Annexure - XXII

Technical Compliance sheet

the work of Supply, Installation, Testing and Commissioning for the Upgradation of the Campus Networking & Security Infrastructure of Cochin Por

TENDER NO. FIN/EDP/NW Upgradation/2026 Dated: 16.11.2026

01. FIREWALL

SL. No	Feature	Specification Required	Compliance (Complied /Higher /Lower)
1	**Make**		
2	**Model**		
3	**Type**	The Firewall must be Next Generation Enterprise Firewall with hardware appliance.	
4	**Form Factor**	Minimum 1U rack-mountable appliance with required rack mounting accessories.	
5	**Architecture Type**	The Firewall should have open architecture with multi-core CPU; no proprietary ASICs; single appliance without clustering/additional appliances.	
6	**Architecture**	The Firewall architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting. Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc.,	
7	**Processor & RAM**	Minimum 8-core x86 CPU with 32 GB RAM or more from Day 1.	
8	**Storage**	Minimum 120 GB SSD from Day 1.	
9	**Interfaces**	8×10/100/1000; 4×1G/2.5G/5G PoE; 6×1G SFP; 4×1G/10G SFP/SFP+ with required SFP transceivers populated from Day 1.	
10	**Management/ HA Interfaces**	2× dedicated HA ports; 10/100/1000 Mbps OOB management; RJ45 console; USB Port; Micro USB Console Port with required cables.	
11	**IPv4/IPv6 Support**	The Firewall should have Full IPv4 and IPv6 firewall/security functionality.	
12	**NGFW Throughput**	Minimum 8 Gbps real-world application-control throughput with Application-ID/AVC, AV/Application Control and logging enabled; OEM performance report required.	
13	**Threat Prevention**	Minimum 4 Gbps real-world NG Threat Prevention throughput with Application-ID/AVC, User-ID/Agent-ID, IPS, AV, Anti-Spyware, Anti-Malware, File Blocking, Sandboxing and logging.	
14	**IPsec VPN/ SSL VPN**	Minimum 4 Gbps with 64 KB HTTP transactions and logging enabled.	

15	**Routing/NAT**	The Firewall should support IPv4/IPv6 static and dynamic routing (OSPF/OSPFv3, BGP), Policy-Based Routing (PBR), ECMP, route/path monitoring, VRF/virtual routing or equivalent, Source/Destination/Static/Dynamic NAT, PAT/NAPT, NAT exemption, NAT64/NAT66 or equivalent, port forwarding and comprehensive NAT logging.	
16	**SSL VPN/ Remote access VPN**	The firewall should support minimum of 500 concurrent remote-access VPN users, with SSL/TLS-based VPN connectivity, and the bidder shall provide all required licenses/subscriptions for the specified concurrent users for the entire contract period.	
17	**New Sessions**	≥100,000 Layer-7 sessions/sec or ≥1M Layer-4 connections/sec.	
18	**Concurrent Sessions**	≥900,000 Layer-7 sessions or ≥10M Layer-4 connections/sessions.	
19	**High Availability**	Active/Active, Active/Passive HA Clustering and should support stateful failover for both Firewall and VPN sessions from Day 1.	
20	**Logging**	The Firewall should have provision to store all Traffic, Threat, URL, VPN & System logs for minimum 30 days from Day 1.	
21	**Fans and Power Supply**	The proposed appliance should have dual redundant hot-swappable power supply and fan assemblies that provide ventilation and cooling for the firewall with required dual power supply cables and The Firewall should support Operating Environment 100–240V AC, 50–60 Hz from Day 1	
22	**URL Filtering**	The appliance should facilitate embedded Web Content Filtering feature with required licenses and Should be able to block different categories/sites based on filtering mechanism.	
23	**Security Features**	The Firewall should have Application Security, Intrusion Prevention System/Intrusion Detection System, Anti-Malware, Advanced Threat Protection, URL/Web Security, Advanced Malware Sandbox, DNS Security & SSL/TLS Inspection with valid subscription/licenses valid for 5 Years from Day 1.	
24	**Test Certification**	EAL4+/NDPP/NDcPP or above under Common Criteria/IC3S by STQC DEIT, Govt. of India or equivalent; hardware TEC certified.	
25	**Equipment Certification**	FCC Class A, CE Class A, VCCI Class A, cTUVus, CB.	
26	**Accessories**	Necessary accessories to be provided by the successful bidder for operational of the item.	
27	**Licensing**	The firewall licenses should be provided with 5 years subscription licenses for Hardware & Software OEM Support, Threat Prevention, Advanced URL Filtering, Malware Analysis & Required VPN Licenses	
28	**Support & Warranty**	The Firewall should have 5 Years comprehensive OEM warranty and 24×7×365 OEM Premium support from the date of successful commissioning.	
29	**Delivery Period**		

