



**THE BHARAT SCOUTS AND GUIDES**

*Creating - Better India*

**भारत स्काउट्स एवं गाइड्स**

*बेहतर भारत के निर्माण की ओर*

National Headquarters

राष्ट्रीय मुख्यालय

Society Registration No. S462 of 1950-1951

**President**

DR. ANIL KUMAR JAIN, M.P. (RAJYA SABHA)

डॉ. अनिल कुमार जैन, सांसद (राज्य सभा)

**Chief National Commissioner**

DR. K.K. KHANDELWAL, I.A.S. (RETD.)

डॉ. के.के. खण्डेलवाल, भा.प्र.से. (से.नि)

Ref. No. BSG/NHQ.

D-7-23/525/2022-23

Date: 06-06-2022

To

M/S \_\_\_\_\_

\_\_\_\_\_

Sub: Quotations are invited for Domain Server with the specifications below.

S. No.	Description	Qty	Remark	Specification to be filled
1	UTP Cat 6 Cable (Box of 305 Mtrs.)	3	Cabling for Wireless	Annexure 1
2	24 Port Jack Panel Cat 6	3	For Existing Cables and Wireless	Annexure 1
3	UTP Cat 6 I/O	12	For Wireless	Annexure 1
4	UTP Cat 6 Patch Cord, 1 Mtr	72	For Existing and Wireless	Annexure 1
5	32U Floor Mount Rack 800mm x 800mm	1	For Mounting Devices and Server	Annexure 2
6	24 Port Layer 2 Semi Managed Switch with 5 Years Extended Warranty	3	For Existing and Wireless	Annexure 3
7	Firewall/ UTM with Bundled Subscription License for 5 years	1	Firewall for Internet Security	Annexure 4
8	Remote VPN Device	8	For Connectivity of Remote Locations	Annexure 5
9	Wireless Access Point	12	Wireless AP	Annexure 5
10	Wireless Controller for Upto 25 AP's	1	For AP Control	Annexure 5
11	Server for AD (2x Quad Core, 32GB RAM, 6x4TB HDD, Raid 5, Rack Mountable)	1	Server	
12	4 Bay NAS with 16TB Raw HDD	1	File Storage	Annexure 6
13	Microsoft Windows Server License 2019	1	Microsoft License for Server	NA
14	Microsoft User Cal License	36	Microsoft License for AD	NA

Lakshmi Mazumdar Bhawan, 16, Mahatma Gandhi Marg, I.P. Estate, New Delhi - 110002 (India)

लक्ष्मी मजुमदार भवन, 16, महात्मा गांधी मार्ग, आई.पी. एस्टेट, नई दिल्ली - 110002 (भारत)

Phones : +91-11-23378667, 23378702, Email : info@bsgindia.org, Website : www.bsgindia.org

15	Microsoft Windows 10 Professional License	28	Microsoft License for Systems	NA
16	Back Up Software License	36	Auto Backup Software	Annexure 7
17	Server License for DLP with 5 Years	1	Server License for DLP	Annexure 8
18	User License for DLP with 5 Years	36	User License for DLP	Annexure 8
19	1" PVC Conduit	800	Pipe for Wireless Cabling	NA
20	5KVA Online UPS with 30 mins battery back up	1	UPS	
21	One Time Installation	1	Service	NA


We are looking for total IT solution for service at our National Headquarters, Regional Headquarters & other Centers (Kolkata, Bengaluru, Faridabad, Guwahati, Delhi, Noida, Pachmarhi)

We are an NGO Certified with 80G certificate. We request you to provide best prices applicable for NGO.

#### Terms & Conditions

1. For details contact: JIT GHOSH – 9038934049
2. Please mention the lead time for delivery & implementation
3. Please share amount along with GST as applicable.
4. Quotation shall be addressed to Director, The Bharat Scouts and Guides and should reach to [supply@bsgindia.org](mailto:supply@bsgindia.org) by 21.06.2022 05.00PM.
5. Share quotation along with Installation & after sales support cost if any.
6. We reserve the right to consider/reject the quotation without giving any reason.

Yours Sincerely

  
(Darshana Pawaskar)  
Jt. Director (SS)

