the total amount will be imposed per month for which the company/firm/agency failed to deliver within the delivery/execution period.
- Quality Factors: The quality of Goods must be of prime quality.
- Condition of Goods / Works: All items must meet in all respects with the specs & conditions of the Order and must be in good condition otherwise they will be liable to reject.
- The last date of issuance of bidding document is day 12-09-2023 at 4:30 p.m.
- The last date of receipt bidding document is 13-09-2023 at 11:30 a.m. The bid shall be opened on the same day at 12:00 noon in presence of the bidders who may wish to be present.
- In case of any holiday or disturbance the bids shall be opened on the next working day as per schedule.
- The Tender Notice shall be available on the Official website www.pprasindh.gov.pk as well as Procuring Agency's website www.uok.edu.pk

Total Amount _____

(Rupees _____ Only)

(Total Earnest Money Rs. _____)

SIGNATURE OF THE PROPRIETOR
AND RUBBER STAMP OF THE COMPANY

Instruction to Bidders (ITB)

Preparation of Bids

1. Scope of Work   The *University of Karachi* plans to develop / acquire a comprehensive integrated solution for all the functional needs and requirements of *Next Generation Firewall / UTM / Cybersecurity Solution* as described in later pages.

2. Method and Procedure of Procurement   National Competitive Bidding Single Stage *Single Envelope* Procedure as per SPP Rules 2010 (updated 2013)

2. Language of Bid   The bid prepared by the Bidder, as well as all correspondence and documents relating to the bid exchanged by the Bidder and the Procuring Agency, shall be written in English language

3. Documents Comprising the Bid   The bid prepared by the Bidders shall comprise the following components:

(a)   Price Schedule completed in accordance with ITB Clauses 4, 5 and 6.

(b)   Bid security furnished in accordance with ITB Clause 9.

4. Bid Prices   4.1   The Bidder shall indicate on the appropriate Price Schedule the unit prices (where applicable) and total bid price of the *Next Generation Firewall / UTM / Cybersecurity Solution* it proposes to supply under the contract.

4.2   The prices shall be quoted inclusive of all taxes, stamps, duties, levies, fees and installation and integration charges imposed till the delivery of services specified in the Schedule of Requirements. No separate payment shall be made for the incidental services.

4.3   Prices quoted by the Bidder shall remain fixed during the Bidder's performance of the contract and not subject to variation on any account, unless otherwise specified in the Bid Data Sheet.

4.4   Prices shall be quoted in Pak Rupees unless otherwise specified in the Bid Data Sheet.

5. Bid Form   The Bidder shall complete the Bid Form and the appropriate Price Schedule furnished in the bidding documents, indicating the *Next Generation Firewall / UTM / Cybersecurity Solution* to be supplied.

6. Bid Currencies   Prices Shall be quoted in Pak Rupees.

7. Documents Establishing Bidder's Eligibility and Qualification   The Bidder shall furnish, as part of its bid, documents establishing the Bidder's eligibility to bid and its qualifications to perform the contract if its bid is accepted.

(a)   That the Bidder has the financial and technical capability necessary to perform the contract;

(b)   That the Bidder meets the qualification criteria listed in the Bid Data Sheet.

8.	**Documents** *"Next Generation Firewall / UTM / Cybersecurity Solution"* **Eligibility and Conformity to Bidding Documents**	The documentary evidence of conformity of the ***Next Generation Firewall / UTM / Cybersecurity Solution*** to the bidding documents may be in the form of literature and data.

9. Bid Security

9.1 The bid security is required to protect the Procuring agency against the risk of Bidder's conduct, which would warrant the security's forfeiture

The bid security shall be denominated in the currency of the bid:
  (a) 2% Bid Security should be deposited with the bid;
  (b) be submitted in its original form; copies will not be accepted;
  (c) remain valid for a period of at least 14 days beyond the original validity period of bids, or at least 14 days beyond any extended period of bid validity

9.2 Bid securities shall be released to the unsuccessful bidders once the contract has been signed with the successful bidder or the validity period has expired.

9.3 The successful Bidder's bid security shall be discharged upon the Bidder signing the contract, and furnishing the performance security.

9.4 The bid security may be forfeited:

  (a) if a Bidder withdraws its bid during the period of bid validity or

  (b) in the case of a successful Bidder, if the Bidder fails:

   (i) to sign the contract in accordance

10. Period of Validity of Bids

10.1 Bids shall remain valid for the period specified in the Bid Data Sheet after the date of bid submission prescribed by the Procuring agency. A bid valid for a shorter period shall be rejected by the Procuring agency as non responsive.

