VIRTUAL UNIVERSITY OF PAKISTAN
FEDERAL GOVERNMENT UNIVERSITY

TENDER NOTICE

Through e-Pak Acquisition and Disposal System (EPADS) v2.0

Sealed Tenders are invited through (EPADS v2.0) **https://epads.gov.pk** from the Firms who are registered with Tax Authorities on Active Taxpayers List (ATL) of FBR, for the following:

Sr. No	Description	Tender Fee (Rs.)	Tender Opening Date	Tender Receiving / Opening Time
1	Tender No. VU/26-27/07/891 **Endpoint Security Solution (ICT)**	2,000/-	August 13, 2026	Receiving: 02:00pm Opening: 02:30pm

Tender documents for the above-mentioned tender(s) are also available on the Virtual University of Pakistan website **(https://www.vu.edu.pk/Opportunities/Tenders).** However, bids shall be submitted **only through EPADS v2.0.** Any bid submitted through any other mode shall not be considered.

The complete tendering process shall be carried out through EPADS v2.0.

Interested bidders are required to register themselves on EPADS v2.0 (https://epads.gov.pk) and submit their bids electronically through the EPADS v2.0 portal.

The Bid Security (if applicable), in the amount and form specified in the bidding documents and drawn in favor of the Virtual University of Pakistan, shall be uploaded as a scanned copy on EPADS v2.0. The original Bid Security, along with one hard copy of the sealed bid, must also be submitted physically to the Virtual University of Pakistan at the address provided below on or before the bid closing date and time.

Bids requiring Bid Security that are submitted without the prescribed Bid Security shall be rejected. The bid submission and opening schedule shall be strictly observed.

The University reserves the right to accept or reject any bid, or to annul the procurement process at any stage, in accordance with the provisions of the Public Procurement Rules, 2004.

This Tender Notice is also available on the PPRA website (www.ppra.gov.pk) and the Virtual University of Pakistan website.

PROCUREMENT DEPARTMENT, DIRECTORATE OF FINANCE
VIRTUAL UNIVERSITY OF PAKISTAN
SIR SYED MEMORIAL SOCIETY BUILDING, 19-ATATURK AVENUE, G-5/1, ISLAMABAD
Phone No. 051-111-880-880 | Extensions: 1366 / 1323 / 1651
Email: po@vu.edu.pk | Website: www.vu.edu.pk | VU NTN: 4388557-8

PID(0775/26

VIRTUAL UNIVERSITY OF PAKISTAN

Sir Syed Memorial Society Building, 19-Ataturk Avenue, G-5/1, Islamabad

http://www.vu.edu.pk

TENDER DOCUMENT

ENDPOINT SECURITY SOLUTION (ICT)

Tender No. VU/26-27/07/891

This tender will be opened on **August 13, 2026 at 02:30pm** in the Procurement Department, Virtual University of Pakistan, Sir Syed Memorial Society, 19-Ataturk Avenue, G-5/1, Islamabad.

Name of Firm/Company: _____

Office Address: _____

Contact Person: _____ Designation: _____

Phone No: _____ Fax No: _____ Cell No. _____

GST Reg. No: _____ N.Tax Number: _____

Active email address (in CAPITAL letters): _____

Status of Firm/Company (Pls. tick appropriate box)

Manufacturer / Authorized Dealer / Distributor ☐

General Supplier / Reseller ☐

ITEMS MARKED WITH (*) MUST BE ATTACHED; OTHERWISE, YOUR BID WILL BE DECLAREDAS NON-RESPONSIVE.

PROCUREMENT METHOD:
"SINGLE STAGE TWO ENVELOPS BIDDING PROCEDURE"

1. Bidding is on the basis of National Competitive Bidding (NCB) in accordance with "Single Stage Two Envelope Bidding Procedure" comprising of "Technical Proposal & Financial Proposal" (Separately Sealed) in single package, as per PPRA-Rules 2004 Clause No. 36(b).
2. No bid shall be considered if;
    - Not uploaded at EPADS v2.0
    - Not provided in shape of hard copy by the given schedule at given location
    - Both uploaded and hard copies of the bids must be with the same bidder name
    - Received without Original Bid Security (if any) and Tender Fee in a single envelop
3. Tender document duly completed should reach the Procurement Department, Directorate of Finance, Virtual University of Pakistan, not later than **02:00 pm on August 13, 2026**. Late Tenders will not be entertained. No telegraphic or faxed bid will be accepted.
4. Technical Proposals shall be opened at **02:30 pm on the same date** in the office of Procurement Department, Directorate of Finance, Virtual University of Pakistan, Islamabad.
5. **VU shall open all bids through EPADS v2.0 as per given schedule and place specified above, in presence of the bidders' representatives who choose to attend the meeting and shall sign an attendance sheet as evidence of their presence.**

6. Sealed Financial Proposals shall be held in safe custody. Financial Proposals will be opened publicly after completing the technical evaluation, in the presence of technically qualified bidder(s), on the date and the timings given afterwards.
7. Financial Proposals of technically non-qualified bidder(s) shall be returned un-opened.
8. If two or more bidders quote the same price in Financial Proposal, then the contract will be equally divided among all those bidder(s) or will be awarded to the bidder with better technical specification or Virtual University may ask the bidders to submit Financial Proposal again.

