KANNUR UNIVERSITY

THAVAKKARA, CIVIL STATION P.O.,
KANNUR, KERALA- 670002
Tel : 0497 2715321, 0497 2715468
email: registrar@kannuruniv.ac.in, sopmub@kannuruniv.ac.in

PMU-B/BII/6314/2025 13.08.2025

NOTICE INVITING E-TENDER

TENDER DOCUMENT FOR SUPPLY, INSTALLATION/UPGRADATION, TESTING AND COMMISSIONING OF CENTRALISED DATA CENTRE AT THAVAKKARA CAMPUS, KANNUR UNIVERSITY

The Registrar, Kannur University Thavakkara Campus, Kannur - 670 002 invites e-tender(s) in Two bid System (two cover) for the Supply, Installation/ Upgradation, Testing and Commissioning of Centralised Data Centre at Thavakkara campus, Kannur University (under PM USHA Scheme) from competitive firms who have experience in establishing such Data Centres.

Name of the work	Supply, Installation/Upgradation, Testing and Commissioning of Centralised Data Centre At Thavakkara Campus, Kannur University.
Tender Notice No.	PMU-B/BII/6314/2025
Tender ID	2025_KnrU_786316
Last date and time for receipt of Tender	08.09.2025, 06.00 PM
Date and time of opening of Tender	10.09.2025, 11.00 AM
EMD	Rs: 3,90,000/-
Security Deposit	5 percentage of the contract value
Tender Fee	Rs. 25000 + 4500 (GST-18%) (Firm should remit GST amount of ₹4,500/ directly to the GST department and upload receipt in the e Procurement portal)
Period of completion	90 Days From the date of Receipt of Purchase Order

The Registrar, Kannur University reserves the right to accept or reject the tenders without assigning any reason thereof. The list of equipment/ accessories proposed to be purchased, including its quantity and specifications are furnished in the Annexure 1. Since this is an e-tender, only those bidders who have enrolled in the **http://etenders.kerala.gov.in** portal with their own Digital Signature Certificate (DSC) can participate in the tender. E-Tender document and other details can be obtained from the above e-tender portal. Tender documents shall not be available for sales elsewhere.

Instruction to Bidders

At any time prior to the deadline for submission of bids, Registrar, Kannur University, Kerala may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Tenderer, modify the Tender document by amendment and will be published as corrigendum in the website. The deadline for submission of bids may also be extended at the discretion of Kannur University, Kerala.

Tendering Process

The tender will be published in the form of e-tender and will be available on the e-tender site of Govt. of Kerala. All the rules and regulations of the e-tendering will be applicable to this tender also. The tender will be invited in the two cover format. i.e. (i) Technical Bid and (ii) Financial Bid. The financial bid of a bidder will be considered if and only if the bidder qualifies in the technical bid evaluation.

Technical Specifications

Network Firewall (Quantity: 2)

Category	Specification	Details
General Requirements	OEM Experience	OEM must have at least 20 years of experience in the security market.
	Scope of Security Gateway	Must support all security gateway requirements, including throughput, connection rate, and next-generation security applications for small offices to data centers in a single hardware appliance.
	Virtualized Security Gateway	Must offer a virtualized solution supporting all next-generation firewall security applications (intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus) managed from a central platform.
Features and Applications	Unified Platform Applications	Must support (exclusively supplied and managed by OEM): Stateful Inspection Firewall, Intrusion Prevention System (IPS), Application Control and URL Filtering, Anti-Bot and Antivirus, IPSec VPN, Logging and Status, Event Correlation and Reporting.
	Stateful Inspection	Use granular analysis of communication and application state to track and control network flow.
	Architecture	Based on x64 architecture, not proprietary or ASIC-based.