OEM Criteria		
All passive components should be from same OEM.		
OEM Should be in India from last 25 Years and should be register on NSE and BSE		
Turn Over of OEM should be More than 500 Cr in last 3 Financial Years.		
<b>Unshielded Twisted Pair Category 6 Cable</b>		<b>Compliance (Yes/No)</b>
<b>Features</b>		
<b>Characteristic</b>	<b>Min. Required Specification</b>	
Features	Category 6 Unshielded Twisted Pair 4 pair should be complied as per ETL Channel verification program for compliance with ANSI/TIA-568.2-D standard and ISO 11801 Class E standards at swept frequencies up to 250MHz	
<b>Mechanical Characteristics</b>		
Construction:	4 twisted pairs separated by internal X shaped, full separator.	
Conductor dia	23 AWG	
Insulation	POLYETHYLENE	
Outer sheath	LSZH GREY - Single sheath	
RIP CORD	YES	
Sequential meter marking	YES	
Temperature Rating	"-20" to +70°C	
Filler Required	YES	
Packing	305 Mtrs.	
<b>Low Frequency Electrical Paramere</b>		
CONDUCTOR RESISTANCE (DC)	93.8 OHMS/1000 MTR @20 Degree C. MAX.	
RESISTANCE UNBALANCE	5%MAX	
MUTUAL CAPACITANCE	5.6 nF/100 mtrs Max.	
CAPACITANCE UNBALANCE PAIR/GROUND	330PF/100M MAX	
Propagation Delay Skew	536 nS/100M	
Nominal Velocity of Propagation	69%	
Charcteristics IMPEDANCE	100±15%OHMS	
Worst Case cable skew	45ns/100m	
PoE compliance:	Meets IEEE 802.3af and IEEE 802.3at for PoE applications	
<b>Cat 6 UTP Loaded Patch Panel - 24 port</b>		<b>Compliance (Yes/No)</b>
<b>Characteristic</b>	<b>Min. Required Specification</b>	
Features	Patch Panel made of powder coated steel, in 24 port configurations Allow for a minimum of 200 re-terminations without signal degradation below standards compliance limit. Have port identification numbers on the front of the panel. Should have self adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel IDC: Suitable for 22-24 AWG stranded and solid wire compatible with both 110 & Krone punch down tools Improved cable management with optional cable management bar Category 6 Unshielded Twisted Pair 4 pair should be complied as per ETL Channel verification program for compliance with ANSI/TIA-568.2-D standard	
Mechanical Characteristics	Plastic Housing: PBT+Glass Fiber, UL94V-0 rated	
Jack Connector	Operating Life: Minimum 750 insertion cycles Material: Phosher bronze with nickel plated Contact Plating: 50µ" Gold plated on plug contact area Contact Force: 20N max	
IDC Connector	Plastic Housing: Polycarbonate, UL94V-2 rated or equivalent IDC Contact Plating: Phosphor bronze with tin plated Wire Accommodation: 22-24 AWG solid Voltage Rating: 125V AC RMS Contact resistance: 20Milliohms Insulation resistance: 100 MegaOhms @ 500V DC	
<b>Cat 6 UTP Patch cord</b>		<b>Compliance (Yes/No)</b>
<b>Characteristic</b>	<b>Min. Required Specification</b>	
Features	Category 6 Equipment cords – 1/2/3/5 Mtr The work area equipment cords shall, at a minimum comply with proposed ANSI/TIA/EIA-568-C.2 Commercial Building Cabling Standards Transmission Performance Specifications for 4 pair Category 6 Cabling. Equipped with modular 8-position modular plugs on both ends, wired straight through with standards compliant wiring.	
Mechanical – Cable	Conductor size: 24 -24 AWG stranded bare copper Jacket: Low Smoke	
Mechanical Characteristics – Plug	Operating life: Minimum 750 insertion cycles Contact blade: Copper Alloy Contact plating: 03Mµ" Gold	
Electrical Characteristics – Plug	Dielectric withstanding Voltage: 1000VDC or 700 VAC Insulation resistance: >500 MegaOhms @ 1000V DC/min Operating temperature: -10oC to 60oC	
RJ-45 Plug and Boot Material	Clear Polycarbonate for RJ-45 And Clear PVC for Boot	
RJ-45 standards	ISO/IEC 60603-7-4 and FCC 47 part 68	
factory molded Boot	Yes Category 6 Unshielded Twisted Pair 4 pair should be complied as per ETL Channel verification program for compliance with ANSI/TIA-568.2-D standard	
<b>Information Outlet</b>		<b>Compliance (Yes/No)</b>
Single Port	Write on labels in transparent plastic window – supplied with plate Face Plate with shutter	

	Should be able to support variety of jacks – UTP, STP etc.	
	Category 6 Unshielded Twisted Pair 4 pair should be complied as per ETL Channel verification program for compliance with ANSI/TIA-568.2-D standard	
	All information outlets for 22-24 AWG copper cable shall:	
	Use insulation displacement connectors (IDC)	
	Allow for a minimum of 200 re-terminations without signal degradation below standards compliance limits.	
Insertion force:	20N max	
	Jack Specification:	
Plastic Housing:	Polycarbonate, UL94V-2 rated or equivalent	
Operating Life:	Minimum 750 insertion cycles	
Contact Material:	Phosphor Bronze with nickel plated	
	Contact Plating: 50 microns gold on plug contact area	
IDC:	Housing PC, UL 94 V-2, 568A/B configuration	
	Operating Life: Minimum 200 Re-terminations	
IDC Contact Plating:	Phosphor bronze with tin plated	
Operation Temp	-20 C to 60 C	

Specification	Compliance	Remarks
Depth adjustable mounting slots for verticals provide the better mounting flexibility maximizing the usable mounting space		
Precision engineering capabilities and best efficient software configuration product technology provides the best product quality and fastest delivery in the industry		
Top and bottom Panel with ventilation and cable entry facility		
Provision to mount the cooling fans on the top panel		
Powder coated finish with pretreatment process meeting all industry standards		
Grounding and Bonding Options		
32U Closed Rack / Width 800 / Depth 800		
Front Door : Lockable Toughened Glass Door		
Rear Door : Steel Door		
Equipment Mounting : DIN Standard 10mm Sq. Slots / Direct M6 Tap		
Mounting Angle : 19" Mounting angles made of formed steel		
Top and Bottom Cover : Welded to Frame, Vented and Field Cable entry exit cut outs		
Mounting Option : Castor wheels (Front 2 wheels with Break and rear without break) Or Levelers Or Base plinth		
Accessories: Doors & Side Panels, Power Distribution Units, Cable Manager, 4 * Fans and Fan Modules, Jacking Feet, 5 * Mounting Hardware, Vertical Power strip with 12 nos of 5/15A sockets (high end).		