2. Core Switch				
Sl.No	**Feature Name**	**Feature Type**	**Specification Required**	**Compliance (Complied /Higher /Lower)**
Make				
Model				
Switch Type		**Layer 3 Manageble Switch**		
1	**General Features**	Ports	Gigabit L2/L3 switch with **24×1G/10G SFP+** and **4×40G/100G QSFP28 uplinks**, console/auxiliary ports and accessories.	
		Power & Cooling	Hot-swappable redundant power supplies and fan trays from Day 1.	
		Switching Architecture	Non-blocking per-slot throughput from Day 1.	
		Software Updates	Software upgrades/updates included in warranty.	
		ASIC	Programmable ASICs, purpose-built for integrated hardware/software performance and capacity optimization.	
		Platform Security	Integrated TPM or equivalent for trusted-source boot and platform integrity.	
		Management	Cloud-based and on-premises management support.	
		Operating Temperature	0°C to 40°C.	
		Licensing	All specified features available from Day 1; required licenses included from Day 1.	
2	**Performance**	Memory	**16 GB DRAM, 32 GB Flash**.	
		Switching Capacity	Up to **1.2 Tbps**.	
		Forwarding Rate	**900 Mpps**.	
		IPv4 Routing	**≥24K** entries.	
		IPv6 Routing	**≥12K** entries.	
		Multicast Routes	**≥4K IPv4/IPv6** multicast routes.	
		MAC Addresses	**≥32K**.	
		VLAN	**≥4K VLAN IDs** and **1K simultaneous VLANs**.	
		ACL/QoS	**≥4K entries**.	
		Packet Buffer	**≥32 MB**.	
		IPv6	IPv6-ready from Day 1.	
		Configuration Backup	Automatic backup of previous configuration.	
		High Availability	MLAG/MCLAG/VPC/VSX for 2-node HA with independent control-plane architecture.	
		Routing Protocols	RIPv2, RIPng, EVPN, BGP/BGP4, VRF, VXLAN, OSPFv2/v3 Routed Access, PBR, PIM-SM, PIM-DM, PIM-SSM and VRRP from Day 1.	
		Link Aggregation	IEEE 802.3ad LACP and port trunking.	

3	**Functionality**	Spanning Tree	IEEE 802.1s MST.	
		L2/QoS Features	STP, Trunking, PVLAN, Q-in-Q, DWRR/equivalent scheduling, CIR/equivalent	
		Configuration Rollback	Rollback to previous successful configuration.	
		Management Protocols	SNMPv1/v2/v3, SSL, SSHv2, Telnet, Ping and Traceroute.	
		Security & Provisioning	TPM and ZTP; IP SLA for voice-quality monitoring.	
		Data Center Bridging	DCB with lossless Ethernet, PFC (**2 priorities/port**), ETS and DCBX (pre-standard LLDP DCBX IEEE 1.01).	
		Storage/Network	SCSI, Lossless iSCSI, RoCE v1/v2 and NVMe over Fabrics.	
		Management Platform	Cloud and on-premises management.	
		802.1X	IEEE 802.1X support.	
		Port Authentication	Port-based authentication.	
		MAC Authentication	MAC-based authentication.	
		L3 Filtering	Source/destination IP/subnet and source/destination TCP/UDP port filtering.	
		Source-Port Filtering	Source-port filtering support.	
		Network Security	RADIUS/TACACS+, Dynamic ARP Protection, Port Security, STP Root Guard and BPDU Guard.	
		Automation	Netconf/YANG/REST API, Python or equivalent management automation.	
		Traffic Monitoring	NetFlow/sFlow/JFlow and port mirroring/equivalent.	
4	**Interface Requirement**	Downlink Ports	**24×1G/10G SFP+** ports.	
		Uplink Ports	**4×40G/100G SFP28** uplink ports with required SFP transceivers populated from Day 1.	
		Accessories	Necessary accessories to be provided by the successful bidder for operational of the item.	
5	**Regulatory Compliance**	Safety	UL 60950 / IEC 60950 / CSA 60950 / EN 60950 or equivalent Indian **IS-13252:2010 or better**.	
		EMC	EN 55022/55032 Class A/B, CISPR22 Class A/B, CE Class A/B, FCC Class A/B or equivalent Indian **IS 6873 Part 7:2012 or better**.	
6	**OEM, Warranty & Support**	Warranty & Updates	Minimum **5-year hardware warranty** with NBD shipment and direct OEM software updates/upgrades.	
		Security Certification	Switch or OS on different hardware platform tested for **EAL2/NDPP or above** under Common Criteria.	
		OEM Qualification	OEM in **Gartner Leaders Quadrant for Wired & Wireless LAN Infrastructure for ≥5 consecutive years**.	
7	**Delivery Period**			

3. DISTRIBUTION SWITCH			
Sl. No	**Feature Type**	**Specification Required**	**Compliance (Complied /Higher /Lower)**
	Make		
	Model		
	Switch Type	**Layer 3 Manageble Switch**	
1	**Architecture**	The should have 24x ports 1G/10G SFP+ fiber ports and 4x 1/10/25G SFP ports. The switch should support two field-replaceable and hot- swappable power supply loaded from day one. the switch should have 1x USB-C Console Port , 1x OOBM and 1x USB Type A Host port. Switch should be upgradable to 40G or 50G for future expansion without a complete any complete forklift upgrade.	
		4GB SDRAM and 16 MB flash and 8 MB Packet buffer size. The switch should support front plane stacking on uplink port or Back plane stacking and should have Stacking Performance of minimum 200 Gbps. The switch should have 880 Gbps of Switching Capacity and 650 Mpps Throughput Capacity	
		The switch should have minimum 60,000 Ipv4 Unicast Routes ,60K Ipv6 Unicast Routes ,8K Ipv4 & IPv6 Multicast routes ,Ipv4/Ipv6 ACL Entries 20K. The Switch should support 32000 MAC address	
2	**IPv6 feature**	IPv6 host enables switches to be managed in an IPv6 network, Dual stack (IPv4 and IPv6), MLD snooping forwards IPv6 multicast traffic, IPv6 ACL/QoS supports ACL and QoS, RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping, IPv6 routing supports Static and OSPFv3 protocols from day-1	
3	**High Availability And Resiliency**	The Switch should support Bidirectional Forward Detection (BFD), (VRRP), (UDLD) to monitor link connectivity, IEEE 802.3ad LACP supports up to 256 LAGs. IEEE 802.1d, IEEE802.1W & IEEE 802.1S.	
		The switch should support MLAG/MCLAG/VPC/VSX feature for 2 node high availability with independent control plane architecture	
4	**Management**	The Switch should support Zero-Touch Provisioning (ZTP) simplifies installation of switching infrastructure using DHCP-based. The Switch should support On-premises and cloud- based management	
		The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading, support Multiple configuration files which can be stored to a flash image	