TERMS AND CONDITIONS:

1. The notice published in the media shall be considered an integral part of this tender document.
2. The Bidder is expected to examine all instructions, forms, terms and specifications in the Bidding Documents carefully. Failure to furnish the required information may result in the rejection of the Bid.
3. Tender shall be opened on the given date, time and venue. In the case of holiday on given tender opening date, same shall be opened on next working day.
4. Tender should be addressed to the Director Finance, Virtual University of Pakistan.
5. VU takes no responsibility for delay, loss or non-receipt of bids sent by post/courier.
6. Original tender Document, along with item specifications must be attached. All pages must be signed and stamped. **(*)**
7. Technical evaluation shall be carried out by the Technical Evaluation Committee and finalized according to the recommendations of the Committee.
8. Please attach financial soundness certificate / Account Maintenance Certificate issued by your bank which should not be older than 03 months. **(*)**
9. The bidder must submit an "Affidavit" on Rs.100/- Stamp Paper that the Bidder/Firm/Company/Contractor is not Blacklisted from Public Procurement Regulatory Authority (PPRA). Draft is given herewith in the document. **(*)**
10. The bidder submit the list of Directors/Partners/Owners along with the bid**.**
11. The bidder must be a registered taxpayer with FBR on Active Taxpayer List (ATL) and certificatemust be attached for NTN and GST. (If GST is exempted, please provide necessary evidence). **(*)**
12. GST should be exclusively/separately indicated in the Tender document and bill/invoice.
13. Bidder(s) should quote their rates (including all applicable taxes & duties at the prevailing rates) clearly on the Tender Document for each item both in figures and words.
14. The bid shall remain valid for a period of three (3) months from the date of opening of the bid. Validity of bid for a shorter period shall be rejected as non-responsive. **(*)**
15. To submit a tender with the Virtual University of Pakistan, bidders are required to deposit **Rs. 2,000/- online in any branch of Allied Bank Limited in Account No. PK58ABPA0010061279710055 (Virtual University of Pakistan). (*)**
16. The original deposit slip must be attached with the bid. This amount is a non-refundable tender fee and is mandatory. Cash, crossed/open cheques, Pay Orders, or Demand Drafts are not acceptable.
17. Bids submitted without the tender fee shall not be accepted. (*)
18. The Bidder shall furnish, as part of its bid, a "Bid Security (Earnest Money)", **amounting to Rs. 300,000/- in shape of DD/PO/CDR or a Bank Guarantee only** (Cheques shall not be accepted) in favour of Virtual University of Pakistan. Bid without earnest money shall not be entertained even (if) bidder is technically qualified. (*)

    A scanned copy of bid security is required to be uploaded through EPADS v2.0 and hard copy must be submitted physically with the bidding documents on the closing date of the tender. (*)

    Please submit original instruments of Tender Fee and Bid Security in a separate envelope within the Main Envelop or in Technical Proposal only. (*)
19. The bid security is refundable to the unsuccessful bidders after finalization of the tender.
20. Bid security of successful bidder (in which warranty is applicable) will be retained till providing the Performance Security in shape of a Bank Guarantee as per detail given ahead.

21. The successful bidder shall have to furnish within **Twenty one (21) days** after the execution / signing of the contract / issuance of Purchase Order, a performance security to the amount of **5% of the contract price / value of the Purchase Order** to VU. The proceeds of the performance security shall be payable to VU as compensation for any loss resulting from the Supplier's failure to complete its obligations under the contract / order. The performance securityshall be denominated in the currency of the contract and shall be in the following form.

    a. A Bank Guarantee issued by any Commercial Bank located in Pakistan ("A" rated or above).

    b. The performance bond will be discharged by VU not later than **15 days** following the date of expiry of the warranty, under the contract / purchase order.

22. If the Performance security is not submitted to VU within the specified period or its amount is less than 5% of the contract price / purchase order value, VU reserves the right to cancel the award of contract / purchase order and forfeit the Bid Security.

23. Items must be delivered to the Virtual University of Pakistan's Head Office at the address mentioned below or as instructed by the university within **Fifteen (15) days** from receipt of the Purchase Order.

    a. No extensions will be allowed unless granted by Purchase committee on solid grounds.
    b. Delay in provision of goods/item(s)/services by the bidder(s)/supplier(s) in accordance with the time schedule prescribed in the General Terms and Conditions (GTC) shall not be tolerated and in such default, penalty for delaying goods/item(s) shall be imposed @ 0.1% per day of the total contract / order amount or value of the items / services delivered after due date, which will be capped to maximum of 10% of the total value of the Contract / purchase order / undelivered items/services.
    c. The penalty on the value of goods/item(s) not delivered in time will be imposed which may lead to cancellation of order without any liability to the university and the said bidder/supplier/firm/company may also be blacklisted.
    d. Moreover, any penalty may be imposed by the VU in case of any default by the bidder/supplier, in addition to initiating legal action against such defaulter. Virtual University has also the right to stop its pending payment or forfeit its guarantee/security submitted to the Virtual University of Pakistan in this procurement or any other contract.