10.2 In exceptional circumstances, the Procuring Agency may solicit the Bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The bid security shall also be suitably extended as per Rule-38 of SPP Rules, 2010 (updated). A Bidder may refuse the request without forfeiting its bid security. A Bidder granting the request will not be required nor permitted to modify its bid.

11. Format and Signing of Bid

11.1 The Bidder shall prepare an original bid indicated in the Bid Data Sheet, clearly marking each "ORIGINAL BID".

11.2 The original and bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the contract. All pages of the bid, except for un-amended printed literature, shall be initialed by the person or persons signing the bid.

11.3 Any interlineations, erasures, or overwriting shall be valid only if they are initialed by the person or persons signing the bid.

Submission of Bids

12. Sealing and Marking of Bids

12.1 The Bidder shall seal the original envelopes, duly marking the envelopes as "ORIGINAL BID". The outer envelopes shall be addressed to the Procuring agency at the address given in the Bidding Documents, and carry statement "DO NOT OPEN BEFORE [13-09-2023].

12.2 If the outer envelope is not sealed and marked as required, the Procuring Agency shall assume no responsibility for the bid's misplacement or premature opening.

13. Deadline for Submission of Bids

13.1 Bids must be received by the Procuring Agency at the address specified in Bidding Documents, not later than the time and date specified in the Bid Data Sheet.

13.2 The Procuring Agency may, at its discretion, extend this deadline for the submission of bids by amending the bidding documents. in such case all rights and obligations of the Procuring agency and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

14. Late Bids

Any bid received by the Procuring Agency after the deadline for submission of bids prescribed by the Procuring agency shall be rejected and returned unopened to the Bidder.

15. Modification and Withdrawal of Bids

15.1 The Bidder may modify or withdraw its bid after the bid's submission, provided that written notice of the modification, including substitution or withdrawal of the bids, is received by the Procuring agency prior to the deadline prescribed for submission of bids.

15.2 No bid may be modified after the deadline for submission of bids.

15.3 No bid may be withdrawn in the interval between the deadline for submission of bids and the expiry of the period of bid validity Withdrawal of a bid during this interval may result in the Bidder's forfeiture of its bid security.

Opening and Evaluation of Bids

16. Opening of Bids by the Procuring agency

16.1 The Procuring agency shall open all bids in the presence of bidders' representatives who choose to attend, at the time, on the date, and at the place specified in the Bid Data Sheet. The bidders' representatives who are present shall sign a register/attendance sheet evidencing their attendance.

16.2 The bidders' names, bid modifications or withdrawals, bid prices, discounts, and the presence or absence of requisite bid security and such other details as the Procuring agency may consider appropriate, will be announced at the opening.

17. Clarification of Bids

During evaluation of the bids, the Procuring agency may ask the Bidder for a clarification of its bid. The request for clarification and the response shall be in writing, and no change in the prices or substance of the bid shall be sought, offered, or permitted.

18. Preliminary Examination	18.1	The Procuring agency shall examine the bids 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 bids are generally in order.
	18.2	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 Supplier does not accept the correction of the errors, its bid will be rejected, and its bid security may be forfeited. If there is a discrepancy between words and figures, the amount in words will prevail.
	18.3	Prior to the detailed evaluation, the Procuring agency will determine the substantial responsiveness of each bid to the bidding documents. A substantially responsive bid is one which conforms to all the terms and conditions of the bidding documents without material deviations. Procuring agency's determination of a bid's responsiveness is to be based on the contents of the bid itself.
	18.4	If a bid is not substantially responsive, it will be rejected by the Procuring agency and may not subsequently be made responsive by the Bidder by correction of the nonconformity.
19. Evaluation and Comparison of Bids	19.1	The Procuring agency will evaluate and compare the bids which have been determined to be substantially responsive.
	19.2	The Procuring agency's evaluation of a bid will be on delivery to consignee's end inclusive of all taxes, stamps, duties, levies, fees and execution charges imposed till the delivery location.
20. Contacting the Procuring agency	20.1	No Bidder shall contact the Procuring agency on any matter relating to its bid, from the time of the bid opening to the time of announcement of Bid Evaluation Report. If the Bidder wishes to bring additional information to the notice of the Procuring agency, it should do so in writing.
	20.2	Any effort by a Bidder to influence the Procuring agency in its decisions on bid evaluation, bid comparison, or contract award may result in the rejection of the Bidder's bid.
21. Post-qualification	21.1	In the Procuring agency may determine to its satisfaction whether that selected Bidder having submitted the lowest evaluated responsive bid is qualified to perform the contract satisfactorily.
	21.2	The determination will take into account the Bidder's financial and technical capabilities. It will be based upon an examination of the documentary evidence of the Bidder's qualifications submitted by the Bidder, pursuant to ITB Clause 7 as well as such other information as the Procuring agency deems necessary and appropriate.