	Performance	- Minimum 1.5 Gbps Threat Prevention throughput (with Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, Zero-Day protection, logging enabled). - Minimum 3.5 Gbps NGFW Throughput (with Firewall, IPS, Application Control, logging enabled). - Minimum 4.5 Gbps IPS throughput. - Minimum 17 Gbps Firewall throughput (1518B UDP). - Minimum 65,000 connections per second. - Minimum 4 million concurrent sessions, expandable to 8 million with additional RAM.
	Hardware Specifications	- Minimum 1 CPU with 2 physical cores. - Minimum 16 GB RAM. - Minimum 200 GB SSD storage. - Support minimum 20 Virtual Systems. - Event logging retention for minimum 180 days (with/without management appliance). - Redundant AC power supplies.
	Security and Authentication	- Encrypted/authenticated communication between management servers and appliance using PKI Certificates. - Support SecureID, TACACS, RADIUS, digital certificates for user authentication.
	Operational Modes	- Support DHCP server and DHCP relay. - Ability to work in Transparent/Bridge mode. - Support Firewall, IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, Threat Emulation, Threat Extraction from day 1. - Support Active/Active and Active/Passive HA configuration.
IPv6 Support	Configuration	Support dual-stack gateway on a bond interface or sub-interface.
	Traffic Handling	Handle IPv6 traffic on IPS, Application Control, Firewall, Identity Awareness, URL Filtering, Antivirus, Anti-Bot modules.
	NAT/Tunnels	Support 6-to-4 NAT or 6-to-4 tunnels.
	Logging	Log and display IPv6 traffic and routing table.
Intrusion Prevention System (IPS)	Detection Mechanisms	Exploit signatures, protocol anomalies, application controls, behavior-based detection.
	Integration	Integrated with firewall on one platform.
	Profiles	Options for client/server-based protection profiles, minimum two pre-defined profiles/policies.
	Fail-Open	Software-based fail-open mechanism based on CPU/memory usage thresholds.
	Signature Management	Automated activation/management of new signatures from updates.
	Exceptions	Support network exceptions based on source, destination, service, or combination.
	Reporting	Centralized event correlation and reporting.

	Protection Activation	Automatic activation based on performance impact, threat severity, confidence level, client/server protections.
	Protection Details	Include protection type, threat severity, performance impact, confidence level, industry reference for each protection.
	Packet Capture	Collect packet captures for specific protections.
	Attack Protection	Detect and block network/application layer attacks for email services, DNS, FTP.
	P2P/Evasive Apps	Detect and block P2P and evasive applications.
	Exclusions	Define network/host exclusions from IPS inspection.
	DNS Protection	Protect against DNS Cache Poisoning, block malicious domains.
	Remote Controls	Detect and block remote control applications tunneling over HTTP.
	SNORT Signatures	Convert SNORT signatures.
	Geo-Based Blocking	Block inbound/outbound traffic based on countries without manually managing IP ranges.
Application Control and URL Filtering	Application Database	Minimum 6,000 known applications.
	URL Categorization	Exceed 200 million URLs.
	Filtering Rules	Support filtering rules with multiple categories.
	HTTPS Inspection	Inspect HTTPS-based URL filtering without SSL decryption.
	Single Site Filtering	Create filtering for single sites supported by multiple categories.
	Granularity	Granular security rules for users and groups.
	Interface	Searchable interface for applications and URLs.
	Risk Categorization	Categorize applications/URLs by Risk Factor.
	Unified Rules	Unified application control and URL security rules.
	Bandwidth Limiting	Limit application usage based on bandwidth consumption.
	Black/White Lists	Black and White lists for URLs.
	Categorization Override	Override mechanism for URL database categorization.
Anti-Bot and Anti-Virus	Integration	Integrated Anti-Bot and Anti-Virus applications on the appliance.
	Detection	Detect and stop suspicious network behavior.

	Detection Engine	Multi-tiered detection using IP, URL, DNS reputation, bot communication patterns.
	Bot Scanning	Scan for bot actions.
	Phishing Protection	Protect against spear phishing attacks.
	Management	Centralized management for Anti-Bot and Anti-Virus policies.
	Reporting	Centralized event correlation and reporting.
	Malicious Websites	Prevent access to malicious websites.
	SSL Inspection	Inspect SSL-encrypted traffic.
	File Protection	Stop incoming malicious files, scan archive files and links in emails, scan files over CIFS protocol.
	Policy Management	Granular policy configuration and enforcement.
Security Management	System Separation	Separate management and firewall systems (management can be virtual or bare metal).
	Centralized Management	Centralized dedicated management system for NGFW appliances.
	Management Features	Includes centralized management, logging, reporting, basic event correlation.
	Dashboard	Real-time dashboard for CPU, memory utilization, state table, concurrent connections, connections per second, security rule hit counter.
	Threat Prevention	Autonomous threat prevention security policy.
	Rule Segmentation	Segment rule base for delegation of duties without affecting other segments.
	Statistics	Basic statistics on firewall health and traffic.
	Rule Structure	Segment rule base in sub-policy and layered structures for autonomous systems and dynamic networks.
	Multi-Domain	Support multi-domain management and global security policy across domains.