24. Notwithstanding anything contrary provided in the provisions of General Terms and Conditions (GTC) Clauses, the Bidder/Supplier shall not be liable for forfeiture of its performance security, liquidated damages, late delivery charges, or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the Contract is the result of an event of the Force Majeure.

    a. For purposes of this clause, "Force Majeure" means an event beyond the control of the Bidder/Supplier and not involving the Bidder/Supplier's fault or negligence and not foreseeable. such as, acts of God, perils of navigation, floods, storms, earthquakes, fire, hostilities, war (declared), terrorism, Port closure, Impositions of restrictions or regulations by any Government or Government Agency, illegality arising from applicable domestic or foreign laws or regulations, blockage and strikes that is politically motivated strikes and is widespread or nationwide, insurrection.

    b. A change in economic/market circumstances or unexpected hike in prices affecting the profitability of a contract or the ease with which parties' obligations can be performed, is not a force majeure event."

    c. If a Force Majeure situation arises, the Bidder/Supplier shall promptly notify the Virtual University in writing within five days from the date of such event of such condition and the cause thereof along with evidence, moreover take all steps that are reasonably necessary to mitigate or remove the consequences of force majeure. Where such notice of Force Majeure is not served by the Party claiming Force Majeure within the period prescribed herein then that Party's right to claim Force Majeure for that event would stand irrevocably waived.

    d. Unless otherwise directed by the Virtual University in writing, the Bidder/Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. The

benefit of Force Majeure shall be in favor of the client (VU), if it happened anytime.

25. Virtual University requires Contractors/Bidders, to the highest standard of ethics during the procurement and execution of contracts. For the purposes of this provision, the terms set forth in PPRA Rules /Act shall be applicable:

    a. VU will bar a firm/company/individual bidders/Contractors /consultant or whatsoevernamed, in accordance with Blacklisting procedures under Public Procurement Rules 2004 in any case if deems so.
    b. Furthermore, the Contractor/ Bidder(s) shall be aware of the provision stated in the General Terms & Conditions of the Contract.

26. Virtual University may, under the applicable Law (s) for a specified period, debar a bidder/ Contractor from participating in any public procurement process of VU, if the bidder or Contractor has

    a. Acted in a manner detrimental to the public interest or good practices.
    b. Consistently failed to perform its obligation under the contract.
    c. Not performed the contract up to the mark.
    d. Indulged in any corrupt practice.

    If VU debars a bidder/Contractor, the procuring agency:

    a. The said bidder/firm/company may also be blacklisted for a period of at least three (03) years.
    b. May forward the decision to the Public Procurement Regulatory Authority (PPRA) for publication on the website of the PPRA; and
    c. May request the PPRA to debar the bidder or contractor for procurement of allprocuring agencies.

27. Virtual University has the right to take any legal action against the bidder/supplier/firm/company, in addition to blacklisting, if it is found involved in corrupt practices.

28. Virtual University reserves the right to increase or decrease the quantity of goods specified ahead at the time of award of tender as per PPRA Rules. VU also reserves the right to place the order on a partial shipment basis.

29. The supplied items should conform to the standard specifications, must be brand new and be free from defects in all respects.

30. Income tax and GST shall be withheld as per Government rules.

31. Payment shall be released after submission of the Commercial invoice & Sales Tax Invoice, duly verified by the technical department. The payment will be made in accordance with SRO 660(I) 2007.

32. Virtual University reserves the right to accept or reject any bid or annul the procurement process a tany time as prescribed under PPRA Rules.

33. A bidder requiring any clarification in the bidding document shall contact the VU in writing within **Five (05) days through EPADS v2.0 or through given email**. The VU will respond in writing to respond to any clarification provided that such request is received within time. Should the clarification result in changes to the essential elements of the bidding documents, the VU shall amend the bidding documents at any time prior to the deadline for the submission of bids. The VU may amend the bidding documents by issuing addenda. Any addendum issue shall be part of the bidding document and shall be communicated in writing to all who obtained the bidding document from the VU. The VU shall also promptly publish the addendum to the Bidder on the VU website and EPADS v2.0.

34. To assist in the examination, evaluation, comparison of the Bids, and qualification of the Bidders, the VU may, at its discretion, ask any Bidder for a clarification of its Bid. Any clarification submitted by a Bidder in respect to its Bid and that is not in response to a request by the VU shall not be considered. The VU request for clarification and the response shall be in writing. No change, including any voluntary increase or decrease, in the prices or substance of the Bid shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the VU in the evaluation of the Bids. If a Bidder does not provide clarifications of its Bid by the date and time set in the VU request for clarification, its Bid may be rejected.

35. Provided that the Bid is substantially responsive, the VU shall correct arithmetical errors on the following basis:

    a. if there is a discrepancy between the unit price and the line-item total that is obtained by multiplying the unit price by the quantity, the unit price shall prevail and the line-item total shall be corrected, unless in the opinion of the VU there is an obvious misplacement of the decimal point in the unit price, in which case the line-item total as quoted shall govern and the unit price shall be corrected.

    b. if there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected.

    c. if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to (a) and (b) above.

36. Bidders shall be requested to accept correction of arithmetical errors. Failure to accept the corrections shall result in the rejection of the Bid.

37. Amicable Settlement

    VU and the Supplier shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with this contract.

    Except as otherwise provided in the contract, any difference, dispute or question arising out of or with reference to this contract which cannot be settled amicably, shall within **(30) thirty days** from the date that either party informs the other in writing that such difference, dispute or question exists, be referred to arbitration.

    Within 30 days of the said notice, one arbitrator shall be nominated in writing by VU and one arbitrator shall be nominated in writing by the Supplier. The two arbitrators shall initiate arbitration proceedings at Islamabad. In case the two arbitrators do not reach any agreement, a third arbitrator shall be selected by the two arbitrators.

