INDIAN INSTITUTE OF TECHNOLOGY GOA

At Goa Engineering College Campus
Farmagudi, Ponda, Goa 403401
E-mail: purchase@iitgoa.ac.in

GSTIN: 30AABAI1653D1ZF
PAN: AABAI1653D
TAN: BLRI08261B

Enquiry No: IITGOA/2020-21/011 **Date: 07/10/2020**

IIT Goa invites sealed quotations in single bid form for the supply and installation of the below mentioned item.

Sl.no.	Description of item	Number of floating licenses required
1	**Antivirus software with 3 years' license.** **Detailed specification is attached.**	**300**

Eligibility criteria:

1. Bidder should have the valid GST registration certification.
2. Bidder should have an ISO certification.
3. The Bidder must have supplied and installed at least 3 Antivirus software within India in last 5 (five) years with at least 200 users per installation. The supplier should provide list of installation in India with all contact details and model details so that IIT Goa can approach contact person for any feedback.
4. Bidder should have a branch / office in Goa state. Valid reference must be attached.

General terms and conditions:

1. Prices: Prices should be quoted in INR – F.O.R., IIT Goa basis only.
2. Payment terms: Within 30 days after the delivery and successful installation of item at IIT Goa.
3. Delivery and installation should be made within 4 weeks of getting a confirmed order.
4. The suppliers shall provide the banking details along with their quote on their letterhead duly signed and stamped.
5. The successful bidder has to submit a Performance Guarantee Bond for 5% of the Purchase Order value and valid till one year OR up-to warranty period, plus 60 days whichever is later from the date of issue of Purchase Order. Performance Guarantee Bond may be submitted within 15 (Fifteen) days from the date of order acknowledgment as a successful bidder.
6. Bidder should provide the onsite support as and when required throughout the license period.
7. Bidder should agree and install the software as per the IIT Goa conditions.
8. Bidder must quote the proposal for at least 3 years of license period.
9. MAF in original must be provided along with documents
10. Kindly attach the compliance certificate of specification provided against specification given in Annexure-1 with valid proof / reference. THIS IS MUST.

a. Bids without valid proof /reference will not consider for evaluation.

11. Bidder must provide the Technical specification (Annexure 1) with Financial proposal (Annexure 2) in a single sealed cover (Single bid system). Put your seal and signature on each page.
12. Validity of the price must not be less than 120 days.
13. For any clarification please email to sysad@iitgoa.ac.in before 14-10-2020.
14. All sealed quotations must be super scribed with the tender enquiry number and should reach to the Assistant Registrar (Stores & Purchase), IIT Goa, at Goa College of Engineering Campus, Farmagudi, Ponda, Goa, 403 401 by 17.00 Hrs. on or before 28/10/2020.

Sd/-

Asst. Registrar (S&P)

Annexure 1

Technical Specification-cum-Compliance Sheet

Sl.no.	Feature Description	Compliance (Yes/ No)	Proof of compliance with page no.
General Specification			
1.	OEM should be present in Gartner's "Leaders" quadrant at least 3 times in last 5 years (2015-2020) for Endpoint security.		
2.	The proposed enterprise endpoint security solution should be of Server based installation and provide enhanced protection for all desktops, laptops, servers, mobiles in the network against malware, viruses, spyware, worms, ransomware and other harmful attacks.		
3.	Must have advanced ransomware protection monitors for suspicious file encryption activities at the endpoint. Terminates malicious activities and even recovers lost files if necessary.		
4.	Solution must have: a. Ability to disable the external drive connectivity though administrator panel. b. Scan external storage devices, mobile device, network locations, email attachments, internet files automatically when connected / downloaded. c. On demand scan for all the files and folders on the system. d. Detection and block access to phishing links. e. Ability to discover unprotected computers within corporate network by IP, hostname, domain name and subnet mask. f. Option to scan rootkit, vulnerability, tracking cookies. g. Ability to exclude specific files and directories from scanning. h. Ability to scan in background without prompting the user repeatedly.		
5.	System should be configured in such a way that at no case no endpoints/remote agents will be able to communicate with OEM cloud for obtaining updates through internet.		
6.	Should support Windows & Linux operating systems.		