WAN Switch (Quantity: 2)

Category	**Specification**	**Details**
Architecture	Form Factor	19" rack-mountable, 24x 10/100/1000 BASE-T PoE+ ports, 4x 10G SFP+ ports, 370W PoE power.
	Ports	1x USB-C Console Port, 1x OOBM, 1x USB Type A Host port.
	Memory	8 GB SDRAM, 16 MB flash, 8 MB packet buffer size.
	Stacking	Support stacking on uplink port or dedicated stack module, minimum 8 switches in stack.
	MAC Addresses	Support 16,000 MAC addresses.

	Routing/ACL	Minimum 2K IPv4 Unicast Routes, 1K IPv6 Unicast Routes, 1K IGMP Groups, 1K MLD Groups, 5K IPv4 ingress ACL Entries, 2K IPv4 egress ACL Entries.
	Performance	128 Gbps switching capacity, 95 Mpps throughput.
	High Availability	Always-on PoE.
IPv6 Features	Management	IPv6 host management in IPv6 network.
	Dual Stack	Support IPv4 and IPv6 connectivity.
	MLD Snooping	Forward IPv6 multicast traffic to appropriate interface.
	ACL/QoS	Support ACL and QoS for IPv6 traffic.
	Routing	Support Static and OSPFv3 protocols.
	Security	RA guard, DHCPv6 protection, dynamic IPv6 lockdown, ND snooping.
High Availability and Resiliency	UDLD	Uni-directional Link Detection to prevent loops in STP-based networks.
	LACP	IEEE 802.3ad LACP, up to 32 LAGs, 8 links per LAG, static/dynamic groups, user-selectable hashing.
	Spanning Tree	IEEE 802.1s Multiple Spanning Tree, legacy support for IEEE 802.1d, 802.1w.
Management	API/ZTP	Built-in programmable REST API, Zero Touch Provisioning (ZTP).
	Management Options	On-premises and cloud-based management, 3rd-party NMS support.
	Monitoring	Scalable ASIC-based wire-speed network monitoring and accounting.
	Security	Restrict access to critical commands, multiple privilege levels, password protection, local/remote syslog.
	SNMP	SNMP v2c/v3, sFlow (RFC 3176).
	RMON	Support events, alarms, history, statistics, private alarm extensions.
	Configuration	TFTP and SFTP for configuration updates.
	Utilities	Debug and sampler utilities (ping, traceroute for IPv4/IPv6).
	NTP	Network Time Protocol for time synchronization.
	LLDP	IEEE 802.1AB LLDP for network mapping.
	Flash Images	Dual flash images for backup, multiple configuration files.
	Port Monitoring	Ingress/egress port monitoring.
	UDLD	Monitor link connectivity, block ports on unidirectional traffic.
	IP SLA	Support IP SLA for Voice with UDP Jitter and VoIP tests.
Multicast	IGMP Snooping	Allow multiple VLANs to receive same IPv4 multicast traffic.
	MLD	Discovery of IPv6 multicast listeners (MLD v1, v2).
	IGMP/ASM	Manage IPv4 multicast networks (IGMPv1, v2, v3).