    The arbitration shall be conducted in accordance with the rules of procedure set forth in the Arbitration Act 1940 or as subsequently amended. The contract of the majority of the arbitrators shall be final and binding on both Parties. Each party shall bear the cost of its own arbitrator and the cost of the third arbitrator shall be borne equally by both parties. In the event of an arbitrator resigning or becoming incapable or unable to act, the party nominating such arbitrator shall be entitled to appoint another one in the place of the outgoing arbitrator. Proceedings shall continue without recommencing as if such arbitrator had been originally nominated.

    An abnormally Low Bid is one where the Bid price, in combination with other constituent elements of the Bid, appears unreasonably low to the extent that the Bid price raises material concerns with the Procuring Agency as to the capability of the Bidder to perform the Contract for the offered Bid price. In the event of identification of a potentially abnormally Low Bid, the VU shall seek written clarification from the Bidder, including a detailed price analysis of its Bid price in relation to the subject matter of the contract, scope, delivery schedule, allocation of risks and responsibilities and any other requirements of the bidding document. After evaluation of the price analysis, in the event that the VU determines that the Bidder has failed to demonstrate its capability to perform the contract for the offered Bid price, the VU shall reject the Bid.

38. The University reserves the right to accept or reject any bid or annul the procurement process at any time in accordance with PPRA Rules.

39. Payment shall be made as per actual verified quantity after submission of the Sales Tax Invoice, duly verified by the concerned department, in accordance with SRO 660(I) 2007. Income tax and GST shall be withheld as per Government rules.

40. Delivered items must conform to standard specifications and VU requirements and free from any defect(s) in all respect.

MANDATORY DOCUMENTS REQUIRED

(MUST BE ATTACHED WITH THE TECHNICALPROPOSAL ON TOP OF ALL DOCUMENTS AND TO BE SUBMITTED AT THE TIME OF OPENING OF TECHNICALS BID(S):

Sr. No	Description	Attached (Yes / No)
	General	
1	Bid Security in the shape of DD/PO/CDR or a Bank Guarantee amounting to Rs. 300,000/-	
2	Tender document duly filled, signed & stamped by the bidder	
3	Tender Fee Rs. 2,000/- in shape of paid Bank Deposit Slip	
4	Financial soundness certificate / Account Maintenance Certificate issued by Bidder's bank	
5	Affidavit on Rs.100 stamp paper that the bidder/firm/company is not Blacklisted from PPRA	
6	Copy of NTN & GST certificate	
7	Copies of Last Three Tax Return of both Income Tax and Sales Tax	
8	Validity of the bid for a period of three (3) months (Confirmation required)	
9	Delivery of ordered items within given Days (Confirmation required on Letterhead)	
	Technical (Certificate(s) required issued by the Principal/Manufacturer of quoted brand)	
1	The bidder must have offices/workshop at 03 major cities, i.e., Lahore, Islamabad/Rawalpindi, Karachi (Please mention the current addresses in the bid)	
2	The bidder must be authorized partner of the quoted brand.	
3	The bidder must submit a current/valid Authorization certificate to participate in this tender issued by the Principal/Manufacturer of the quoted items.	
4	The brand should be established since a minimum of ten (10) years.	
5	Local partner representation should be at least three (03) years.	
6	Warranty and support Coverage from Principal/Manufacturer through its authorized distributor/dealer.	

NOTE:

- Your bid will be rejected if any of the above documents are not attached with the bid.
- Warranty certificate on the supplier(s) letterhead shall be provided in original by the successful bidder(s)/supplier(s) upon delivery along with the invoice.

Bidder's Name:_____

Sign & Stamp of Bidder: _____

EVALUATION CRITERIA:

i. Initial scrutiny of tender documents/bids
ii. Technical Evaluation as per BOQ
iii. Evaluation of Demo / sample Unit(s) **if needed**
iv. Selection of technically compliant bidder(s)
v. Financial Evaluation of compliant bidders(s)
vi. Award of tender to the Most advantageous bidder(s)

Procurement Department
Directorate of Finance
Virtual University of Pakistan
Sir Syed Memorial Society Building,
19-Ataturk Avenue, G-5/1, Islamabad
UAN: 051-111-880-880
Technical Queries Ext 1651
Financial Queries 1323, 1354
VU NTN: 4388557-8
Email: po@vu.edu.pk

Declaration by the Bidder
Should be on Rs.100/- stamp paper

I, being the owner/proprietor/director/authorized representative of the firm/company, hereby certify that I have read and understood all the terms and conditions of this office and accept the same without any reservation.

I further confirm that all items and/or services provided shall be of the best quality, strictly in accordance with the prescribed standards, specifications, and requirements. I undertake to replace or redo, at my own cost, any item or service found to be substandard, unsatisfactory, or defective, without any claim whatsoever against the Virtual University of Pakistan (VU).

In case of failure to comply with the above, I understand and agree that VU shall have the right to impose penalties, confiscate the earnest money and blacklist the firm/company in accordance with applicable rules.

I hereby also confirm to provide on-site warranty including service & support with parts for complete unit(s) (where applicable) from the date of delivery.

I further declare that, as of the date of this undertaking, the firm/company is not blacklisted by the Public Procurement Regulatory Authority (PPRA) or any other government organization.