Desired Specification/Qualitative Requirement	Compliance (Yes/No)
<b>Switch (Layer 2)</b>	
Switch Should Support 24 10/100/1000BASE-T PoE , 4 SFP ports and RJ-45 console port. All Gigabit Ethernet ports support IEC 61000-4-5 surge protection (6KV)	
switch should support Operating Temperature -5 to 50 °C (23 to 122 °F)	
Switch Should Support Min. 56 Gbps Switching Capacity and Maximum 64 Byte Packet Forwarding Rate is 41.7 MPPS, 16K MAC address table.	
The Switch shall have the intelligence to detect the loop occurring from the unmanaged network segment. Dying Gasp for quick trouble shooting during power failures or system shut downs	
Switch Should Support IEEE 802.3af & at compliance (for PoE ports) and 193W Power Budget.	
Switch Should Support IGMP Snooping v1, v2 and MLD snooping v1/v2	
Switch shall support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) & LLDP-MED.	
Switch Should Support IEEE 802.3az Energy Efficient Ethernet (EEE) Power saving Technology, Power Saving by Link Status, Time-based PoE, System hibernation, Port shut off, Cable length detection Etc.	
Switch Should Support 4K VLAN ID's, Min 256 static VLAN , Multicast VLAN and Auto Voice & Video VLAN	
Switch Should Support Port Mirroring One to one/Many to One,	
Switch should support Quality of Service (QoS), 802.1p, Strict, Weighted Round Robin (WRR), Bandwidth Control.	
Switch Should Support IP interfaces, Static routing for inter-VLAN Communication	
Switch should support Access Control List (ACL), Port Base, MAC Base, IP Based, L2 & L3 ACL (IPv4 and IPv6) ITU-T G.8032 ERPS sub-50 ms protection and recovery	
Switch Should Support Security Features like Broadcast/Multicast/Unicast Storm Control, Traffic segmentation, TLS, DoS attack prevention, 802.1X Port-based Access Control , Port Security, ARP Spoofing Prevention, DHCP Server Screening, IP-MAC-Port Binding, ARP Inspection, DHCP Snooping.	
Switch Should Support 802.1X Authentication local/RADIUS database (IPv4 & IPv6), port-based access control, EAP, OTP, TLS, TTLS, PEAP and Support MD5 authentication	
Switch Should Support features Cable diagnostics, IPv4 & IPv6 Inspection, SSH v2 feature, 802.3x Flow Control and HOL Blocking Prevention	
Switch Should Support Management thru Web-based and CLI.	
Switch Should Support SNMP v1/v2c/v3, SNTP, ICMP v6, IPv4/v6 Dual Stack, Dual image, Dual configuration	
Switch should have EMI CERTIFICATE as per EN/FCC/IC/CE.	
Switch should have SAFETY CERTIFICATE as per UL/ IEC/EN 60950	
Switch should be supplied with the all necessary components like Power supply, Power cord, Console Cable, Rack-mount kit, Installation Guide, etc. and necessary software image file to fulfil all above mention feature set from day 1.	

	<ul style="list-style-type: none"> <li>• Firewall should block attacks such as DNS cache poisoning, FTP bounce, improper commands.</li> </ul>		
<b>Security</b>			
<b>Security</b>	<ul style="list-style-type: none"> <li>• Protects HTTP, HTTPS, FTP, POP3, POP3S, IMAP, IMAPS, SMTPS and SMTP.</li> <li>• Pattern-based spyware blocking at the gateway.</li> <li>• Centralized, daily updates, automatic and manual updates or offline update.</li> <li>• Advance Threat Protection should have Instant identification and immediate response to today's most sophisticated attacks. Multi-layered protection identifies threats instantly</li> </ul>		
<b>APPLICATION CONTROL</b>			
<b>APPLICATION CONTROL</b>	<ul style="list-style-type: none"> <li>• Firewall should have feature to identify, allow, block or limit usage of applications beyond ports and protocols.</li> <li>• Firewall should provide protection against Block potentially unwanted Applications</li> <li>• Application signature database of 3000+ Applications for Application Control</li> </ul>		
<b>API Support</b>			
<b>API Support</b>	<ul style="list-style-type: none"> <li>• The solution Should support API for 3rd party integration</li> <li>• The API has option to add, update, or delete configurations.</li> <li>• The API should have option to add or update policies for IPS, Web filter, Application filter</li> <li>• The solution API should have option to Manage physical interfaces and view Port wise Network and Zone details</li> <li>• The Solution API should have option to update Gateway details. routes traffic between networks.</li> <li>• The Solution API should have option to add or delete route.</li> </ul>		
<b>Central Management and Reporting</b>			
<b>Central Management and Reporting</b>	<ul style="list-style-type: none"> <li>• The Central Management Solution should support manage all Firewall policies and configuration from a single console</li> <li>• The Central Management solution should have option to manage backup, schedule Firmware update for any date/time</li> </ul>		
<b>License</b>			
<b>License</b>	<ul style="list-style-type: none"> <li>• Five Year Subscription license for Firewall, Advanced Threat Protection (ATP), Prevention System (IPS), Anti-malware, Zero day threat protection , Web and App visibility, control, and protection, 24x7 support, security and software updates, adv. exchange warranty for the period of licenses. License period will be counted after activation.</li> </ul>		
<b>MAF</b>	<ul style="list-style-type: none"> <li>• Manufacturing authorization certificate valid for this specific enquiry should be enclosed.</li> </ul>		

