Ref. No.: DAVV/ITC/Antivirus/2023-24/1

On-Line Tender Notice

Tenders are invited to **Supply, Installation, and configuration of Server security enterprise-level Software at IT Centre Devi Ahilya Vishwavidyalaya, Indore.** The tender document may be downloaded on payment of Rs. 2000/- (Rs. Two Thousand only) at http://www.mptenders.gov.in (main portal)

The formats of Technical and financial bid, declaration, specifications and terms & conditions, are given in the tender document and the same is available at http://www.mptenders.gov.in (main portal) and can be seen at DAVV website www.dauniv.ac.in

Sr No.	Particulars	Description
1	Name	**Supply, Installation, and configuration of Server security enterprise level Software**
2	Uploading/Publication of Tender Document	14/07/2023 by 10:30 hrs.
3	Downloading of Tender Document through website https:www.mptenders.gov.in	14/07/2023 by 11:00 hrs.
4	Seek clarification start Date	14/07/2023 by 11:00 hrs.
5	Seek clarification End Date	19/07/2023 by 17:00 hrs.
6	Contact No.	0731-2761358 , head.itc@dauniv.ac.in
7	Last date of tender submission	03/08/2023 by 17:00 hrs.
8	Technical tender opening	04/08/2023 by 11:00 hrs.
9	Financial Tender Opening	Date will be notified on University website https:// www.dauniv.ac.in
10	Tender Security/Earnest Money Deposit (EMD)	INR Rs.12000 /- (Rs. Twelve thousand Only) to be paid online through e-procurement portal in favor of Registrar, Devi Ahilya Vishwavidyalaya, Indore. Tenderer is required to Upload the scanned copy of e-transaction details.
11	Tender Fee	INR Rs. 2000/- (Rupees Two Thousand only) (non-refundable) + GST to be paid online through e-procurement portal in favor of Registrar, Devi Ahilya Vishwavidyalaya, Indore. Tenderer is required to upload the scanned copy of e-transaction details.

1. The on line Technical Tender will be opened by the committee constituted for this purpose in presence of the tenderers or authorized representatives interested to be present on prescribed date. The financial tenders of technically qualified tenderers will only be opened after technical evaluation by the technical committee. The tenderers should bring ID proofs and representatives should bring the authorization letter from their authorized signatory for attending the process of tender opening.

NOTE: Any Amendment in tender, Notification etc. will not be published in News Paper, it will be uploaded at DAVV's web site www.dauniv.ac.in

Registrar,
DAVV

INFORMATION TECHNOLOGY CENTRE, DAVV, INDORE

CENTRAL LIBRARY BUILDING,(UTD), KHANDWA ROAD CAMPUS, INDORE ☎ 0731-2761358

DAVV/ITC/Antivirus/2023-24/1 **Date:- 14/07/2023**

Online tenders are invited under two bid systems (Technical and Financial) for the **Supply, Installation, and configuration of Server security enterprise-level Software (7 users) at IT Centre, Devi Ahilya Vishwavidyalaya, Indore.** The tender document may be downloaded on payment of Rs. 2000/- (Rs. Two Thousand only) from http://www.mptenders.gov.in (main portal) and can be seen at DAVV website www.dauniv.ac.in.

The formats of the Letter, Technical bid, and financial bid are given in Annexure I, Annexure II, and Annexure III respectively.

General Terms and Conditions:

1. Tenderer must submit OEM authorization letter failing this will result in tender rejection.
2. The letter must also mention that all support and services will be ensured by OEM for the successful and effective execution of software.
3. Attach technical leaflet to ensure that quoted product has all required mentioned features.
4. We do not intend to call vendors for financial negotiations. The vendor should, therefore, quote their lowest possible rates.
5. Quotations received after the due date and time will be summarily rejected**.**
6. DELIVERY PERIOD: 15 days from the date of placing the order.
7. The Vendor should not be blacklisted by any Government of India Agency /PSU, or any State Government department. The Vendor shall furnish a written declaration in the format given in section III.

Annexure I

DAVV/ITC/Antivirus/2023-24/1

To:
The Registrar
DAVV, Indore.

Dear Sir,

We, the undersigned, have examined the Tender Document, hereby offer to **Supply, Installation and configuration of Server security enterprise-level Software (7 users).** We hereby submit our proposal, which includes general information, declaration, Technical proposal, and Commercial proposal. We have submitted the Earnest Money Deposit online, as mentioned in the tender document.

All the rates quoted in our proposal are in accordance with the terms specified in the tender documents. All the prices and other terms and conditions of this proposal are valid for a period of 180 calendar days from the last date of submission of tenders.

We do hereby confirm that our prices include all taxes including GST or other tax. We have studied the clauses relating to Indian Taxes and hereby declare that if any Tax, Surcharge on Tax, and any other Corporate Tax is altered under the law, we shall pay the same.