		The Switch should support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitterfor VoIP tests. The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	
5	**Multicast**	The Switch should support IGMP Snooping, supports MLD v1 and v2, IGMPv1, v2, and v3, MSDP, PIM-SM, PIM-DM, LLDP-MED	
6	**Layer 2 Switching**	The Switch should support VLAN and tagging for IEEE 802.1Q (4094 VLAN IDs) & 1K Active VLAN, IEEE 802.1v, MVRP, VXLAN encapsulation (tunnelling) ,VxLAN-EVPN	
7	**Layer 3 Routing**	The Switch should support Border Gateway Protocol (BGP) provides IPv4 and IPv6 routing, (MP-BGP) ,EVPN, VXLAN , (ECMP), OSPFv2, OSPFv3, PBR, IPv4 & IPv6 Static routing, Dual IP Stack From day 1	
		The Switch should support Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones	
8	**Security**	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	
		The Switch should support Access control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header	
		The Switch should support Remote Authentication Dial-In User Service (RADIUS) & (TACACS+)	
		The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload	
		from DOS attacks. The Switch should support Switch CPU protection to provide automatic protection against malicious network traffic trying to shut down the switch	
		The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications	
		The Switch should support Dynamic IP lockdown with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing.	
		The Switch should support Dynamic ARP protection to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data	
		The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator. The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network EN 60950-1, EC 60950-1,EN61000,EN 60825, RoHS (EN 50581:2012) and WEEE regulations	

		Switch or Switch's Operating System on different hardware plateform should be tested for EAL 2/NDPP or above under Common Criteria Certification.	
		The OEM shall be in Leaders Quadrant of Gartner report for Wired & Wireless LAN Infrastructure for minimum 5 Consecutive Years.	
		Security Certification: Switch or OS on different hardware platform tested for **EAL2/NDPP or above** under Common Criteria.	
9	**OEM, Warranty & Support**	Warranty & Updates: Minimum **5-year hardware warranty** with NBD shipment and direct OEM software updates/upgrades.	
10		10G SFP+ LC LR 10km SMF C-class Transceiver – 24 Nos	
11	**Delivery Period**		

4. Access Switch Type – 1 (24 Port)			
Sl. No	**Feature Type**	**Specification Required**	**Compliance (Complied /Higher /Lower)**
	Make		
	Model		
	Switch Type	**Layer 3 Manageble Switch**	
1	**Architecture**	Shall be 19" Rack Mountable	
		The switch should have dedicated Console Port	
		4GB SDRAM and 16 MB flash and 12 MB Packet buffer size	
		The Switch should support 8000 MAC address	
		The switch should have minimum 512 Ipv4 Unicast Routesand 512 Ipv6 Unicast Routes ,512 Igmp Groups ,512 Mld Groups ,256 Ipv4 and 128 ingress ACL Entries.	
		The Switch should have 24x ports 10/100/1000 BASE-T ports and 4x 1/10 SFP+ ports	
		The switch should have 128 Gbps of Switching Capacity and 95 Mpps Throughput Capacity	
2	**IPv6 feature**	IPv6 host enables switches to be managed in an IPv6 network	
		Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols	
		MLD snooping forwards IPv6 multicast traffic to the appropriate interface	
		IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic	
		IPv6 Static routing	
		RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
3	**High Availability And Resiliency**	The switch should support standard stacking technology forming a single logical switch using multiple physical switches managed by a single management IP address and a single switch config file for the entire stack .	
		The Switch should support Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni- directional traffic is detected, preventing loops in STP- based networks	
		The Switch should support IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm	
		The Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are required and legacy support for IEEE 802.1d and IEEE 802.1w	

		The switch should support Strict priority (SP) queuing, Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ, Ratelimiting ,per-queue minimums	
		Large buffers for graceful congestion management	
4	**Management**	The Switch should support Built-in programmable and easy to use REST API interface	
		The Switch should support On-premises and cloud- based management	
		The Switch should support Zero-Touch Provisioning (ZTP) simplifies installation of switching infrastructure using DHCP-based	
		The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	
		The Switch should support Industry-standard CLI with a hierarchical structure	
		The Switch should support Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access	
		The Switch should support SNMP v2c/v3 provides SNMP read and trap support of industry standard Management	
		Information Base (MIB), and private extensions sFlow (RFC 3176)	
		The Switch should support Remote monitoring (RMON) with standard SNMP to monitor essential network functions.	
		Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, XRMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms and events	
		The Switch should support TFTP and SFTP support offers different mechanisms for configuration updates;	
		The Switch should support Debug and sampler utility support ping and traceroute for IPv4 and IPv6	
		The Switch should support Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients	
		The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management	
		information from adjacent devices on a network, facilitating easy mapping by network management applications	
		The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading	
		The Switch should support Assignment of descriptive names to ports for easy identification	
		The Switch should support Multiple configuration files which can be stored to a flash image	