	OEM criteria	Compliance	Remark
OEM Criteria	<ul style="list-style-type: none"> <li>Proposed solution should have ISO 9001:2015 certification</li> <li>OEM should have 24*7*365 via email, phone and remote assistance with support centre in India</li> <li>Appliance should be Make In India products .Preference shall be given to Class 1 local supplier as defined in public procurement (Preference to Make in India)</li> </ul>		
GENERAL	<ul style="list-style-type: none"> <li>Must have a 64-bit hardware platform &amp; based on Multi-Core Architecture with Optimization for excellent throughput for all your key processes.</li> <li>The Proposed solution should have option for visibility into encrypted traffic flows, support for TLS 1.3 without downgrading the performance.</li> <li>The device should be having security functions like Firewall, VPN (IPsec Site to Site &amp;SSL Client VPN), Gateway level antivirus, Category based web and application filtering, Intrusion prevention system, Traffic shaping, DoS/DDoS.</li> <li>Solution should offer with Central management solution with option to manage multiple firewalls from day one.</li> <li>Multiple WAN link balancing multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules, should support more than two ISP.</li> </ul>		
INTERFACE AND CONNECTIVITY	<ul style="list-style-type: none"> <li>Firewall must be supplied with minimum 8 nos. of 10/100/1000 GbE copper and 1 GbE SFP ports</li> </ul>		
TECHNICAL	<ul style="list-style-type: none"> <li>Support a minimum of 1024 VLANs.</li> <li>Built in storage capacity of integrated Minimum 50 GB for Logs and reports</li> <li>The Proposed solution should have Min 2GB of RAM/Memory or higher to handle network traffic volumes.</li> <li>Should have option for LAN bypass in case hardware fails network should pass without interruption.</li> <li>Firewall should block attacks such as DoS, IP/ ICMP/ TCP-related.</li> <li>Encryption support of AES 128-256 bit, 3DES 56-168 bit.</li> <li>Proposed solution should have authentication agents for client OS platform</li> <li>Supporting on Windows, MAC, Linux, mobile devices platforms. May also support clientless authentication</li> <li>Local, Active Directory, LDAP Server, RADIUS, TACACS+, eDirectory and Kerberos authentication methods.</li> </ul>		
<b>PERFORMANCE</b>			



PERFORMANCE	<ul style="list-style-type: none"> <li>• Firewall must support at least 6,000,000 concurrent connections.</li> <li>• Firewall must support at least 70,000 new sessions per second processing.</li> <li>• Firewall should support up to 4 Gbps of Firewall IMIX throughput.</li> <li>• Firewall should support integrated IPS throughputs of minimum 3 Gbps.</li> <li>• Firewall should have a minimum Firewall throughput of 7 Gbps.</li> <li>• Firewall should have a minimum Threat Protection throughput 800 Mbps.</li> <li>• Firewall should support the standard Layer 3 mode of configuration with Interface IPs. It should be possible to protect the firewall policies from being compromised.</li> <li>• Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type.</li> <li>• Firewall should be able to filter traffic even if the packets are fragmented.</li> <li>• All known internet-based applications should be supported for filtering; like Telnet, FTP, SMTP, HTTP, DNS, ICMP, DHCP, ARP, etc.</li> <li>• Firewall should support SSL inspection over HTTPS</li> <li>• Firewall should support CLI and GUI based access to the firewall modules.</li> <li>• FIREWALL LOGGING, STATISTICS AND REPORTING</li> <li>• Firewall logs must contain information about the firewall policy rule that triggered the log.</li> <li>• Firewall must provide at a minimum basic statistic about the health of the firewall and the amount of traffic traversing the firewall.</li> <li>• Firewall should have support to log (in detail) all connections which are blocked or pass through the firewall.</li> <li>• Firewall should have support to generate performance statistics on real-time basis.</li> <li>• Firewall should have the capability to produce reports which measure usage.</li> <li>• Firewall should have application-based and user-based logs.</li> </ul>		
URL FILTERING	<ul style="list-style-type: none"> <li>• Firewall should support minimum of at least 70+ predefined categories.</li> <li>• Should have flexibility to create network, user, Web and app-based traffic shaping (QoS) policy.</li> <li>• Blacklist and White listing based on IPs and URLs.</li> <li>• Exceptions based on network objects defined.</li> <li>• Notification of custom messages or URL redirection.</li> <li>• INTRUSION PREVENTION</li> <li>• IPS should protect for 5000+ Signatures database.</li> <li>• Firewall should block attacks such as DoS- SYN, IP/ICMP/TCP/UDP related attacks.</li> <li>• Solution should have IPS deep packet inspection engine with an option to select</li> <li>• IPS patterns which can be applied firewall rule for better protection and should have option to create custom signature</li> </ul>		

5

		<b>Compliance (Yes/No)</b>	Remarks
<b>General Features</b>	<ul style="list-style-type: none"><li>• Appliance based hardware device with Plug and play mode</li><li>• Proposed solution should be managed from HO firewall</li><li>• Proposed solution should have minimum throughput of 250 Mbps</li><li>• Proposed solution must have 4 x 10/100/1000 Base-TX (1 GbE Copper) LAN interface</li><li>• Proposed solution must have 1 x 10/100/1000 Base-TX (shared with SFP) WAN interface</li><li>• Proposed solution must have optional bay for wi-fi or dongle connectivity.</li><li>• Proposed solution Must have optional 2nd power supply</li></ul>		
<b>License</b>	<ul style="list-style-type: none"><li>• Five Year perpetual license for device replacement in case device gets faulty.</li></ul>		