21.3 An affirmative determination will be a prerequisite for award of the contract to the Bidder. A negative determination will result in rejection of the Bidder's bid, in which event the Procuring agency will proceed to the next lowest evaluated bid to make a similar determination of that Bidder's capabilities to perform satisfactorily.

22. Award Criteria

The Procuring agency will award the contract to the successful Bidder whose bid has been determined to be substantially responsive and has been determined to be the lowest evaluated bid, provided further that the Bidder is determined to be qualified to perform the contract satisfactorily.

23. Procuring agency's Right to Accept any Bid and to Reject any or All Bids

23.1 Subject to relevant provisions of SPP, Rules, 2010 (updated), the Procuring agency reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time prior to contract award.

23.2. Pursuant to Rule 45 of SPP Rules 2010 (updated), Procuring agency shall hoist the evaluation report on Authority's web site, and intimate to all the bidders seven days prior to notify the award of contract.

24. Notification of Award

Prior to the expiration of the period of bid validity, the Procuring agency shall notify the successful Bidder in writing, that its bid has been accepted.

25. Signing of Contract

25.1 At the same time as the Procuring agency notifies the successful Bidder that its bid has been accepted, the Procuring agency will send the Bidder the Contract Form provided in the bidding documents, incorporating all agreements between the parties.

25.2 Within the period specified in BDS, of receipt of the Contract Form, the successful Bidder shall sign and date the contract and return it to the Procuring agency.

26. Performance Security

Failure of the successful Bidder to comply with the requirement of ITB Clause 25shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the Procuring agency may make the award to the next lowest evaluated Bidder or call for new bids.

27. Corrupt or Fraudulent Practices

27.1 The Government of Sindh requires that Procuring agency's (including beneficiaries of donor agencies' loans), as well as Bidders/Suppliers/ Contractors under Government-financed contracts, observe the highest standard of ethics during the procurement and execution of such contracts. In pursuance of this policy, the SPPRA, in accordance with the SPP Act, 2009 and Rules made thereunder:

    (a) **"Corrupt and Fraudulent Practices"** means either one or any combination of the practices given below;

      a. **"Coercive Practice"** means any impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the

property of the party to influence the actions of a party to achieve a wrongful gain or to cause a wrongful loss to another party;

b. "**Collusive Practice**" means any arrangement between two or more parties to the procurement process or contract execution, designed to achieve with or without the knowledge of the procuring agency to establish prices at artificial, noncompetitive levels for any wrongful gain;

c. "**Corrupt Practice**" means the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence the acts of another party for wrongful gain;

d. "**Fraudulent Practice**" means any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation;

(b) "**Obstructive Practice**" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process, or affect the execution of a contract or deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making false statements before investigators in order to materially impede an investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or acts intended to materially impede the exercise of inspection and audit rights provided for under the Rules.

Bid Data Sheet

The following specific data for the *Next Generation Firewall / UTM / Cybersecurity Solution* to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITB). Whenever there is a conflict, the provisions herein shall prevail over those in ITB.

Introduction	
ITB 1	**Name and address of Procuring Agency:** *University of Karachi, Karachi*.
ITB 1	**Name of Contract.** *"Next Generation Firewall / UTM / Cybersecurity Solution"*
Bid Price and Currency	
ITB 4	Prices quoted by the Bidder shall be *"fixed" and in" Pak Rupees"*
Preparation and Submission of Bids	
ITSB 19	*Qualification requirements:* 1) NTN 2) Sales Tax 3) Registration with SRB for works & services 4) Minimum three years' experience relevant field 5) Turnover of at least last three years
ITB 7	**Amount of bid security.** As per SPP –Rules, 2010, Clause 37(1)
ITB 8	**Bid validity period.** 90 days
ITB 10	**Number of copies.** *One Original*
ITB 19.1	**Deadline for bid submission.** *13-09-2023* at *11:30 hours*
ITB 20	**Bid Evaluation:** ○ Lowest evaluated bid in terms of Value for Money. ○ As per specifications mentioned in the bidding document.
	Under following conditions, Bid will be rejected: 1. Conditional tenders/bids; 2. Bids not accompanied by bid security (Earnest Money); 3. Bids received after specified date and time; 4. Bidder submitting any false information; 5. Black Listed Firms by Sindh Government or any entity of it

SUMMARY SHEET
TENDER NOTICE

S. No.	Bid Value	Price in PKR

Total Bid Value in PKR		
Earnest Money @ 2% in PKR		
Pay Order/Demand Draft No:		**Date:**
Signature :	**Seal :**	