Layer 2 Switching	VLANs	4094 VLAN IDs.
	Jumbo Packets	Support frame size up to 9198 bytes.
	Protocol VLANs	IEEE 802.1v to isolate non-IPv4 protocols.
	RPVST+	Rapid Per-VLAN Spanning Tree for improved bandwidth usage.
	MVRP	Automatic VLAN learning and assignment.
	VXLAN	Support VXLAN encapsulation for scalable virtual networks.
	BPDU Tunneling	Transparent STP BPDUs.
	Port Mirroring	Minimum 4 mirroring groups.
	STP	IEEE 802.1D STP, 802.1w RSTP, 802.1s MSTP.
	IGMP	Control multicast packet flooding.
Layer 3 Routing	OSPF	Faster convergence, OSPFv2 (IPv4), OSPFv3 (IPv6).
	Static Routing	Manually configured IPv4/IPv6 routes.
	IP Optimization	Directed broadcasts, TCP parameters, ICMP error packets.
	Dual Stack	Separate IPv4/IPv6 stacks for transition.
Security	TPM	Integrated Trusted Platform Module for platform integrity.
	ACL	Support IPv4/IPv6 filtering based on Layer 2/3 headers.
	ACL Filtering	Filter by IP field, source/destination IP address/subnet, TCP/UDP port number (per-VLAN/port).
	Authentication	EST, RADIUS, TACACS+.
	Control Plane	Control Plane Policing for DOS protection.
	Authentication Methods	IEEE 802.1X, Web, MAC, up to 32 sessions per port.
	Secure Access	SSHv2, SSL, SNMPv3.
	Protection	CPU protection, ICMP throttling, identity-driven ACL, STP BPDU protection, Dynamic IP lockdown, Dynamic ARP protection, STP root guard, port security, MAC address lockout, source-port filtering, Secure Shell, SSL, Secure FTP, Critical Authentication Role, MAC Pinning.
	Management Security	Management Interface Wizard, security banner.
	Compliance	RoHS (EN 50581:2012), WEEE regulations.
Certification	Standards	EN 60950-1:2006, EN 62368-1, UL 60950-1, CAN/CSA-C22.2 No. 60950-1-07, IEC 60950-1:2005, IEC 62368-1:2014, CNS-14336-1.
Warranty and Support	Warranty	Limited Lifetime warranty from OEM with NBD shipment and software updates.

Core Switch (Quantity: 2)

Category	Specification	Details
General Features	Form Factor	Gigabit Layer 2 and Layer 3 switch with console, OOBM, USB ports, all accessories.
	Redundancy	Hot-swappable redundant power supply and fan tray from day 1.
	Throughput	Non-blocking throughput from day 1.
	Software	Software upgrades/updates included in warranty.
	ASICs	Programmable ASICs for optimized performance.
	TPM	Integrated TPM for platform integrity.
	Environment	Operating temperature: 0°C to 40°C, 15% to 95% relative humidity.
	Licenses	All features available from day 1 with required licenses.
Performance	Memory	16 GB DRAM, 32 GB flash memory.
	Switching Capacity	Up to 1.28 Tbps.
	Forwarding Rates	900 Mpps.
	Routing	24K+ IPv4 unicast routes, 12K+ IPv6 unicast routes, 4K+ IPv4/IPv6 multicast routes.
	MAC Addresses	140K+ MAC addresses.
	VLANs	Minimum 1K VLANs simultaneously.
	ACL/QoS	4K+ ACL/QoS entries.
	Packet Buffer	32 MB or more.
	IPv6	IPv6 ready from day 1.
	Backup	Automatic backup of previous configuration.
Functionality	Architecture	Distributed and redundant architecture, synchronized upgrades/failover, live operation upgrades.
	Stacking	Long-distance stacking across racks and floors.
	Protocols	RIPv2, RIPng, EVPN, BGP, BGP4, MP-BGP, VRF, VXLAN, EVPN, OSPFv2/v3, PBR, PIM-SM, DCBX, PFC, ETS, PIM-DM, PIM-SSM, VRRP from day 1.
	LACP	IEEE 802.3ad LACP, port trunking.
	Spanning Tree	IEEE 802.1s Multiple Spanning Tree.
	Features	STP, Trunking, Q-in-Q, DWRR or equivalent, CIR/Equivalent, eight egress queues per port.
	Rollback	Support rollback to previous successful configuration.
	Management	SNMPv1/v2/v3, SSL, SSHv2, Telnet, ping, traceroute, ZTP, IP SLA for Voice (UDP Jitter, VoIP tests).
	NMS	Manageable from cloud and on-premises NMS.
	Filtering	IP Layer 3 filtering (source/destination IP address/subnet, TCP/UDP port number), source-port filtering.

