NETAJI SUBHAS OPEN UNIVERSITY
DD 26, Sector – I, Salt Lake, Kolkata – 700064
Tele-Fax: 03340663224, Ph: 0334066-3213/3200
Website: www.wbnsou.ac.in

Memo No.: AC/095/17-18 Dated: 06.07.2017

Sealed Quotations are being invited from reputed vendors for supply & installation of Server, OS, Device CAL and Antivirus at Examination Department of NSOU, Golpark Campus, Kolkata. The detail specifications are mentioned hereunder.

Specification: **Server, OS, Device CAL, Antivirus and Installations**

SL. NO.	ITEM DESCRIPTION
1.	**HP DL180 Gen9 8SFF CTO Server** 1 × HPE DL180 Gen9 E5-2630v4 Processor 2 × HPE 16 GB 2R×4 PC4-2400 T-R Memory 3 × HPE 1.8 TB SAS 10K SFF SC 512e HDD 1 × HP 9.5mm SATA DVD-RW HP H240 FIO Smart HBA 2 × HPE 900 W AC 240 VDC Power supply
2.	Win Svr STD Core 2016 SNGL OLP 2Lic NL Academic Core Lic
3.	Windows Server 2016 Device CAL OLP NL Academic
4	Enterprise Security (Trend Micro) for Endpoints Standard for 3 years for 10 users

Data migrations from old servers to this server are compulsory in installation part.

NETAJI SUBHAS OPEN UNIVERSITY
DD 26, Sector – I, Salt Lake, Kolkata – 700064
Tele-Fax: 03340663224, Ph: 0334066-3213/3200
Website: www.wbnsou.ac.in

Sr No	Specifications	compliance
	Antivirus Protection and Other features	
1	Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.	Yes
2	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	Yes
3	Must include capabilities for detecting and removing rootkits	Yes
4	Must provide Real-time spyware/greyware scanning for file system to prevent or stop spyware execution	Yes
5	Must have capabilities to restore spyware/grayware if the spyware/grayware is deemed safe	Yes
	Must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation	Yes
7	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process	Yes
8	To address the threats and nuisances posed by Trojans, the solution should be able to do the following:	Yes
8.1	Terminating all known virus processes and threads in memory	Yes
8.2	Repairing the registry	Yes
8.3	Deleting any drop files created by viruses	Yes
8.4	Removing any Microsoft Windows services created by viruses	Yes
8.5	Restoring all files damaged by viruses	Yes
8.6	Includes Cleanup for Spyware, Adware etc	Yes
9	Must be capable of cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether	Yes
10	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak	Yes
11	Behavior Monitoring	Yes
11.1	Must have behavior monitoring to restrict system behavior, keeping security-related processes always up and running	Yes
11.2	enable Certified Safe Software Service to reduce the likelihood of false positive detections	Yes
12	Must provide Real-time lock down of client configuration – allow or prevent users from changing settings or unloading/uninstalling the software	Yes
13	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	Yes
14	CPU usage performance control during scanning	Yes

14.1	Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer	Yes
14.2	Adjusts the scanning speed if:	Yes
14.2a	The CPU usage level is Medium or Low	Yes
14.2b	Actual CPU consumption exceeds a certain threshold	Yes
15	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	Yes
16	Should have Integrated spyware protection and cleanup	Yes
17	Should have the capability to assign a client the privilege to act as a update agent for rest of the agents in the network	Yes
19	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	Yes
20	Safeguards endpoint mail boxes by scanning incoming POP3 email and Outlook folders for Threats	Yes
21	shall be able to scan only those file types which are potential virus carriers (based on true file type)	Yes
22	Should be able to detect files packed using real-time compression algorithms as executable files.	Yes
23	Client machine acting as update agent which is delivering pattern updates to rest of the machines in the LAN, should have the capability to upgrade program upgrades also. No separate web server should be required	Yes
24	Should have a provision for setting up a local reputation server so that for verifying reputation of any file, endpoints should not contact Internet always.	Yes
25	Shall be able to scan Object Linking and Embedding (OLE) File	Yes
26	Protect documents against unauthorized encryption or modification to	Yes
27	Should monitor newly encountered programs downloaded through HTTP or email.	Yes
28	Should capable to inspection the program to detect & Block for Compromised executable files.	Yes
29	Anti-exploit Protection : Should capable to terminate that exhibit abnormal behaviour associated with exploit attacks	Yes
30	Enable program inspection to detect & block compromised executable files	Yes
31	Block processes commonly associated with ransomware	Yes
32	High Fidelity Machine Learning to perform in-depth file analysis to detect emerging unknown security risks	Yes
Cloud computing		
1	Must Have in the cloud based protection and support for Online and Offline mode client protection	Yes
1.1	Must provide Web threat protection by the following ways:	Yes
1.1a	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	Yes
1.1b	Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location	Yes

NETAJI SUBHAS OPEN UNIVERSITY
DD 26, Sector – I, Salt Lake, Kolkata – 700064
Tele-Fax: 03340663224, Ph: 0334066-3213/3200
Website: www.wbnsou.ac.in