		The Switch should support Ingress and egress port monitoring enable more efficient network problem solving	
		The Switch should support Unidirectional link detection (UDLD) monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices	
5	**Multicast**	The Switch should support IGMP Snooping to allow multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN	
		The Switch should support Multicast Listener Discovery (MLD) enables discovery of IPv6 multicast listeners; supports	
		MLD v1 and v2	
		The Switch should support Internet Group Management Protocol (IGMP) and Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3	
6	**Layer 2 Switching**	The Switch should support 4094 VLAN IDs	
		The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of	
		up to 9198 bytes	
		The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.	
		The Switch should support MVRP to allow automatic learning and dynamic assignment of VLANs	
		The Switch should support Bridge Protocol Data Unit (BPDU) tunnelling to Transmits STP BPDUs transparently	
		The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups	
		The Switch should support STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	
		The Switch should support Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network	
7	**Layer 3 Routing**	The Switch should support Static IP routing.	
		The Switch should support Static IPv4 and IPv6 routing to provide simple manually configured IPv4 and IPv6 routes	
		The Switch should support Dual IP stack to maintain separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design	

8	**Convergence**	The Switch should support IP multicast snooping (data-driven IGMP) to prevent flooding of IP multicast traffic	
		The Switch should support LLDP-MED (Media Endpoint Discovery) to define a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones	
		The Switch should support Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and	
		LLDP-MED to automatically configure a VLAN for IP phones	
		The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	
		The Switch should supportAccess control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can	
		either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header	
		The Switch should supportACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis	
		The switch should support Enrollment over Secure Transport (EST)and Remote Authentication Dial-In User Service (RADIUS)	
		The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security	
		The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS	
		attacks	
		The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	
		The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X,	
		to authenticate clients that do not support IEEE 802.1X	
		The Switch should support MAC-based client authentication	
		The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications	

9	**Security**	The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3	
		The Switch should support Switch CPU protection to provide automatic protection against malicious network traffic	
		trying to shut down the switch	
		The Switch should support ICMP throttling defeats, ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic	
		The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access	
		security policy and VLAN assignment specific to each authenticated network user	
		The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks	
		The Switch should support Dynamic IP lockdown with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing	
		The Switch should support Dynamic ARP protection to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data	
		The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes	
		The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator	
		The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to	
		the network	
		The Switch should support Source-port filtering to allow only specified ports to communicate with each other	
		The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks	
		The Switch should support Secure Sockets Layer (SSL) to encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch	
		The Switch should support Secure FTP to allow secure file transfer to and from the switch and protect against unwanted file downloads or unauthorized copying of a switch configuration file	
		The Switch should support Critical Authentication Role to ensure that important infrastructure devices such as IP phones are allowed network access even in the absence of a RADIUS server	

		The Switch should support MAC Pinning to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected	
		The Switch should support Management Interface Wizard to help secure management interfaces such as SNMP, telnet/SSH,SSL, Web.	
		The Switch should support Security banner displays a customized security policy when users log in to the switch	
10	**Certification**	The Switch should support Green initiative for RoHS (EN 50581:2012) and WEEE regulations	
		EN 60950-1/IEC 60950-1	
		EN 60825	
		CAN/CSA C22.2 No. 60950, 2nd Edition UL 60950-1, 2nd Edition	
11	**OEM, Warranty & Support**	Warranty & Updates: Minimum **5-year hardware warranty** with NBD shipment and direct OEM software updates/upgrades.	
12		10G SFP+ LC LR 10km SMF C-class Transceiver – 8Nos	
13	**Delivery Period**		

5. Access Switch Type – 2 (12 Port)			
Sl. No	**Feature Type**	**Specification Required**	**Compliance (Complied /Higher /Lower)**
	Make		
	Model		
	Switch Type	Layer 3 Manageble Switch	
1	**Architecture**	Shall be 19" Rack Mountable	
		The switch should have dedicated Console Port	
		4GB SDRAM and 16 MB flash and 12 MB Packet buffer size	
		The Switch should support 8000 MAC address	
		The switch should have minimum 512 Ipv4 Unicast Routesand 512 Ipv6 Unicast Routes ,512 Igmp Groups ,512 Mld Groups ,256 Ipv4 and 128 ingress ACL Entries.	
		The Switch should have 12x ports 10/100/1000 BASE-T ports and 2x 1/10 SFP+ ports	
		The switch should have 128 Gbps of Switching Capacity and 95 Mpps Throughput Capacity	
2	**IPv6 feature**	IPv6 host enables switches to be managed in an IPv6 network	
		Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols	
		MLD snooping forwards IPv6 multicast traffic to the appropriate interface	
		IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic	
		IPv6 Static routing	
		RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
3	**High Availability And Resiliency**	The switch should support standard stacking technology forming a single logical switch using multiple physical switches managed by a single management IP address and a single switch config file for the entire stack .	
		The Switch should support Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni- directional traffic is detected, preventing loops in STP- based networks	
		The Switch should support IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG and provide support for static or dynamic groups and a user-selectable hashing algorithm	
		The Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are required and legacy support for IEEE 802.1d and IEEE 802.1w	

		The switch should support Strict priority (SP) queuing, Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ, Ratelimiting ,per-queue minimums	
		Large buffers for graceful congestion management	
4	**Management**	The Switch should support Built-in programmable and easy to use REST API interface	
		The Switch should support On-premises and cloud- based management	
		The Switch should support Zero-Touch Provisioning (ZTP) simplifies installation of switching infrastructure using DHCP-based	
		The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	
		The Switch should support Industry-standard CLI with a hierarchical structure	
		The Switch should support Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access	
		The Switch should support SNMP v2c/v3 provides SNMP read and trap support of industry standard Management	
		Information Base (MIB), and private extensions sFlow (RFC 3176)	
		The Switch should support Remote monitoring (RMON) with standard SNMP to monitor essential network functions.	
		Supports events, alarms, history, and statistics groups as well as a private alarm extension group; RMON, XRMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms and events	
		The Switch should support TFTP and SFTP support offers different mechanisms for configuration updates;	
		The Switch should support Debug and sampler utility support ping and traceroute for IPv4 and IPv6	
		The Switch should support Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients	
		The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management	
		information from adjacent devices on a network, facilitating easy mapping by network management applications	
		The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading	
		The Switch should support Assignment of descriptive names to ports for easy identification	