SIGNATURE & STAMP

Name: _____

Designation: _____

TERMS AND CONDITIONS OF CONTRACT FOR SUCCESSFUL BIDDER:

TERMS AND CONDITIONS OF CONTRACT FOR THE SUCCESSFUL BIDDER

1. **Implementation and Deployment**

   The OEM/Successful Bidder shall be responsible for the complete implementation, deployment, configuration, integration, testing, and commissioning of the proposed Endpoint Security Solution across all designated servers and endpoints. The scope shall include:

   - Installation and configuration of all software components.
   - Performance tuning and optimization.
   - Configuration of security policies in accordance with OEM best practices.
   - Functional and operational testing prior to handover.

2. **Installation Schedule**

   All installation, configuration and maintenance activities shall be planned to minimize disruption to the University's normal operations. The Successful Bidder shall coordinate implementation activities with the University and provide an implementation schedule indicating the timeline for deployment. Any planned service interruption shall only be carried out with the prior approval of Virtual University (VU).

3. **Documentation**

   Upon successful implementation, the Successful Bidder shall provide comprehensive technical documentation in both hard and soft copy, including but not limited to:

   - Endpoint Security configuration documentation.
   - Server Security configuration documentation.
   - Detection and Response configuration.
   - Attack Surface Management configuration.
   - Security policies and exceptions.
   - System architecture and deployment diagram.
   - Administrative and operational manuals.
   - Backup and restoration procedures (where applicable).

4. **Compatibility**

   The Successful Bidder shall ensure that the proposed solution is fully compatible with the University's existing ICT infrastructure, including supported operating systems, Active Directory, virtualization platforms, and other required integrations. Any additional software components, licenses, or utilities required for the complete operation of the proposed solution shall be supplied by the Successful Bidder at no additional cost to the University.

5. **Software Updates and Upgrades**

   During the entire subscription/support period, the Successful Bidder shall provide, at no additional cost:

   - Software version upgrades.
   - Security patches.
   - Signature and threat intelligence updates.
   - Detection engine updates.
   - Feature enhancements released by the OEM.

6. **Technical Support**

The Successful Bidder shall provide comprehensive OEM-backed technical support throughout the subscription/support period, including:

- Remote and on-site support, whenever required.
- Troubleshooting and fault rectification.
- Configuration assistance.
- OEM escalation support for critical issues.

7. **Training**

OEM recommended trainings with respect to quoted solution will be arranged by the OEM/successful bidder for the quoted solution with certification track for at least two (02) VU resources through certified trainer/professional.

8. **Implementation Timeline**

The Successful Bidder shall complete the deployment, configuration, integration, testing, and commissioning of the complete solution within fifteen (15) calendar days from the date of delivery of all software licenses.

9. **Acceptance Testing**

Final acceptance of the solution shall be subject to successful completion of installation, configuration, integration, functional testing, training and demonstration that all specified features are operating satisfactorily. The project shall be considered complete only after issuance of an Acceptance Certificate by Virtual University.

10. **Warranty and Support**

The Successful Bidder shall provide comprehensive OEM-backed support and subscription services for the period specified in the BOQ from the date of deployment of complete solution. The support shall include software updates and support, technical assistance, and replacement or reactivation of licenses, where applicable.

11. **Failure to Provide warranty and Support**

Failure of the Successful Bidder to fulfill the contractual warranty, subscription, or support obligations may result in action under the applicable procurement rules and the terms of the contract, including forfeiture of performance security, imposition of penalties, termination of the contract, and blacklisting for a period of three (03) years.

12. **Integrity Pact**

The Successful Bidder shall execute an Integrity Pact in the prescribed format, affirming that no official or employee of Virtual University has any direct or indirect interest in the contract or any benefit arising therefrom. Any violation of the Integrity Pact shall render the contract liable to cancellation and may result in legal or administrative action in accordance with the applicable laws and procurement regulations.

SLA AGREEMENT FOR SUCCESSFUL BIDDER

The Successful Bidder shall provide comprehensive OEM-backed technical support for the supplied Endpoint Security Solution throughout the subscription/support period. Support shall include incident management, troubleshooting, software updates, configuration assistance, bug fixes, performance optimization, and escalation to the OEM where required.

Scope of Services

SLA time period = 03 Years

The bidder agrees to provide technical support for Endpoint Security Solution as specified in the purchase order.

Support Availability

- **Critical Incidents:** 24x7x365 support.
- **Non-Critical Incidents:** Monday to Friday during normal business hours (excluding public holidays), unless otherwise agreed.
- Support shall be available through telephone, email, remote access, and on-site visits whenever required.

1. Service Levels

Severity	Description	Initial Response Time	Resolution / Workaround Time
Critical (Severity-1)	Complete failure of the Endpoint Security Solution, management console inaccessible, widespread endpoint protection failure, ransomware outbreak, or security incident affecting production systems with no available workaround.	Within 30 minutes	Within 4 hours
High (Severity-2)	Major functionality impaired affecting multiple endpoints or critical servers, significant degradation in protection, or failure of core security functions.	Within 1 hour	Within 8 hours
Medium (Severity-3)	Partial functionality affected, isolated endpoint issues, policy deployment failures, reporting issues, or non-critical feature malfunction.	Within 4 hours	Within 1 business days
Low (Severity-4)	General queries, configuration assistance, cosmetic issues, documentation requests, or enhancement guidance.	Within 1 business day	Within 3 business days

2. Penalties

2.1 **Failure to Meet SLAs**: In the event that the bidder fails to meet the specified response time or resolution time outlined above, penalties shall be applied as follows:

- For the delay beyond the agreed response time, a penalty of Rs. 5,000/hour shall be applicable.
- For the delay beyond the agreed resolution time, a penalty of Rs. 10,000/day shall be applicable.
- If the bidder does not provide resolution within time VU reserves the right to blacklist the bidder for the period of three (03) years.