7.	**The solution should have latest machine learning technology in built from day one.**		
8.	**Should support the existing IIT Goa network setup without any modifications.**		
9.	**Automatic update of EPS (End Point Security) server should happen from OEM server and EPS client should get updates from EPS server.**		
10.	**a. Version updates and updates of virus definitions should happen automatically across all servers and clients without downtime.** **b. Should conserve network bandwidth, WAN bandwidth while updating clients with all policies.**		
11.	**Must provide Web threat protection by the following ways:** **a. Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings.** **b. Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location.** **c. Must have the capabilities to define Approved URLs to bypass Web Reputation policies.** **d. Must provide real-time protection by referencing online database with millions of rated Web domains.** **e. Configure Web reputation policies and assign them to individual, several, or all end users machine.**		
12.	**Should be able to deploy the Client software using the following mechanisms:** **a. Client installation Package (Executable & Microsoft Installer (MSI) Package Format), should support silent installer, unmanaged clients, specific installer for servers.** **b. Web install.** **c. Login Script setup** **d. Remote install** **e. From a client disk image**		
13.	**Must provide a secure Web-based management console to give administrators transparent access to all clients on the network.**		
14.	**Must be capable of uninstalling and replacing existing client antivirus software and to ensure unavailability of any residual part of the software.**		
15.	**The solution should support client installation on all the following:** **a. Microsoft Windows 32 bit & 64 bit versions of Windows 7, Windows 8, Windows 10 OS and higher versions if any.**		

	b. Microsoft Windows Server 2008,2012,2016,2019 with all its versions and higher versions if any. c. Linux latest versions.		
16.	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack.		
17.	Solution should have single console to manage desktop AV , mail and web gateway software solution.		
18.	End user should not be able to tamper the endpoint security agent, uninstall, disable or change the security settings.		
19.	Password protection feature must be provided for client side endpoint protection.		
20.	The proposed solution must have the option of Antimalware scanning of POP3 emails.		
21.	The proposed solution should be able to detect and prevent the advanced persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.		
Server Security Specifications			
22.	Management Server installation should support either Windows or Linux operating system.		
23.	Anti-malware should support Real Time, Manual and Schedule scan.		
24.	Solution should have flexibility to configure different real time and schedule scan times for different servers.		
25.	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc.		
26.	Solution should provide policy inheritance exception capabilities.		
27.	Solution should have the ability to lock computer (prevent all communication) except with management server.		
28.	Solution should have ability to run internal port scan on individual servers to know the open ports which will help administrator create rules.		
29.	The Solution should support Deep Packet Inspection (HIPS/IDS).		
30.	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.		
31.	Deep Packet Inspection should support virtual patching of both known and unknown vulnerabilities until the next scheduled maintenance window.		
32.	Deep Packet Inspection should support virtual patching of both known and unknown vulnerabilities until the next		

	scheduled maintenance window.		
33.	**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. Smart 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.**		
34.	**Deep packet inspection should have signatures to control 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.**		
35.	**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...)**		
36.	**Should provide recommendation for removing 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.**		
37.	**The solution should allow imposing HTTP Header length restrictions.**		
38.	**The solution shall have the capability to inspect and block attacks that happen over SSL.**		
39.	**The solution should allow or block resources that are allowed to be transmitted over http or https connections.**		
40.	**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.**		
41.	**Solution should be capable of blocking and detecting of IPv6 attacks.**		
42.	**Solution should offer protection for virtual, physical, cloud environments.**		
43.	**Solution should support automatic and manual tagging of events.**		
44.	**Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behavior, such as modifications, or changes in ownership or permissions.**		
45.	**The solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.**		
46.	**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.		
47.	**Solution should have a Log Inspection module which provides the ability to collect and analyze operating system, databases and applications logs for security events.**		
48.	**Solution should be able to recommend the rules to be applied on individual hosts/endpoints.**		
49.	**The solution shall support operating systems like Windows, Linux (multiple variants), AIX, Solaris and HP-UX.**		
50.	**Solution should have single centralized web based management console.**		
51.	**The solution shall be able to deliver all the above mentioned features like Firewall, Anti-malware, Deep Packet Inspection, Integrity Monitoring, Log Inspection & Application control in a single agent.**		
52.	**Agent installation should not require a restart of the server.**		
53.	**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.**		
54.	**The solution should be able to automate discovery of new agents that are installed on any servers.**		
55.	**The solution shall have the capability to disable the agents temporarily from the Central Management console & such action should be logged.**		
56.	**The solution shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.**		
57.	**Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.**		
58.	**The solution shall allow updates to happen over the internet, or shall allow updates to be manually imported in the central management system and then distributed to the agents.**		
59.	**Solution should have API level integration with public cloud service providers like AWS & Azure from the management console.**		
60.	**Report generation should include followings.** **<u>Management reports</u>** **a. Virus detection reports** **b. Detailed infected files / systems report.** **c. Detailed antivirus deployment reports including**		