1.1c	Must have the capabilities to define Approved URLs to bypass Web Reputation policies	Yes
1.1d	Must provide real-time protection by referencing online database with millions of rated Web domains	Yes
1.1.e	Configure Web reputation policies and assign them to individual, several, or all End users machine.	Yes
1.2	Must provide File reputation service	Yes
1.2a	Must be able to check the reputation of the files hosted in the internet	Yes
1.2b	Must be able check the reputation of the files in webmail attachments	Yes
1.2c	Must be able to check the reputation of files residing in the computer	Yes
2	Solution should work on the plugin architecture so that in future if we need to enhance the of our network we can do that without a major client level activity	Yes
3	Must have smart feedback to enable feedback from the client agents to the threat research centers of the vendor. This will enable it to deliver automatic, real-time protection against the latest threats and provides "better together" security.	Yes
4	Uses any alternate method other than the conventional pattern based scanning with the following features:	Yes
4.1	Provides fast, real-time security status lookup capabilities in the cloud	Yes
4.2	Reduces the overall time it takes to deliver protection against emerging threats	Yes
4.3	Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints	Yes
4.4	Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.	Yes
Manageability and integration		
1	Should be able to deploy the Client software using the following mechanisms:	Yes
1.1	Client Packager (Executable & Microsoft Installer (MSI) Package Format)	Yes
1.2	Web install page	Yes
1.3	Login Script Setup	Yes
1.4	Remote installation	Yes
1.5	From a client disk image	Yes
1.6	Support MS Systems Management Server (SMS)	Yes
2	Must provide a secure Web-based management console to give administrators transparent access to all clients and servers on the network	Yes
3	The management server should be able to download updates from different source if required, which could be the vendor's update server, any other server or a UNC path	Yes
4	If the update from the Management server fails, the security clients with the privilege should be able to get updated directly from the vendor's server	Yes
5	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns	Yes
6	Should have role based administration with active directory integration	Yes
6.1	To create custom role type	Yes
6.2	To add uses to a predefined role or to a custom role	Yes
7	Should have integration with the Active directory	Yes
8	Shall support grouping of clients into domains for easier administration	Yes
9	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)	Yes

10	Shall offer centrally managed Client Firewall and IDS and also have virtual patching and it should be an automated process.	Yes
11	Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network	Yes
12	All features (antivirus, anti-spyware, Enterprise Client Firewall and damage cleanup) are installed at the same time via client deployment methods and managed centrally via the web-based management console	Yes
13	Security Compliance leverages Microsoft Active Directory services to determine the security status of the computers in the network	Yes
	Platform Support	
1	Windows XP SP3 32-bit Edition	Yes
2	Windows 2003 32-bit Edition	Yes
3	Windows XP SP2 /2003 64-bit Edition	Yes
4	Windows Vista (32-bit & 64-bit)	Yes
5	Microsoft Windows Storage Server 2003	Yes
6	Windows 7, 32-bit version & 64-bit version, Win 8/8.1, Win 10	Yes
6	Microsoft Cluster Server 2003	Yes
7	Windows Server 2008 and Windows Server 2008 R2, 64-bit version	Yes
8	client installation on guest Windows 2000/2003/2008 operating systems hosted on the following virtualization applications:	Yes
8.1	VMware ESX/ESXi Server 3.5 or 4 (Server Edition)	Yes
8.2	* VMware Server 1.0.3 or later (Server Edition)	Yes
8.3	* VMware Workstation and Workstation ACE Edition 6.0	Yes
9	Should support Intel x64 processor & AMD x64 processor	Yes
10	Virtual Desktop Support: Solution should support Virtual Desktop for the following platforms:	Yes
10.1	· VMware vCenter™ 3.5 and 4 (VMware View™ 4)	Yes
10.2	· Citrix™ XenServer™5.5 and 5.6 (Citrix XenDesktop™ 4)	Yes
	Notification, Reporting and logging	
1	Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, Pager, SNMP trap or Windows NT Event log	Yes
2	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from personal firewall, and/or network virus logs exceed certain thresholds, signaling a possible attack.	Yes
3	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack	Yes
4	Shall offer customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log	Yes
	Certification & Credential	
1	The OEM company / Product should be in leader in Gartner Magic Quadrant.	Yes

NETAJI SUBHAS OPEN UNIVERSITY
DD 26, Sector – I, Salt Lake, Kolkata – 700064
Tele-Fax: 03340663224, Ph: 0334066-3213/3200
Website: www.wbnsou.ac.in