3. Miscellaneous

Any modifications or amendments to this SLA must be made in writing and signed by both parties.

4. Signatures

This SLA is executed in duplicate originals, each of which shall be deemed an original and all of which shall constitute together but one and the same agreement.

Client Signature: _____ Date: _____

Bidder Signature: _____ Date: _____

SPECIFICATIONS / DESCRIPTION

(Item 1.) Endpoint Security Solution

(Item 1a.) Standard Server Security Licenses

1. Solution required for **175 Devices.**
2. The proposed solution should provide protection and detection that is purpose built for endpoints.
3. The proposed solution must include signature-based detection and behavior monitoring detection.
4. The proposed solution must be able to provide machine learning on file and process.
5. The proposed solution must have a feature to protect against file-encrypting malware and the capability to roll back the changes made by malicious applications.
6. The proposed solution must have the ability to automatically terminate programs that exhibit abnormal behavior.
7. The proposed solution must have the ability to block processes associated with ransomware.
8. The proposed solution must have the ability to deny malicious hosts file modification, malicious program library injection, malicious Windows shell modification, malicious system file modification and malicious system process modification.
9. The proposed solution must be able to protect against CnC connections.
10. The proposed solution must include host-based firewall and web protection to prevent access to malicious websites.
11. The proposed solution must include Intrusion Prevention System (IPS) that shows CVE being protected.
12. The proposed solution must support recommended IPS configuration that ensures protection against known vulnerabilities.
13. The proposed solution must provide application control features to implement blacklisting or whitelisting or lock-down.
14. The solution must be able to restrict device access on endpoints by assigning rights to read, read / write, write and deny access to USB drives. The device control feature must also provide restrictions for Network Drives.
15. The proposed solution should protect against data leaks via USB drives and other channels based on specified sensitive content.
16. The proposed solution should be able to stop data leakage on web, email, data on keywords, data on expressions, data based on file type and block the AutoRun function on USB storage devices.
17. The proposed solution should be leader in Gartner Magic Quadrant for Endpoint Security.

(Item 1b.) Advance Server Security Licenses

1. Solution is required for **25 Servers**
2. Solution should have detection & response capability including but not limited to device isolation, process termination, IOC (Indicators of compromise) sweeping.
3. The solution must provide single dashboard for physical, virtual and cloud servers.
4. Proposed solution must have support for following OS Windows, Linux.
5. Proposed solution must provide IPS for Windows & Linux.
6. Provides layered defence against advanced attacks and provide shield against vulnerabilities on OS level and application level.
7. Should be able to detect suspicious lateral movement techniques and remote execution activities.
8. Should be able to detect suspicious file transfers and executable deployment activities over network shares and alert batch file upload on network share.
9. Should be able to identify and alert on suspicious (RDP) possible attempt of brute force.
10. Should be able to prevent access to administration share .

11. Should be able to detect and monitor usage of cloud storage and file-sharing applications.
12. Should be able to detect and monitor file transfer activities using standard and legacy file transfer protocols.
13. Should be able to detect and monitor remote administration and remote access tools.
14. The proposed solution must provide firewall feature on Windows and Linux and IPS functionality for supported Windows and Linux operating systems.
15. The proposed solution must have application control feature to quickly identify new suspicious files.
16. The proposed solution must be able to detect and alert on administrator log-ins on servers.
17. The proposed solution must be able to alert when log file is cleared (e.g. Windows Event Logs).
18. The proposed solution must be able to detect PowerShell command execution.
19. Should be able to detect ftp event on Windows and hosts file modification on Windows.
20. Should be able to detect file attribute changes in /usr/bin and /user/sbin on Unix.
21. Should be able to detect change in the attribute Permissions of any log file under /var/log path.
22. Should be able to alert when command history is cleared.
23. Should be able to detect installation of root certificate and removable devices on Linux.
24. Should be able to identify create and delete activity of users and groups.
25. Should be able to detect when task scheduler entries are modified, Windows start up programs are modified and a software is installed or uninstalled on Unix.
26. Should be able to provide lock-down ability (to block all new executable) if needed on Linux.
27. Should be able to provide information on the user and process associated with launching of executable.
28. Should be able to provide a way to block suspicious list of hashes on Linux and a mechanism to block suspicious web traffic.
29. Should be able to list down the vulnerabilities being protected with relevant CVE and CVSS score.

(Item 1c.) Detection & Response Licenses

1. The Solution is required for **200 Devices.**
2. The proposed solution should support integration across endpoint, email and network.
3. The proposed solution must include pre-built detection models for alerts, which can be investigated upon.
4. The proposed solution must allow creation of customized detection models for alerts, which can be investigated upon.
5. The detection models, which generate the alert triggers, must combine multiple rules and filters using a variety of analysis techniques including data stacking and machine learning.
6. The proposed solution must provide a list of correlated alerts that contain all the security-related events detected in our environment.
7. The proposed solution must include comprehensive view that lets user focus on high-priority correlated alerts to start investigations.
8. The proposed solution must display correlated alerts that help identify and mitigate potential system breaches.
9. The proposed solution must have the ability to create insights using advanced correlation and machine learning techniques.
10. The proposed solution must provide predefined threat hunting queries on threats to aid in search queries.
11. The solution should provide advanced investigation and threat analysis capabilities utilizing automation, machine learning, artificial intelligence, or equivalent technologies.
12. The proposed solution based on gather telemetry must be able to determine if certain indicators signal an ongoing attack, enabling customer to take timely prevention, investigation and mitigation actions against targeted attack campaigns.