		The Switch should support Multiple configuration files which can be stored to a flash image	
		The Switch should support Ingress and egress port monitoring enable more efficient network problem solving	
		The Switch should support Unidirectional link detection (UDLD) monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices	
5	**Multicast**	The Switch should support IGMP Snooping to allow multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN	
		The Switch should support Multicast Listener Discovery (MLD) enables discovery of IPv6 multicast listeners; supports	
		MLD v1 and v2	
		The Switch should support Internet Group Management Protocol (IGMP) and Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3	
6	**Layer 2 Switching**	The Switch should support 4094 VLAN IDs	
		The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of	
		up to 9198 bytes	
		The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.	
		The Switch should support MVRP to allow automatic learning and dynamic assignment of VLANs	
		The Switch should support Bridge Protocol Data Unit (BPDU) tunnelling to Transmits STP BPDUs transparently	
		The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups	
		The Switch should support STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	
		The Switch should support Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network	
7	**Layer 3 Routing**	The Switch should support Static IP routing.	
		The Switch should support Static IPv4 and IPv6 routing to provide simple manually configured IPv4 and IPv6 routes	

		The Switch should support Dual IP stack to maintain separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design	
8	**Convergence**	The Switch should support IP multicast snooping (data-driven IGMP) to prevent flooding of IP multicast traffic	
		The Switch should support LLDP-MED (Media Endpoint Discovery) to define a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones	
		The Switch should support Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and	
		LLDP-MED to automatically configure a VLAN for IP phones	
		The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensure the boot process started from a trusted combination of switches.	
		The Switch should support Access control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can	
		either deny or permit traffic to be forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header	
		The Switch should supportACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis	
		The switch should support Enrollment over Secure Transport (EST)and Remote Authentication Dial-In User Service (RADIUS)	
		The Switch should support Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request to provide additional security	
		The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS	
		attacks	
		The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards	
		The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X,	
		to authenticate clients that do not support IEEE 802.1X	
		The Switch should support MAC-based client authentication	

9	**Security**	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications	
		The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3	
		The Switch should support Switch CPU protection to provide automatic protection against malicious network traffic	
		trying to shut down the switch	
		The Switch should support ICMP throttling defeats, ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic	
		The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access	
		security policy and VLAN assignment specific to each authenticated network user	
		The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks	
		The Switch should support Dynamic IP lockdown with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing	
		The Switch should support Dynamic ARP protection to blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data	
		The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes	
		The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator	
		The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to	
		the network	
		The Switch should support Source-port filtering to allow only specified ports to communicate with each other	
		The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks	
		The Switch should support Secure Sockets Layer (SSL) to encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch	
		The Switch should support Secure FTP to allow secure file transfer to and from the switch and protect against unwanted file downloads or unauthorized copying of a switch configuration file	

		The Switch should support Critical Authentication Role to ensure that important infrastructure devices such as IP phones are allowed network access even in the absence of a RADIUS server	
		The Switch should support MAC Pinning to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected	
		The Switch should support Management Interface Wizard to help secure management interfaces such as SNMP, telnet/SSH,SSL, Web.	
		The Switch should support Security banner displays a customized security policy when users log in to the switch	
10	**Certification**	The Switch should support Greeninitiative for RoHS (EN 50581:2012) and WEEE regulations	
		EN 60950-1/IEC 60950-1	
		EN 60825	
		CAN/CSA C22.2 No. 60950, 2nd Edition UL 60950-1, 2nd Edition	
11	**OEM, Warranty & Support**	Warranty & Updates: Minimum **5-year hardware warranty** with NBD shipment and direct OEM software updates/upgrades.	
12		10G SFP+ LC LR 10km SMF C-class Transceiver – 18 Nos	
13	**Delivery Period**		

6. Network Monitoring Software

SL. No	Network Management System - Technical Specifications	Compliance (Complied /Higher /Lower)
Make		
Model		
	General	
1	For effective operations and management of IT Operations, there is a need for an industry-standard Infrastructure Monitoring System. Given the expanse and scope of the project, NMS becomes very critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup of are: Network Monitoring	
2	The OEM of the proposed solution should be a company with 15 years of presense in India and the solution should be deployed in min. 5 projects in Government/PSU segment in India with minimum 500 nodes monitored in each of the deployment in last 5 years. The documentary proof should be submitted at time of the bid submission.	
3	The proposed NMS solution must comply with the following standards: ISO 27034-1 for application security, ISO 27001:2022 for information security management, ISO 15408 for OT Security and IEC 62443-4-1:2018, GDPR and POPIA for data privacy, and SOC 2 Type 2 for service organization controls. This ensures robust security, regulatory compliance, and comprehensive data protection across all managed network operations. Valid supporting Cdertficate documents must be submitted with the bid.	
4	OEM Should provide support for all upgrades and updates during the contract Period.The OEM should have a support centre with Dedicated Support mail id and toll free number in INDIA. OEM Should provide escalation matrix along with bid submission.	
5	Network/Infra Monitoring	
6	The proposed solution must be a natively unified observability platform, architected from the ground up to seamlessly integrate full-stack monitoring, netroute tracing, and telemetry correlation within a single cohesive system without requiring any third-party plugins, tool-switching, or modular bolt-ons.	
7	The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: Event and Alarm management, Auto-discovery of the Network environment, Correlation, and root cause analysis, Reporting and analytics	
8	The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN connectivity with granular visibility up to individual ports level.	
9	The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events. The proposed solution should be ITILv4 gold certified with minimum 14 practices. Valid certificate must be provided at the time of bid submission.	