HP			
Server:	**DL180 Gen9**		
Item	**Description of Requirement**	**Compliance**	**Remarks**
Chassis	2 U Rack Mountable		
CPU	1 x E5-2630V4 Processor		
CPU L3 CACHE Memory	30MB (1 x 30 MB) L3 cache (MAX) - 15 MB (1 x 15 MB) L3 cache (MIN) depending upon processor model		
Motherboard	Intel® C610 Series Chipset		
Memory	32 GB (2 x 16 GB) Memory scalable to at least upto 512GB, using DDR4 Load Reduced DIMM (LRDIMM) memory modules. Should be capable of identifying and reporting whether genuine OEM memory is installed. Each LRDIMM should work at 2133MHz, 1. 2V even after populating all the DIMMs in the channel.		
Memory Protection	Advanced ECC with multi-bit error protection and memory online spare mode		
HDD Bays	Up to 8 SFF/16SFF/8LFF/12 LFF max, HDD/SSD		
Optical drive Bay	One optional optical drive bay to install DVD-ROM or DVD-RW .		
Hard disk drive	3 x 1.8 TB 10K SAS HDD, should be scalable upto 25.6TB (SFF) or 72TB (LFF)		
Controller	Embedded 6Gb/s SATA controller RAID controller with RAID 0/1/10/5 for SATA Disk. OR PCIe 3.0 based 12Gb/s Raid Controller with RAID 0/1/1+0/5/50/6/60/1 Advanced Data Mirroring/10 Advanced Data Mirroring with 4GB battery backed write cache (onboard or in a PCI Express slot)		
Networking features	Server should support one of the following: 1. 1Gb 2-port network adaptor supporting advanced features such as TCP segmentation offload, VLAN tagging, MSI-X, Jumbo frames, IEEE 1588, and virtualization features such as VMDQ. 2. 10Gb 2-port Ethernet adaptor supporting enterprise class features such as VLAN tagging, adaptive interrupt coalescing, MSI-X, NIC teaming (bonding), Receive Side Scaling (RSS), jumbo frames, PXE boot and virtualization features such as VMware NetQueue and Microsoft VMQ.		
Interfaces	Video - 1 4 USB ports (standard) Micro SD slot - 1		
Bus Slots	Six PCI-Express 3.0 slots		
Power Supply	Redundant Power Supplies (from early 2015)		
Fans	Hot-plug system fans		
Graphics	Integrated Matrox G200 video standard 1280 x 1024 (32 bpp) 1920 x 1200 (16 bpp)		
Industry Standard Compliance	ACPI 2.0b Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support ASHRAE A3/A4		

Embedded system management	Should support monitoring ongoing management, service alerting, reporting and remote management with embedded Gigabit out of band management portServer should support configuring and booting securely with industry standard Unified Extensible FirmwareSystem should support RESTful API integrationSystem management should support provisioning servers by discovering and deploying 1 to few servers with Intelligent ProvisioningSystem should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
Security	Power-on password Serial interface control Administrator's password TPM 1.2 UEFI		
Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Oracle Solaris VMware		
Secure encryption	System should support Encryption of the data on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.		
Provisioning	Essential tools, drivers, agents to setup, deploy and maintain the server should be embedded inside the server. There should be a built -in Update manager that can update firmware of system by connecting online.		
Remote Management	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication. 2. Server should have dedicated 1Gbps remote management port. Remote management port should have 4GB NAND flash with 1GB available for user access. NAND flash should be used for keeping system logs and downloading firmware from HP website or internal repository 3. Server should support agentless management using the out-of-band remote management port. 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur. 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available. 6. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media Group License Activation		

NETAJI SUBHAS OPEN UNIVERSITY
DD 26, Sector – I, Salt Lake, Kolkata – 700064
Tele-Fax: 03340663224, Ph: 0334066-3213/3200
Website: www.wbnsou.ac.in

Server Management	The Systems Management software should provide Role-based security		
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD. Should support automatic event handling that allows configuring policies to notify failures via e-mail, pager, or SMS gateway or automatic execution of scripts.		
	Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a Personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be accessible on premise (at customer location - console based) or off premise (using internet).		
	Should support scheduled execution of OS commands, batch files, scripts, and command line apps on remote nodes		
	Should be able to perform comprehensive system data collection and enable users to quickly produce detailed inventory reports for managed devices. Should support the reports to be saved in HTML, CSV or XML format.		
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		
	The Server Management Software should be of the same brand as of the server supplier.		
	Infra Platform /Infra Software to support a variety of different hypervisors, such as VMware, Microsoft Hyper-V, Red Hat KVM, and HP Integrity VM		
	Solution available to Deploy a fast and easy installation via software appliance delivery mode. With its own OS and Database to provide infra and lifecycle management		
	Management software should support integration with popular virtualization platform management software like vCenter, SCVMM and RedHat RHEV		

Quotations are to be submitted (after physical verification on the site) along with relevant documents like PAN, TAN, Trade License, Certificate of authorization are required to be submitted along with quotation. Govt. approved agency/vendor is required. The rate should cover the service warranty period after installation.

Delivery / Work location: Office of Controller of Examination, NSOU Golpark Campus.

Place of Submission: The box earmarked and kept at the Dept. of Finance, 4th Floor, DD-26, Salt Lake City, Kolkata-700064

Addressed to: The Finance Officer
Netaji Subhas Open University
4th Floor, DD-26,
Salt Lake City, Kolkata-700064

Last date of submission: 18th July, 2017 by 3 pm

Finance Officer
NSOU