13. The proposed solution must provide case management feature to keep track of incident investigations, procedures, and supplemental information for threat alerts and risk events.
14. The proposed solution must pinpoint activities to MITRE ATT&CK Tactics and Techniques.
15. The proposed solution must provide the ability to perform automated IOC based intelligence sweeping.
16. The proposed solution provides the ability to collect file for further analysis from managed endpoints.
17. The proposed solution should provide the ability to dump process memory, isolate endpoint, take remote shell of managed endpoints, run remote custom scripts and integrate with Azure AD, Active Directory, Okta or OpenLDAP.
18. The proposed solution must provide the ability to execute automated response playbook with the ability to isolate affected endpoint.
19. The proposed solution must allow collection of system information, OS version, interface detail, volume information, and system drive environment.
20. The proposed solution must allow collection of file timeline focusing on creation time, absolute path, modification time, access time, record time, directory information, file name, file version and file size.
21. The proposed solution must allow collection of process information focusing on process name, PID, Parent PID, creation time etc.
22. The proposed solution must allow collection of autostart entries, scheduled tasks, registry information and event logs.
23. The proposed solution must allow leveraging of valuable indicators of potential threats from both custom and curated intelligence reports for auto and manual sweeping.
24. The solution should support integration with industry-standard threat intelligence platforms and feeds, including STIX/TAXII or equivalent mechanisms.
25. The solution should support advanced endpoint investigation and threat hunting capabilities using industry-standard frameworks such as YARA, OSQuery, or equivalent technologies.
26. The solution should support secure communication through direct Internet connectivity, relay servers, gateways, proxies, or equivalent mechanisms.
27. The proposed solution must allow minimum 30 days of telemetry retention either natively or through integrated storage options.
28. The proposed solution must allow automated collection and submission of files to sandbox for analysis.
29. The proposed solution must allow manual submission of files to cloud sandbox for analysis.
30. The proposed solution must allow manual submission of URLs to cloud sandbox for analysis.
31. The proposed cloud sandbox offering for manual submission must be able to analyze the following password protected document file types DOCX, PPTX, XLSX, PDF, 7ZIP, RAR and ZIP in their original form with the option to specify password.
32. The proposed solution must provide a detailed PDF report of detection.
33. The proposed vendor must be leader in Gartner's Endpoint Protection Report and Forrester's Network Analysis & Visibility Report

(Item 1d.) Attack Surface Management Licenses

1. Solution is Required for **200 Devices**
2. Support integration with SIEM, XDR, SOAR and other security platforms through documented APIs or standard connectors.
3. The proposed solution should provide visibility into the organization's security posture by presenting information related to asset risks, detected threats or ongoing attacks, vulnerabilities, and other relevant security risk factors.
4. The proposed solution should provide an overall assessment of the organization's security posture based on analysis of relevant risk factors such as vulnerabilities, threat exposure, detected security events, darkweb and configuration-related risks.

5. The proposed solution should provide visibility into organizational security exposure by identifying vulnerabilities, configuration weaknesses, suspicious user activities, and other relevant security risks across managed assets and environments.
6. The proposed solution must provide dashboards showing attack trends, threat severity, attack frequency and overall threat exposure occurring in the organization.
7. The proposed solution should provide monitoring and reporting capabilities for security configuration and operational health of managed assets, including deployment status, feature enablement, software versions, and system health information.
8. The proposed solution should be able to continuously identify, categorize and document all the assets within the organization's digital ecosystem. Assets should be listed and categorized but not limited to the following asset categories:
    a. Internet-facing Assets
    b. Internal device Assets
    c. Account Assets
    d. Application Assets
9. The proposed solution should be able to provide contextual visibility into all assets by:
    a. Criticality based on asset attribute and activity.
    b. Historical risk assessment result
10. The proposed solution should be able to integrate with third party vendors for ingest or enrich attack surface data.
11. The proposed solution should have built-in support for security playbooks that can be used for automated remediation.
12. As part of External Attack Surface Management, the proposed solution should be able to assess the security posture of Internet and other external facing assets in the organization.
13. As part of External Attack Surface Management, the proposed solution should be able to list all domains and respective subdomains belonging to the organization.
14. As part of External Attack Surface Management, the proposed solution should be able to list all Public IP addresses belonging to the organization.
15. As part of External Attack Surface Management, the proposed solution should be able to provide the Internet-facing asset's latest risk score, host provider, services, ports and show when the asset was last seen.
16. As part of External Attack Surface Management, the proposed solution must be able to provide risk assessment for each domain and IP address asset and assign a risk score that can be monitored over time.
17. The proposed solution should provide the capability to assign and manage priority or risk classification levels for external assets such as domains and IP addresses, with the ability for administrators to manually adjust classifications as required.
18. As part of External Attack Surface Management, the proposed solution should be able to summarize IP address asset's location per country and provide geographic visibility of Internet-facing assets, including country or region information.
19. As part of External Attack Surface Management, the proposed solution should be able to provide the ability to add company owned domains, subdomains and IP addresses for discovery.
20. For internal device assets, the proposed solution should be able to utilize multiple discovery data providers.
21. For internal device assets, the proposed solution should be able to provide the internal device asset's latest risk score, OS, IP address, last user, vulnerabilities, discovery source and when the device was first and last seen.
22. For internal device assets, the proposed solution should be able to provide risk assessment for each device asset and assign a risk score that can be monitored over time.
23. For internal device assets, the proposed solution should be able to classify or prioritize device assets based on their importance, business relevance, or associated risk within the organization. The

solution should also allow authorized administrators to modify or customize the assigned classification or priority levels.