IEEE 802.11b/g/n/ac/ax, 11ax 1800, PoE (802.3at) Access Point	Compliance (Yes/No)
The Access Point should be compliant with IEEE 802.3ab, IEEE 802.3u, IEEE 802.3az IEEE 802.11a/b/g/n/ac/ax Wave 2 wireless interface	
The Access Point support WPA/WPA2/WPA3™ Personal/Enterprise, WEP 64/128-bit, SSID broadcast disable, MAC address access control, internal RADIUS server	
The Access point should support MU-MIMO slices through congestion, reducing wait time for all users, Support Wi-Fi 6 delivers greater network efficiency and lower latency, with nearly four times the capacity of previous Wi-Fi standards	
The Access Point should be compliant with IEEE 802.3af and 802.3at for providing PoE based power	
The Access point should support Band Steering makes sure connected devices get the best available frequency band	
<b>Interface and antenna</b>	
Minimum 2 x dual-band internal antennas 3.2 dBi antenna for 2.4 Ghz & internal 4.3 dBi antenna for 5 Ghz	
Support 2.4 - 2.483 GHz, 5.15 - 5.35 GHz, 5.47 - 5.85 GHz	
Access Point should provide Maximum Output Power - 23 dBm in 2.4 GHz band & 26 dBm 5 GHz band:	
Access Point should support Up to 1800 Mbps	
Access point must have 1 x RJ45 console port for Debugging, 1 x 10/100/1000 Ethernet (PoE) LAN, factory reset, power input	
The AP should support Software controller and Hardware controller of same OEM	
The Access Point should have option for inbuilt IOS feature to manage group of Access point without any software	
The Access point should support SNMP v1, v2c, v3	
The Access point should have support for Other Features Fast Roaming Support with 802.11k, 802.11v, and 802.11r and Passpoint Hotspot 2.0 Support	
WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WEP 64/128-bit encryption, SSID broadcast disable, MAC address access control, Network Access Protection (NAP), ARP spoofing prevention, WLAN partition	
The Access point support Local/POP3/RADIUS/PassCode/LDAP authentication for captive portal	
The Access point should have built-in internal RADIUS server allowing users to create their accounts within the device itself	
Telnet, Secure Telnet (SSH), Web (HTTP), Secure Socket Layer (SSL), Traffic control, SNMP v1/v2c/v3	
Temperature • Operating: 0 to 40°C (32 to 104°F) • Storage: -20 to 65°C (-4 to 149°F)	
The AP should be supplied with Wall and ceiling mounting bracket	
The Access Point should have option for inbuilt IOS feature to manage group of Access point without any software	
The Access Point can work multiple operation modes: Access Point, Wireless Distribution System (WDS) with Access Point, WDS/Bridge (No AP Broadcasting), and Wireless Client.	
<b>Wireless Controller</b>	
Make and Model	
Controller should Device Interfaces:- Gigabit LAN, USB 3.0, SD Slot, Factory Reset Button and Console Port	
NAT pass through by using https agent (Can manage multiple APs behind NAT device)	

Provide access points information such as status, IP address, MAC address, channel, network, firmware version, model name...etc.	
Provide wireless client information such as IP address, MAC address, authentication type, channel, associated SSID...etc.	
Controller should view, create and configure logical sites and networks that are related to the physical locations of the wireless devices in the network.	
Bandwidth Optimization, Configure the bandwidth settings for access points in this network, Allocate average bandwidth for each client, Allocate specific bandwidth for this SSID, Allocate the maximum bandwidth for each station, Allocate different bandwidth for 11a/b/g/n stations	
Controller should Upload SSL certificate of network Aps.	
Captive portal: AP supports internal DB, remote radius, POP3, MAC address and passcode authentication, Payment gateway, Captive portal page customization, Hotspot printing and External captive portal	
Controller should be capable of managing up to 100 Access Points (APs) without licensing charges.	
Should support Wireless LAN Management Features like AP grouping, Multi-tenancy, Visualized topology, NAT pass-through, AP discovery (layer 2 and layer 3), and Report system.	
Should have Multiple SSID with VLAN, Captive portal with multiple SSID and VLAN	
Should support features Band steering, Airtime Fairness, Auto RF management, Bandwidth optimization and Client access control	
Should support Rate limiting and bandwidth control for guest and hotspot portal.	
Controller should support Auto Channel, Output Power Control, Self-healing around failed Aps in RF Management and Control.	
Should support Band steering, L2 roaming, Bandwidth optimization and Airtime fairness.	
Controller should have Web-based user interface (HTTPS) for easy management.	
Should support Scheduling in Firmware update and Configuration update.	
Certification: RoHS, Emission (EMI) - CE, FCC, IC and BSMI:- Safety - CE/ LVD, UL	