Yours sincerely,

Signature with seal

Name and Designation of Authorized Signatory

Date & Place

Online Technical Bid A

I. General Information

Sno.	Particulars	Details
1	Name and Address of the Tenderer	
2	Year of establishment	
3	Contacts	
	Office Telephones	
	Mobile No.	
	e-mail address	
4	Category of tenderer (whether company, partnership firm or proprietary concern)	
5	Name of the Chief Executive and Telephone No	
6	GST Registration Nos.	
7	Income Tax PAN / GIR No	

Signature with seal:

Name and Designation of Authorized Signatory

Date & Place:

II. Compliance with technical specifications:

S.No.	Technical Specifications	Product Name and Code
1	**Supply, Installation and configuration of Server Security enterprise level software (7 users) – per server VM for agentless and agent-based Security with Anti-malware, Behavioral Analysis, Web reputation, Intrusion Prevention, Firewall, and application control, Integrity Monitoring and Log inspection modules, including security Manager, 1 per VM host with 3 years license subscription bundle with support warranty from OEM.** **The software must include the following features:**	
		Compliance (Yes/No)

S.No	Technical Specifications - Server Security		Compliance (Yes/No)
1	**Security Modules**	All modules i.e. Antimalware, HIPS, Firewall, Application control, FIM, Log correlation, C&C prevention must be available in single agent	
2	**Supported OS Platforms**	The proposed server security solution must support multiple platforms of server operating systems i.e. Windows, Linux RedHat,CentOS,Oracle,Debian,SUSE, Ubuntu,Solaris,AIX,Amazon Linux etc.	
		The Proposed solution must support Anti-malware, HIPS, Integrity Monitoring, Host Firewall for the below mentioned server operating system:	
		Microsoft Windows Server (2008 &2008 R2, 2012 & 2012 R2, 2016,2019), Red Hat Enterprise Linux (6,7,8), Solaris (10.0,11.0,11.1,11.2,11.3,11.4), Oracle Linux (6,7,8), AIX (6.1,7.1,7.2), CentOS (6,7,8) and Suse Linux (11,12,15)	
3	**Firewall Security Feature**	The firewall shall be bidirectional for controlling both inbound and outbound traffic and should have the capability to define different rules to different network interfaces	
		Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc. and should detect reconnaissance activities such as port scans and should support stateful inspection functionality	
		Solution should provide policy inheritance exception capabilities and ability to lock computer (prevent all communication) except with management server.	

		Solution should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules.	
		The firewall should be able to detect protocol violations of standard protocols and provision inclusion of packet data on event trigger for forensic purposes.	
		Solution should have security profiles that allows firewall rules to be configured for groups of systems, or individual systems.	
4	**HIPS Security Features**	The proposed solution should support Deep Packet Inspection (HIPS/IDS) and should support creation of customized DPI rules if required.	
		Deep Packet Inspection should support virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window.	
		Virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.	
		Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.	
		Solution should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (Eg. Selecting rules, configuring policies, updating policies, etc...)	
		The solution should provide recommendations for automatic removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.	
		The solution should allow imposing HTTP Header length restrictions and have the capability to inspect and block attacks that happen over SSL.	
		The solution should allow or block resources that are allowed to be transmitted over http or https connections and capable of blocking and detecting of IPv6 attacks.	

		Detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.	
		Solution should offer protection for virtual, physical, cloud and docker container environments.	
		Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).	
		Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.	
		Solution should work in Tap/detect only mode and prevent mode and support automatic and manual tagging of events also have CVE cross referencing when applicable for vulnerabilities.	
		Solution should provision inclusion of packet data on event trigger for forensic purposes and shall protect against fragmented attacks also should allow to block based on thresholds	
		Deep packet inspection should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.	
		Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto- Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.	

5	**Integrity Monitoring Security Features**	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, and registry keys to detect suspicious behavior, such as modifications, or changes in ownership or permissions.	
		The solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.	
		Solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).	
		Solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.	
		Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.	
		Solution should have automated recommendation of integrity rules to be applied as per Server OS and can be scheduled for assignment/assignment when not required.	
		Solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities.	
		In the Event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so.	
		Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be Auto-Provisioned based on Server Posture.	
		Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.	

		Solution should support the following: Multiple groups of hosts with identical parameters, Regex or similar rules to define what to monitor, Ability to apply a host template based on a regex of the hostname, Ability to exclude some monitoring parameters if they are not required, Ability to generate E Mail and SNMP alerts in case of any changes, Solution should support creation of custom Integrity monitoring rule and Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.	
6	**Anti-Malware Security Features**	Anti-malware should support Real Time, Manual and Schedule scan and should have flexibility to configure different real time and schedule scan times for different servers and should have feature to try & backup ransomware encrypted files and restoring the same as well.	
		Solution should support excluding certain file, directories, file extensions from scanning (real time/schedule) and use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies.	
		Solution should support True File Type Detection, File extension checking and have heuristic technology blocking files containing real-time compressed executable code.	
		The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects using Machine learning	
		The proposed solution should be able to perform behaviour analysis for advanced threat prevention and have its own threat intelligence portal for further investigation, understanding and remediation an attack.	
		Solution deployment should cause limited interruption to the current network environment also should have Ransomware Protection in Behaviour Monitoring.	
		Solution should have Highly Accurate machine learning - Pre-execution and Run time analysis, document exploit prevention to address known/Unknown threats.	
7	**Log Analysis functional Features**	Solution should have a Log Inspection module which provides the ability to collect and analyse operating system, databases and applications logs for security events.	

		Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules as well.	
		Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/unassigment of rules when not required.	
		Solution should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g. all Linux/Windows servers use the same base security profile allowing further fine tuning if required.	
		Solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.	
		Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.	
		Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match.	
		Ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.	
		Solution must support decoders for parsing the log files being monitored.	
8	**Application Control Functional Features**	Solution should allow administrators to control what has changed on the server compared to initial state and should prevent unknown and uncategorized applications from running on critical servers also must support Global Blocking on the basis of Hashes and create blacklist for the environment.	
		Solution should have option to allow to install new software or update by setting up maintenance mode and should have ability to scan for an inventory of installed software & create an initial local ruleset.	
		Change or new software should be identified based on File name, path, time stamp, permission, file contents etc. and must have ability to enable maintenance mode during updates or upgrades for predefined time period.	

		Logging of all software changes except when the module is in maintenance mode and Should support Windows & Linux operating systems.	
		Should have the ability to enforce either Block or Allow unrecognized software and must support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.	
9	**Command & Control Functional Features**	solution must be able to block all communication to Command & control center and must be able to identify communication over HTTP/HTTPS protocols and commonly used Http ports.	
		Solution must provide by default security levels i.e. High, Medium & low so that it eases the operational effort and Solution must have an option of assessment mode only so that URLs are not blocked but logged.	
		solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list of allowed/blocked URL's.	
10	**Management Features**	Management of proposed solution should support both windows as well as linux platform in high availability configuration for DC/DR setup.	
		The solution shall be able to deliver all the above mentioned features like Anti- malware, Host Based Firewall/ IPS, File Integrity Monitoring, Log Inspection & Application control in a single agent.	
		Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not and Agent installation should not require a restart of the server.	
		Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Active Directory.	
		Any policy updates pushed to the agent should not require to stop the agent, or to restart the system and Solution should provide ability to hide agent icon from getting displayed in system tray.	

		The solution should be able to automate discovery of new agents that are installed on any servers and should have the capability of supporting new Linux kernels as & when they are released.	
		The solution shall allow to do all configurations from the central management console like enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.	
		The solution should give the flexibility of deploying features either as agent based or agentless for different modules depending on organization's data center environment.	
		The proposed solution should be managed from a single centralized web-based management console.	
		The solution shall have the capability to disable the agents temporarily from the Central Management console & such action should be logged.	
		The solution shall allow to do all configurations from the central management console including, but not limited to enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.	
		The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.	
		Should support integration with Microsoft Active directory and should allow grouping into smart folders based on specific criteria like OS, policy etc. for easy manageability.	
		Solution should support the logging of events to a non-proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL.	
		The solution shall allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.	
		The solution should support forwarding of alerts through SNMP, E-Mail and should be able to generate detailed and summary reports.	

		The solution shall allow scheduling and E Mail delivery of reports and should have a customizable dashboard that allows different users to view based on their requirement.	
		The solution should support Web Services if it is required to export data out to other custom reporting solutions and shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.	
		Administrators should be able to selectively rollback rules applied to agents and should maintain full audit trail of administrator's activity.	
		Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.	
		OEM must have contributed at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.	
		Solution should integrate with existing APT component running in GUVNL environment also as per RFP specifications having common threat sharing platform.	
		The solution shall allow updates to happen over internet or shall allow updates to be manually imported in the central management system and then distributed to the managed agents. Additionally solution must also have an option of defining machine to be updater relay only.	
11	**Global Certification**	The Proposed solution should be Leader in server security market as per IDC latest report	
		The Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per latest Frost & Sullivan Reports	
		The proposed OEM should be in Leader Quadrant as per Gartner Magic Quadrant of EPP category from last 3 consecutive years	
		The proposed solution should be EAL 2 + certified	

Signature with seal:

Name and Designation of Authorized Signatory

Date & Place:

III . Declaration:

DECLARATION

I………………………………………………………………….. do hereby declare that our company/firm is not blacklisted by the Government of India/ any state Govt./ public sector undertaking/University and has not been involved in any litigation which threatens the solvency of the company/firm during the last five years.

I further undertake that if the above declaration probes to be wrong/incorrect or misleading our tender/contract stands to be canceled/terminated.

Signature of Authorized Person:

Name and designation:

Seal

Date: ………………
Place: ……………..