24. For internal device assets, the proposed solution should be able to identify managed and unmanaged devices.
25. For internal device assets, the proposed solution should be able to list all discovered internal device assets.
26. For internal device assets, the proposed solution should be able to show device asset's cloud application usage and activity.
27. For internal device assets, the proposed solution should be able to show device asset's use of sanctioned and unsanctioned cloud applications.
28. For internal device assets, the proposed solution should be able to provide comprehensive asset visibility and profiling, including device information such as operating system, device type, network and user-related details, asset activity, usage information, connection details, and associated security or risk indicators.
29. For internal device assets, the proposed solution should be able to perform Response Actions (for example: Isolate, Remote Shell, Run Custom Script).
30. For account assets, the proposed solution should be able to utilize multiple discovery data providers
31. For account assets, the proposed solution should be able to identify both domain and service accounts.
32. For account assets, the proposed solution should be able to provide the account's latest risk score, user type, role, location, job title and when the account was first and last seen.
33. For account assets, the proposed solution should be able to provide risk assessment for both domain and service accounts and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events and risk level for each discovered risk.
34. For account assets, the proposed solution should be able to Provide risk-based prioritization and classification of user and service accounts for both domain and service account. Account's criticality indicates the importance of the account in an organization. Administrators should be able to manually change the account criticality rating.
35. For account assets, the proposed solution should be able to enumerate application roles granted to discovered service accounts.
36. For account assets, the proposed solution should be able to enumerate granted consent permissions to discovered service accounts.
37. For account assets, the proposed solution should be able to list all discovered accounts and able to show account's cloud application usage and activity.
38. For account assets, the proposed solution should be able to show account's use of sanctioned and unsanctioned cloud applications.
39. For account assets, the proposed solution should be able to show account's latest account risk score, user type, role, location, job title and when the account was first and last seen.
40. For account assets, the proposed solution should be able to provide a summary of an account by building an asset profile. Details should include basic account info (level, role, group membership, etc.), Activity, Device Usage, Email usage information, Identity-related risk assessment and account security posture information.
41. For account assets, the proposed solution should be able to perform Response Actions (for example: disable account, enable account, force password reset).
42. For application assets, the proposed solution should be able to utilize multiple discovery data providers (Reliance to existing agent should be supplemented by additional discovery providers).
43. For application assets, the proposed solution should be able to identify both Cloud and Local Applications.
44. For application assets, the proposed solution should be able to allow a cloud application to be set as a sanctioned or an unsanctioned app.

45. For application assets, the proposed solution should be able to provide the application's latest risk level, category, which users are using the application, which devices the application were accessed, app usage, whether the application is sanctioned, and when the application was last seen.
46. For application assets, the proposed solution should be able to provide risk level for both cloud and local applications and assign a risk level for each.
47. For application assets, the proposed solution should be able to show compliance information for cloud applications.
48. For application assets, the proposed solution should be able to show cloud application usage by users.
49. For application assets, the proposed solution should be able to show cloud application usage by devices.
50. The proposed solution should be able to provide following vulnerability management metrics for both internal and Internet facing assets over time and be able to provide historical trend analysis and benchmarking information where available:
    a. Highly Exploitable unique CVEs.
    b. Mean Time to Patch.
    c. Average Unpatched Time
    d. Vulnerable endpoints
51. The proposed solution should be able to support automation/playbook actions for vulnerability detection events.
52. Vulnerability Assessment and Prioritization should be based on both external factors (threat intel, e.g. whether a CVE is highly actively exploited) and internal factors (asset criticality, exploit attempts based on detection logs).
53. The proposed solution should be able to provide capability to identify emerging or zero-day vulnerabilities using threat intelligence and provide recommended remediation where available.
54. The proposed solution should be able to keep track of discovered risks events by specifying remediation status for every discovered event. Events status should be able to be assigned per event (for example: Remediated, Dismissed etc.).
55. The proposed solution should be able to provide reports that can be generated on demand or via schedule.
56. The proposed solution should allow generated reports to be sent via email and reports content to be filtered to narrow down output based on selected criteria.
57. The proposed solution must be the leader in Forrester Attack Surface Management.

FINANCIAL PORTION

(Must be placed in separate sealed envelope marked as "FINANCIAL PROPOSAL"
Items List as Per Specifications Given In Technical Portion

Sr. No.	Description	Unit Price Rs.	GST (If applicable)	Total Unit Price Rs.	Qty	Total Amount Rs.
Item# 1	Endpoint Security Solution				01	
	Grand Total Amount Rs.					

Grand Total Amount in words (Rs.): _____

_____

Rate of GST applied: _____ %