7

<b>SPECIFICATION FOR NAS (NETWORK ATTACHED STORAGE)</b>	<b>Compliance (Yes/No)</b>
Dimensions should be DxWxH (mm) : 22 x 133 x 204 or above	
Number of Bays should be 4 Bays or more	
Maximum Capacity : Up to 48TB of storage	
Processor : Quad core 1.4GHz High Performance ARM Cortex A15 or better	
Memory : 2GB RAM or more	
Drive Types Supported : SATA/SSD 2.5" or 3.5"	
Faster file backups and access up to 200MBps read and 160MBps write speeds	
HD 1080p streaming and real-time transcoding to any device, anywhere	
Link aggregation for 2x the performance	
Perfect for streaming and data backup for multiple users	
High performance anti-virus with near-0 throughput loss	
Advanced BTRFS file system	
Desktop app for complete file syncing and automatic backup	
Hot Swappable Drives : Yes	
eSATA Port for Additional Storage : 1 Port or more	
LAN Ports : 2 Gigabit Ethernet LAN ports or more	
USB Ports : (3) USB 3.0 ports or more	
Should have 16TB RAW space from Day 1	
Should support Raid from Day 1	

8

SR.NO.	SPECIFICATION	Compliance
1	The proposed backup solution should be available in a single management console on various OS platforms such as Windows, Linux and MAC	
2	The proposed backup solution shall have same GUI across heterogeneous platforms to ensure easy administration.	
3	The proposed backup solution has in-built frequency and calendar based scheduling system.	
4	The proposed backup solution should be certified "hot-online" backup solution for different type of Enterprise databases and applications. It should have a supported integration minimum with latest versions of MSSQL Database, Oracle Database. Application aware backup license should not be separate from base agent license.	
5	The proposed backup solution shall also support granular recovery for VMware, Exchange server, Share point. For Virtual environment VM license should be unlimited including application aware backup.	
6	The proposed backup solution shall also support SAN backup	
7	The proposed backup solution shall also support NAS backup	
8	The proposed backup software should give the option to allow de duplication to be done either on the Application Server or on the Backup Server or at the Target Device.	
9	The backup software should support backup to cloud. Vendor Cloud or any 3rd party cloud like AWS, Azure, Google etc..	
10	The proposed backup solution shall support synthetic full backup / Virtual full backups.	
11	The proposed backup solution shall be able to copy data across firewall.	
12	The proposed backup solution shall support for write protect or restore protect on file level or folder level .etc	
13	The proposed backup solution shall support File and Folder level backup & restore feature	
14	The proposed backup solution shall support file name or folder name or host name wise sort	
15	The proposed backup solution must support at least AES 256-bit encryption capabilities. Encryption should be at both level like intransit and Storage	
16	The proposed backup solution should have blockchain technology for files authentication. If files gets changed by anyone that should be trackable.	
17	The backup software should support missed job execution	
18	The Backup software should be able to recover only critical volumes and later restore other volumes that were backed up in separate sessions.	
19	The backup software should support the Cold replication functionality	
20	The proposed backup solution must support monitoring & reporting methods while backing-up and restoring	
21	The proposed solution must work in backup from Physical image to Virtual image or vise versa	
22	The proposed solution must work with both AD and workgroup systems for client backups	
23	Compressed mechanism for security like 128bit or mentioned if any other	
24	The proposed solution must work with Backup policies pertaining to retention period definition as per organization policies	

25	The proposed solution should have inbuilt Anti Ransomware protection for live system as well as backed up data and map drive for endpoints. Also it should be capable to revert back any ransomware infected file to original stage	
26	The proposed solution should have inbuilt Cryptomining protection for live system.	
27	The proposed solution should not replicate entire storage or backed up data. It should have provision to select specific date for off host backup processing.	

### Product Capabilities

Data Loss Prevention	Compliance (Yes/No)
Proposed Solution should be able to identify Sensitive Data using Sensitive Keyword based markers	
Proposed Solution should be able to identify Sensitive Data using Pattern/Regex based markers	
Proposed Solution should be able to identify Sensitive Data using Unstructured Fingerprinted Data based markers	
Proposed Solution should be able to identify Sensitive Data using file types and file attributes-based markers	
Proposed Solution should be able to block data transfer via devices (USB drives, MTP, Printers, CD/DVD, Bluetooth Connected devices etc)	
Proposed Solution should be able to prevent Data Loss via devices (USB drives, Printers, CD/DVD) using content identification	
Proposed Solution should be able to prevent Data Loss via restricted enforce encryption of USB storage devices	
Proposed Solution should be able to identify and whitelist USB storage devices for internal use	
Proposed Solution should be able to allow USB storage devices to be used in 'Read-Only' Mode	
Proposed Solution should be able to Monitor, Shadow Log and Block all SMTP outbound traffic via email clients (Outlook, Thunderbird, Outlook express, etc.)	
Proposed Solution should be able to Monitor, Shadow Log and Block all Webmail outbound traffic via browsers (Outlook Web, O365, Gsuite)	
Proposed Solution's Monitoring and shadow logging scope should extend to Fields 'From, To, CC, BCC, Subject, Message Body and Attachment'	
Proposed Solution should be able to Block SMTP and Webmail based on Whitelisted or Blacklisted Domains or Email Addresses (Sender domain)	
Proposed Solution should be able to Block SMTP and Webmail based on Whitelisted or Blacklisted File Types	
Proposed Solution should be able to Block SMTP and Webmail based attachments on Whitelisted or Blacklisted File Attributes (Password Protection / Data Classification Meta Tags etc)	
Proposed Solution should be able to Block SMTP and Webmail based on Whitelisted or Blacklisted File Names & extension	
Proposed Solution should be able to Block SMTP and Webmail based on inspection and identification of sensitive content in Subject, Message Body and Attachment	
Proposed Solution should also support for Agent-less Gateway based protocol capable of performing able to Block email based on inspection and identification of sensitive content in Subject, Message Body and Attachment for users accessing corporate emails via personal / alien devices	
Proposed Solution should be able to Monitor, Shadow Log and Block all File Uploads and HTTP POST/PUT content from Browsers.	
Proposed Solution should be able to Block Web File Uploads based on Whitelisted or Blacklisted Domains or Email Addresses (Sender domain)	
Proposed Solution should be able to Block Web File Uploads based on Whitelisted or Blacklisted File Types	
Proposed Solution should be able to Block Web File Uploads based on Whitelisted or Blacklisted File Attributes (Password Protection / Data Classification Meta Tags etc)	
Proposed Solution should be able to Block Web File Uploads based on Whitelisted or Blacklisted File Names	
Proposed Solution should be able to block Web File Uploads based on inspection and identification of sensitive content inside files	
Proposed Solution should be able to generate alert for Web Uploads based on inspection and identification of sensitive content inside HTTP POST/PUT content in browsers	
Proposed Solution should be able to Monitor, Log and Block all Application Network Activity	
Proposed Solution should be able to Monitor, Shadow Log and generate alerts for Application File Access Activity	