10	The proposed monitoring solution shall be licensed solely on the basis of the number of monitored devices/nodes, entitling unlimited monitoring parameters, interfaces, log data, and flow data (ingestion, processing, and storage) per licensed device, with no separate licensing, capping, tiering, throttling, or cost escalation based on any parameter other than device count. Bidders must submit an authorized OEM declaration confirming the same, failing which they shall be treated as non-compliant and disqualified at the technical evaluation stage.	
11	The proposed solution should provide a configurable observability data pipeline supporting controlled telemetry ingestion, parsing, field-level enrichment, categorization, schema normalization, transformation, derived attributes, policy evaluation, metric generation, anomaly detection, selective indexing/retention, downstream forwarding and automated action within a continuous processing framework. The solution should enable telemetry to be transformed and operationalized before storage or downstream forwarding so that organizations can control data volume, quality, operational relevance and destination using policy rather than relying exclusively on post-ingestion analytics.	
12	All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring	
13	The solution must offer interactive end-to-end network path mapping with hop-by-hop performance analysis, threshold-based alerting, and historical trend insights. It should correlate node-level metrics with service impact, enrich paths with metadata (e.g., ISP info, geo/IP), and support policy enforcement with contextual visualizations.	
14	The solution must support custom dashboards for different role users such as Management, admin, and report users	
15	The proposed solution should allow the application of advanced statistical transformations and functions over selected KPIs, including but not limited to: Anomaly Detection Forecasting Moving Average Median Function Logarithmic Scale Transformation Delta/Derivative Functionality	
16	The solution should provide superior view of infrastructure health across system,networks, application and other IT Infrastructure components into a consolidated, central console	
17	The proposed solution must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.	
18	The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the- box implementation automating the work required to use OEM validated designs and best practices.	
19	The proposed solution must provide Health Monitoring reports of the network with settable periodicity -@24 Hrs, 1 week, 1 month.	

20	The proposed solution must provide the graphical layout of the network element with modules drawn using different colors to indicate their status	
21	The proposed solution should have multiple alerting feature to get the notification via email, sms and third-party systems	
22	The proposed solution should provide alert console with alert summary such as no. of correlated alert, network alert, server alert, virtualization alert, cloud alert, application alert etc.	
23	The system must have provision to overlay alert on reported metric to understand alert triggering behaviour across multiple drill down pages	
24	Widgets should allow advanced visualization customizations, such as: Toggling legends, adding rotation and adding threshold markers Conditional formatting (icon/color based on thresholds) Column visibility toggles and value formatting Metric/unit conversion and display customization Text Widget to bifurcate sections	
25	The proposed solution should offer a wide variety of intuitive widget visualizations to represent telemetry data effectively, including: Line Chart, Area Chart, Stacked Bar, Horizontal Bar, Vertical Bar, Pie, Donut, Top-N, Grid/Table, Sparkline, Treemap, Sankey, Bubble, Heatmap, Geo-Map, and Gauge	
26	The proposed NMS solution must provide agentless as well as agent-based monitoring for server infrastructure. The agents should be able to set polling interval as low as 10 second with low overhead on target server infrastructure.	
27	The platform should include a dynamic runbook automation engine, allowing users to create, modify, and execute automation runbooks from the UI across a variety of incident response and administrative tasks.	
28	The solution should support macros that automatically provide the possible root cause, potential impact, and recommended resolution steps whenever an alert is triggered, along with the probable reasons behind the alert occurrence.	
29	The solution should support custom plugin development using Python, allowing tailored data collection logic and protocol support extensions.	
30	The proposed solution should be able to take back up of running and startup configuration of network devices. It should also provide versioning for backup to track changes.	
31	Remediation actions for compliance failures must be executable directly from compliance results, streamlining compliance enforcement processes.	
32	The solution must allow compliance results to be exported in universally accepted formats including CSV and PDF for external reporting and audit verification.	
33	The proposed solution should have a built-in capability to forward collected logs to specified external destinations for streamlined data handling and integration.	
34	The proposed solution should enable easy parsing of multi-line logs by specifying regex expressions directly through an intuitive user interface.	

35	The proposed solution should facilitate keyword-based searches across both raw and indexed log data, ensuring comprehensive log data retrieval.	
36	The proposed solution should offer diverse visualization widgets including bubble charts, tree maps, geo-maps, etc., to facilitate rapid and insightful data visualization.	
37	The proposed solution should leverage AI–augmented analytics to automatically generate a concise, context-aware summary upon drill-down of any time-series metric, delivering key distribution statistics, percentile markers, trend and volatility insights, anomaly/outlier detection, and basic auto/cross-correlation patterns in an intuitive narrative or widgetized format—without requiring manual query building or domain expertise	
38	The proposed solution should automatically generate a AI–driven KPI description that includes probable root causes, recommended corrective actions, and correlated metrics, enabling rapid contextual analysis and accelerated troubleshooting without dependency on manual investigation.	
39	The proposed solution should automatically detect log severity levels to facilitate immediate out-of-the-box (OOTB) analytics.	
40	The solution must include advanced traffic visualization widgets such as Sankey diagrams, Bubble charts, Geo-maps, and Tree maps, providing intuitive, multi-dimensional views of network traffic for enhanced analytical interpretation and reporting.	
41	The proposed solution must natively support Next-Generation Network-Based Application Recognition (NBAR2), enabling precise identification and categorization of application traffic for detailed monitoring and analysis.	
42	The solution must include capabilities for Border Gateway Protocol (BGP) enabled flow collection, enhancing accuracy in network traffic routing analytics and peering management.	
43	**Delivery Period**	