	successful, pending and failure. **d. All reports must be comparative by day, week and month wise.** **e. Ability to export the reports in PDF, XML, HTML & excel or equivalent format.** **<u>User reports</u>** **a. Should generate detailed report including IP address, hostname, filename, timestamp and threat details.** **b. Ability to export the reports in PDF, XML, HTML & excel or equivalent format.**		
61.	**Documentation must be provided with following features.** **a. Administrator and User guide.** **b. Detail process of antivirus software deployment, configuration and usage.**		

Name of the Firm	
Postal Address	
Contact Person	
Contact number	
Email ID	

Annexure 2

Financial proposal

Sl.no.	OEM	Description of Item	Number of licenses	Rate per license	Total
1					
2					
3					
	Sub Total				
	GST @ 5%*				
	Grand Total				
In words:					

* **IIT Goa will provide relevant taxation related documents for GST applicable at 5%.**

FORMAT FOR PERFORMANCE GUARANTEE BOND

(To be typed on Non-judicial stamp paper of the value of Indian Rupees of One Hundred) (TO BE ESTABLISHED THROUGH ANY OF THE NATIONAL BANKS (WHETHER SITUATED AT GOA OR OUTSTATION) WITH A CLAUSE TO ENFORCE THE SAME ON THEIR LOCAL BRANCH AT GOA OR ANY SCHEDULED BANK SITUATED AT GOA. BONDS ISSUED BY CO-OPERATIVE BANKS ARE NOT ACCEPTED.

To,
The Registrar,
Indian Institute of Technology, Goa
Farmagudi, Ponda,
Goa – 403401

LETTER OF GUARANTEE

WHEREAS Indian Institute of Technology, Goa (Buyer) have invited Tenders vide Tender No..... Dt. ..... for purchase of .....

AND

WHEREAS the said tender document requires that any eligible successful tenderer (seller) wishing to supply the equipment / machinery, etc. in response thereto shall establish an irrevocable Performance Guarantee Bond in favour of **"Registrar, Indian Institute of Technology, Goa"** in the form of Bank Guarantee for Rs ..... (**5% (five percent) of the purchase value**) and valid till **one year or upto warranty period whichever is later** from the date of issue of Performance Guarantee Bond may be submitted within 15 (Fifteen) days from the date of Order Acknowledgment as a successful bidder.

NOW THIS BANK HEREBY GUARANTEES that in the event of the said tenderer (seller) failing to abide by any of the conditions referred in tender document / purchase order / performance of the equipment / machinery, etc. this Bank shall pay to Indian Institute of Technology, Goa on demand and without protest or demur Rs..... (Rupees.....).

This Bank further agrees that the decision of Indian Institute of Technology, Goa (Buyer) as to whether the said Tenderer (Seller) has committed a breach of any of the conditions referred in tender document / purchase order shall be final and binding.

We, ... (name of the Bank & branch) hereby further agree that the Guarantee herein contained shall not be affected by any change in the constitution of the Tenderer (Seller) and/ or Indian Institute of Technology, Goa (Buyer).

Notwithstanding anything contained herein:

1. Our liability under this Bank Guarantee shall not exceed Rs. ..... .
   (Indian Rupees ..... only).
2. This Bank Guarantee shall be valid up to .....(date) and
3. We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only and only if IIT Goa serve upon us a written claim or demand on or before ..... (date).
4. This Bank further agrees that the claims if any, against this Bank Guarantee shall be enforceable at our branch office at ..... situated at ..... (Address of local branch).

Date:

Yours truly,

Signature and seal of the Guarantor:

Name of Bank:

Instruction to Bank: Bank should note that on expiry of Bond Period, the Original Bond will not be returned to the Bank. Bank is requested to take appropriate necessary action on or after expiry of bond period.