Once deployed Proposed Solution should be able to Scan, Inventories, Categorise and List all applications running in the organisation environment (including all running versions) for identification of any rogue applications	
Proposed solution should be able to block all rogue applications from making a network connection by way of an essential application whitelisting method	
Proposed solution should be able to Sandbox applications; to restrict them from only making network connections to specified destination IPs or URLs	
Proposed solution should be able to Bypass specified applications (eg; Core systems etc), to ensure no interception, logging or blocking of outbound traffic	
Proposed solution should be able to Bypass Logs and Shadow Logs; based on email/web domains	
Proposed Solution should be able to Monitor, Log and Block all Browser/URL Activities	
Proposed Solution should support pre-defined and categorised Web/URL list as per industry standards	
Proposed Solution should support Additions, Changes, Removals or Customisation of Web Categorisation Lists	
Proposed System Should Support creation of Custom Web Categorisation Lists	
Proposed Solution Should enable blocking or allowing of Web/URLs/IPs based on Whitelisting or Blacklisting approaches	
Proposed solution should be able to Bypass specified URLs/IPs (eg; Core systems etc), to ensure no interception, logging or blocking of outbound traffic	
Proposed Solution should have the ability to run endpoint Data-at-Rest scans and Data Discovery	
Proposed Solution should have the ability to inspect content using Optical Character Recognition (OCR)	
<b>Insider Threat Management</b>	
Proposed Solution should have the ability to identify User malicious activities across avenues of Data Theft, Productivity Loss, IT Misuse, Financial Loss, Operational Loss, Inappropriate Employee Behaviour and Cyber Security Risks.	
Proposed Solution should have the ability to identify User malicious activities and behavioral anomalies across channels of Application Activity, Application File Access Activity, Browser Activity, User Activity Time Tracking, CD/DVD Activity, Data At Rest Activity, File Upload Activity (Web and FTP), Gmail and OWA activity, Network File Share Activity, Printer Activity, Search Activity, SMTP Activity, Secure Email Gateway Activity, USB activity	
Proposed Solution should have a highly customisable Incident rule creation interface; with the ability to add multiple parameters of triggers behind each incident for minimising false positives	
Proposed Solution should have a highly customisable Incident rule creation interface; that allows for each incident to be tagged to avenues of impact (Data Loss Potential, IT Misuse etc), while being able to assign a High / Medium / Low severity for the Incident.	
Proposed Solution should have Dashboard Notifications for each Incident or Violation	
Proposed Solution should have the ability to automate Email Alerts for each incident real time	
Proposed Solution should have the ability to automate Email Alerts for Daily Summary of Incidents each day	
Proposed Solution should have a Summary Incident Dashboard for easy referral of organisation level User Behaviour Assessment	
Proposed Solution Incident Summary Dashboard should detail counts of each violation and also a comparative analysis of previous period performance vis-à-vis present period performance	
Proposed Solution should have easy navigation from the Incident Summary Dashboard to inspect any incident in details	
Proposed Solution should have inbuilt Scoring Matrix and a reporting mechanism that is automated to run analytics based on number of incidents, avenue and severity of Impact	
Proposed Solution Should be able to calculate and display Organisation Compliance Score based on Policies set for Data Loss Prevention internally to the platform	
Proposed Solution be able to calculate and display Organisation Data Protection Score based on number of Incidents with Data Loss Potential and severity of Impact	