7. Server for NMS

SL. No	Features	Full specification / proposed selection	Compliance (Complied /Higher /Lower)
	Make		
	Model		
1	**Server Form Factor**	1U Rack Mount Server	
2	**Processor architecture**	Latest Gen Intel Xeon 6	
3	**Processor sockets**	Minimum 1	
4	**Proposed processor**	Latest Intel Xeon 6731P	
5	**Processor cores**	Minimum 32 cores	
6	**Processor base frequency**	Minimum 2.5 GHz	
7	**Processor TDP**	245 W	
8	**Processor cache**	Minimum 144 MB L3 Cache	
9	**Memory type**	DDR5 SmartMemory RDIMM	
10	**Memory slots**	Minimum 16 DIMM slots, 8 memory channels	
11	**Proposed memory**	128 GB DDR5 RDIMM	
12	**Maximum memory capacity**	Scalable up to 4 TB, subject to DIMM and CPU configuration	
13	**Maximum memory speed**	Up to 6400 MT/s or higher, Subject to processor and DIMM configuration dependent	
14	**Proposed SSD storage**	2 × 480 GB Enterprise SSD	
15	**Proposed HDD storage**	2 × 2.4 TB Enterprise SAS 12G HDD	
16	**Drive configuration**	SFF chassis suitable for compatible 2.5-inch drives; exact drive cage/backplane to be validated	
17	**Storage controller**	Intel VROC configuration	
18	**RAID**	Raid Type1 configuration	
19	**Network connectivity**	Minimum 2 × 10 GbE Ethernet Ports	
20	**Expansion slots**	Up to 2 PCIe 5.0 x16 FHHL slots on the applicable SFF configuration	
21	**OCP networking**	OCP 3.0 PCIe 5.0 x16 slot; optional second OCP slot	
22	**Remote management**	Dedicated Remote management tool	
23	**Security**	TPM 2.0 with Secure Boot, Hardware root and secure firmware update	
24	**Operating system**	Support for Ubuntu Linux, Windows Server and other enterprise operating systems	
25	**Virtualization**	Support for VMware ESXi, Microsoft Hyper-V and KVM	
26	**Cooling**	Seven system fans with redundant hot-pluggable cooling fans	
27	**Power supply**	Hot-pluggable redundant power supply units, minimum 1+1 configuration options: 1000 W, 1500 W or 2400 W	

28	**Redundant power**	Dual redundant power supplies	
29	**USB ports**	Front USB 3.2 Gen 1 and Management service port; Rear USB ports	
30	**Video**	Rear VGA; optional front Display Port	
31	**Rack mounting**	Railing kit and cable management arm	
32	**Warranty**	5 Year Comprehesive Support and Warranty	
33	**Delivery Period**		

8. Endpoint Protection			
SL. No	**Technical Specification**	**Proposed Specification**	**Compliance (Complied /Higher /Lower)**
	Make		
	Model		
1	**Product category**	Endpoint Protection & Security	
2	**Deployment model**	Centralized Endpoint Security (On-premises)	
3	**Endpoint coverage**	Physical endpoints, Windows PCs, supported Windows servers, MAC Computers, POS and ATM endpoints; subject to product compatibility	
4	**Antivirus protection**	Real-time malware detection and prevention	
5	**Malware protection**	Protection against realtime viruses, trojans, spyware, malware and other malicious software	
6	**Ransomware protection**	Behavioral detection and ransomware protection capabilities	
7	**Machine learning**	Pre-execution and runtime machine-learning detection	
8	**Behavioral analysis**	Detection of suspicious scripts, process injection, ransomware and memory-based attacks	
9	**Fileless malware protection**	In-memory analysis for detecting fileless threats	
10	**Zero-day threat protection**	Exploit prevention and protection techniques for emerging threats	
11	**Web protection**	Web reputation and malicious URL blocking	
12	**Command-and-control protection**	Detection and blocking of supported command-and-control communications	
13	**Exploit protection**	Protection against supported software exploitation techniques	
14	**Host firewall**	Availability depends on supported platform and licensed configuration	
15	**Application control**	Capabilities depend on supported platform and licensing	
16	**Device control**	Control of supported endpoint devices and removable media	
17	**Data loss prevention**	Availability depends on the applicable edition and licensing	
18	**Ransomware rollback**	Availability depends on product configuration and supported platform	
19	**Sandbox integration**	Integration with supported sandbox and breach-detection solutions	
20	**Extended detection and response**	Integration with other XDR capabilities, subject to licensing	
21	**Centralized administration**	Centralized management through the on-premises management console	
22	**Policy management**	Centralized configuration and enforcement of endpoint security policies	
23	**Security updates**	Security intelligence and protection updates, subject to entitlement and network configuration	

24	**Event monitoring**	Security-event visibility and reporting through supported management and integration components	
25	**Supported operating systems**	Supported Windows and macOS versions, depending on product release and feature	
26	**Licensing basis**	Subscription based - Centralized Enterprise license	
27	**Subscription**	5 Years with 24/7 OEM Support	
28	**Licence**	500 Users End Point License	
29	**Warranty**	5 Year Comprehesive Support and Warranty	
30	**Delivery Period**		