Proposed Solution be able to calculate and display Organisation Productivity Score based on number of Incidents with Productivity Loss and severity of Impact	
Proposed Solution Should Have an Executive Dashboard that summarises overall organisational health scores and areas of concern	
Proposed Solution's Executive Dashboard should provide easy navigation and drill down capabilities to investigate areas of concerns - department, region, zone to user level.	
Proposed Solution should isolate and centralise visibility of risky users and malicious activities to Executive Committee	
Proposed Solution should be able to generate detailed incident forensics report	
<b>User and Entity Behaviour Analytics</b>	
Proposed Solution should do activity tracking of Users and Devices across all activity channels	
Proposed Solution should log all relevant details where applicable in each channel for forensic investigations and audits; including but not limited to Device ID, User ID, Application, URL, Website Category, Files accessed, Files Transferred, File Names, File Sizes, Printer ID, Network Connectivity Details, Email from / to/ cc/ bcc/ subject/ body/ attachment	
Proposed Solution should be capable of Shadow Logging Emails, File Uploads, USB Transfers, Print, Application File Access, Web Uploads etc	
Proposed Solution should be able to handle if different users were to login to same device in tandem or vice versa; trailing user activity across devices and device activity across users and reporting them in accumulation	
Proposed Solution should be capable of Filtering Activity Reports by User / Or by Device	
Proposed Solution should be capable of logging all User/Device activity for Application Activity	
Proposed Solution should be capable of logging all User/Device activity for Application File Access Activity	
Proposed Solution should be capable of logging all User/Device activity for Browser Activity	
Proposed Solution should be capable of logging all User/Device activity for Active Window Time Tracking	
Proposed Solution should be capable of logging all User/Device activity for CD/DVD Activity	
Proposed Solution should be capable of logging all User/Device activity for File Upload Activity	
Proposed Solution should be capable of logging all User/Device activity for FTP File Upload Activity	
Proposed Solution should be capable of logging all User/Device activity for Gmail Web Activity	
Proposed Solution should be capable of logging all User/Device activity for Network File Share Activity	
Proposed Solution should be capable of logging all User/Device activity for Outlook Web Activity	
Proposed Solution should be capable of logging all User/Device activity for Search Engine Activity	
Proposed Solution should be capable of logging all User/Device activity for Email Gateway Activity	
Proposed Solution should be capable of logging all User/Device activity for SMTP Email Activity	
Proposed Solution should be capable of logging all User/Device activity for USB	
Proposed Solution should be capable of logging all User/Device activity for Printer Activity	
Proposed Solution should be capable of logging all User/Device activity for Data-at-Rest Activity	
Proposed Solution should be capable of Entity Level Behaviour Analytics depiction of Browser Activity	
Proposed Solution should be capable of Entity Level Behaviour Analytics depiction of Application Activity	
Proposed Solution should be capable of Entity Level Behaviour Analytics depiction of Gmail / OWA Activity	
Proposed Solution should be capable of Entity Level Behaviour Analytics depiction of File Upload Activity	

Proposed Solution must support all required features to be handled by a SINGLE endpoint agent	
Proposed Solution must perform all monitoring and block activities at the endpoint; continuing to perform those actions irrespective of if User is connected to internal / private / VPN network or offline (Only Blocking)	
Proposed Solution must include a Gateway Component for Email Monitoring or Blocking; originating via alien / personal devices	
All Modules of the Proposed Solution must be hosted on a single server; with one exception allowed for email gateway	
All Modules of the Proposed Solution must be centrally configured and managed on a single platform	
Proposed Solution should support Windows, Mac (BigSur, Catalina, Monterey) and Linux OS (Ubuntu) Desktop endpoints	
Proposed Solution should support Windows or Linux OS Servers	
Proposed solution should be able to take periodic screenshot to monitor detailed employee activity for forensic evidence	
Proposed solution should be able to initiate event-triggered screenshot for sensitive application activity and sensitive window title-based activity forensic evidence	
Proposed solution should be password protected from being uninstalled and should be tamper proof	
Proposed Solution should be able to implement temporary policies for uplifting the user privileges for a defined duration	
Proposed solution should support Sub-Admin Accounts with different privileges and different User Groups	
Proposed Solution should also log and support audit of all Admin and Sub-Admin Activities	
Proposed Solution should support integrations with Windows Active Directory; for scheduled Sync of organization and User information	
Proposed Solution should support integrations with Windows Bitlocker for Key synchronisation	
Proposed Solution should support integrations with Data Classification Tools, agnostic of the vendor	
Proposed Solution should support integrations with DRM and Encryption Tools	
Proposed Solution should support integrations with SIEM Solutions (Qradar)	
Proposed Solution should support coexistence with an existing network level Web Proxy	
Proposed Solution should support extraction of Raw Data Logs or Filtered Reports via CSV/ PDF formats	
Proposed Platform should be capable of generating Alerts on any Policy Changes or Agent Uninstallation / Deletion performed by an Admin or a Sub-Admin	
Proposed Solution should be capable of being deployed in Stealth Mode at the endpoints	
Proposed Solution should be capable of providing options for Customised Pop-up Messages for any blocked activity	
Proposed Solution should offer a globally adjustable Sync Interval for Policy and Log Synchronization	
Proposed Solution should offer User/Device level adjustable Sync Interval for Screenshots and Shadow Logs synchronization to manage locations with lower bandwidth	
Proposed Solution should Support White Listing or Bypassing of Domains, URLs, IPs etc to prevent Data interception or logging for such entities.	
Proposed Solution should support Policy Setting as well as Reporting separately for Devices and Users	
Proposed Solution should support Agent Installation via Manual or Automated (Silent / Verbose) methods	
Proposed Solution should Support AD GPO or other third-party solutions for Remote Agent Push	
Proposed Solution Console should in real time indicate Agent Connectivity Status, last connected time and Agent Version	
Proposed Solution should support future agent update deployment via the Console	
Proposed Solution should also support a CSV based Organization / Group / User Information imports and manual Workgroup User Creation	
Proposed solution must support LDAP based authentication mapping for Admins & Sub-Admin accounts	

Proposed solution musts have 2FA for Administrator login	
Proposed solution must store all information in encrypted form	
Proposed solution should be Make In India	