9. Windows Server (For AD Server & AV Server)

Sl. No	Section	General Specification	Compliance (Complied /Higher /Lower)
	Make		
	Model		
1	**Server Form Factor**	1U Rack Mount Server	
2	**Processor architecture**	Latest Gen Intel Xeon 6	
3	**Processor sockets**	Minimum 1	
4	**Proposed processor**	Latest Intel Xeon 6724P	
5	**Processor cores**	Minimum 16 cores	
6	**Processor base frequency**	Minimum 2.5 GHz	
7	**Processor TDP**	150 W	
8	**Processor cache**	Minimum 72 MB L3 Cache	
9	**Memory type**	DDR5 SmartMemory RDIMM	
10	**Memory slots**	Minimum 16 DIMM slots, 8 memory channels	
11	**Proposed memory**	64 GB DDR5 RDIMM	
12	**Maximum memory capacity**	Scalable up to 4 TB, subject to DIMM and CPU configuration	
13	**Maximum memory speed**	Up to 6400 MT/s or higher, Subject to processor and DIMM configuration dependent	
14	**Proposed SSD storage**	2 × 480 GB Enterprise SSD	
15	**Drive configuration**	SFF chassis suitable for compatible 2.5-inch drives; exact drive cage/backplane to be validated	
16	**Storage controller**	Intel RAID configuration	
17	**RAID**	Raid Type1 configuration	
18	**Network connectivity**	Minimum 2 × 10 GbE Ethernet Ports	
19	**Expansion slots**	Up to 2 PCIe 5.0 x16 FHHL slots on the applicable SFF configuration	
20	**OCP networking**	1 × Rear OCP 3.0 PCIe 5.0 x16 slot (standard/embedded) + 1 × optional Rear OCP 3.0 PCIe 5.0 x16 slot	
21	**Remote management**	Dedicated Remote management tool	
22	**Security**	TPM 2.0 with Secure Boot, Hardware root and secure firmware update	
23	**Operating system**	Support for Ubuntu Linux, Windows Server and other enterprise operating systems	
24	**Virtualization**	Support for VMware ESXi, Microsoft Hyper-V and KVM	
25	**Cooling**	Seven system fans with redundant hot-pluggable cooling fans	
26	**Power supply**	Hot-pluggable redundant power supply units, minimum 1+1 configuration options: 1000 W, 1500 W or 2400 W	
27	**Redundant power**	Dual redundant power supplies	

28	**USB ports**	1 × Front USB 3.2 Gen1, 2 × Rear USB 3.2 Gen1 and 2 × Internal USB 3.2 Gen1 ports; optional 1 × Front USB 2.0 port	
29	**Video**	1 × Rear VGA port (standard); optional 1 × Front DisplayPort through Universal Media Bay	
30	**Rack mounting**	Railing kit and cable management arm	
31	**Warranty**	Comprehensive 5 Year Warranty	
32	**Delivery Period**		

10. Network Racks

Sl.No	Section	General Specification	Compliance (Complied /Higher /Lower)
	Make		
	Model		
1	**Product Type**	Wall-Mount Network Rack	
2	**Rack Height**	15U, 12U,9U	
3	**Construction**	Heavy-duty CRCA steel construction with powder-coated finish	
4	**Front Door**	Lockable toughened glass or perforated metal front door	
5	**Rear Door**	Lockable steel/perforated rear door with easy access	
6	**Side Panels**	Removable and lockable side panels	
7	**Mounting Rails**	Adjustable 19-inch mounting rails with U-markings	
8	**Load Capacity**	Suitable for supporting standard networking and IT equipment	
9	**Cable Management**	Vertical and horizontal cable management provision	
10	**Ventilation & Cooling**	Natural ventilation with provision for fan mounting	
11	**Cooling**	Fan tray with AC cooling fans (where applicable)	
12	**Power Distribution Unit (PDU)**	PDU with adequate power sockets and surge protection (if applicable)	
13	**Earthing**	Integrated grounding/earthing provision for rack and doors	
14	**Accessories to be Included**	Fully Loaded 1 U LIU (1U - 6/12 Port) & Termination of approx 224 Total OFC cores Fully Loaded CAT6 Patch Panel (24 Port) & Termination of approx 350 Total LAN cables. LC/LC OFC Patch Cord (Approx 150 Nos) Cage nuts, mounting screws, washers, cable organizers, grounding kit, blanking panels (where applicable) and all necessary accessories.	
15	**Finish**	Scratch-resistant powder-coated finish	
16	**Standards Compliance**	IEC 60297 or equivalent	
17	**Cable Entry**	Top and bottom cable entry provisions with suitable cut-outs	
18	**Warranty**	5 Years	
19	**Delivery Period**		

11. SFP Modules

Sl. No	Parameter	General Specification	Compliance (Complied /Higher /Lower)
	Make		
	Model		
1	**Product Description**	10G SFP+ LC LR 10km SMF C-Class Transceiver	
2	**Form Factor**	SFP+	
3	**Data Rate**	10 Gbps	
4	**Connector Type**	Duplex LC	
5	**Fiber Type**	Single-Mode Fiber (SMF)	
6	**Maximum Transmission Distance**	10 km	
7	**Optical Standard**	10GBASE-LR	
8	**Wavelength**	1310 nm	
9	**Compliance**	IEEE 802.3ae 10GBASE-LR, SFP+ MSA	
10	**Digital Diagnostics**	Digital Optical Monitoring (DOM/DDM) Support	
11	**Operating Temperature**	Commercial Temperature Range	
12	**Compatibility**	Should be same brand of switches, compatible with supported Networking switches equipped with SFP+ ports	
13	**Hot-Pluggable**	Yes	
14	**Warranty**	5 Year OEW Warranty	
16	**Delivery Period**		