	Security	IEEE 802.1X, RADIUS/TACACS+, Dynamic ARP protection, Port Security, STP root guard, BPDU guard.
	Automation	Management automation via REST-API, Python or equivalent.
	Monitoring	Sflow, port mirroring or equivalent.
Interface Requirement	Ports	24x 1G/10G SFP+ ports, 4x 40GbE/100GbE (QSFP+/QSFP28), populated as per design.
Regulatory Compliance	Safety	UL 60950, IEC 60950, CSA 60950, EN 60950, IS-13252:2010 or better.
	EMC	EN 55022/55032 Class A/B, CISPR22 Class A/B, CE Class A/B, FCC Class A/B, IS 6873 (Part 7):2012 or better.
Warranty and Support	Warranty	Minimum 5 years hardware warranty with NBD shipment, software updates/upgrades from OEM.
	Certification	Switch/OS tested for EAL 2/NDPP or above under Common Criteria Certification.

Distribution Switch (Quantity: 4)

Category	**Specification**	**Details**
Architecture	Ports	24x 10-Gigabit SFP+ slots with transceivers, 4x 1/10/25 SFP28 slots with DACs, dual hot-swap PSUs (2).
	Form Factor	19" rack-mountable, mounting kit included.
	Processor/Memory	Quad-core CPU, 8 GB DRAM, 32 GB eMMC/flash, 8 MB packet buffer, 32,000 MAC address entries.
	ASICs	Programmable ASICs for optimized performance.
	Performance	800 Gbps switching capacity, 600 Mpps forwarding rate.
	Stacking	Frontplane or backplane stacking, minimum 200 Gbps stacking performance, minimum 8 switches in stack.
	Routing/ACL	64K IPv4 Unicast Routes, 32K IPv6 Unicast Routes, 8K IPv4/IPv6 Multicast Routes, 8K IGMP Groups, 4K MLD Groups, 4K/1.25K/5K IPv4/IPv6/MAC ACL ingress entries, 2K/0.5K/2K IPv4/IPv6/MAC ACL egress entries.
IPv6 Features	Management	IPv6 host management, dual stack (IPv4/IPv6).
	MLD Snooping	Forward IPv6 multicast traffic.
	ACL/QoS	Support ACL and QoS for IPv6 traffic.
	Routing	Static and OSPFv3 protocols.
	Security	RA guard, DHCPv6 protection, dynamic IPv6 lockdown, ND snooping.
High Availability and Resiliency	BFD	Bidirectional Forward Detection for sub-second failure detection.
	VRRP	Support for highly available routed environments in IPv4/IPv6.
	UDLD	Uni-directional Link Detection to prevent STP loops.

	LACP	IEEE 802.3ad LACP, up to 256 LAGs, 8 links per LAG, static/dynamic groups, user-selectable hashing.
	Spanning Tree	IEEE 802.1s Multiple Spanning Tree, legacy support for 802.1d, 802.1w.
	Port Trunking	Static/dynamic trunks, up to 8 links per trunk.
Management	API/ZTP	Built-in REST API, Zero Touch Provisioning (ZTP).
	Management Options	On-premises, cloud-based, 3rd-party NMS support.
	Monitoring	Scalable ASIC-based wire-speed monitoring, sFlow (RFC 3176).
	Security	Restrict access to critical commands, multiple privilege levels, password protection, syslog.
	SNMP	SNMP v2c/v3, industry-standard MIB, private extensions.
	RMON	Support events, alarms, history, statistics, private alarm extensions.
	Configuration	TFTP, SFTP for configuration updates.
	Utilities	Ping, traceroute for IPv4/IPv6.
	NTP	Network Time Protocol for time synchronization.
	Flash Images	Dual flash images, multiple configuration files.
	Port Monitoring	Ingress/egress port monitoring.
	IP SLA	Support IP SLA for Voice (UDP Jitter, VoIP tests).
Multicast	IGMP Snooping	Reduce IPv4 multicast traffic.
	MLD	Discovery of IPv6 multicast listeners (MLD v1, v2).
	PIM	PIM Sparse Mode (SM), Dense Mode (DM) for IPv4/IPv6.
	IGMP/ASM	Manage IPv4 multicast (IGMPv1, v2, v3).
	MSDP	Route multicast traffic through core networks.
Layer 2 Switching	VLANs	4094 VLAN IDs.
	Jumbo Packets	Support frame size up to 9198 bytes.
	Protocol VLANs	IEEE 802.1v for non-IPv4 protocols.
	RPVST+	Rapid Per-VLAN Spanning Tree.
	MVRP	Automatic VLAN learning and assignment.
	VXLAN	Support VXLAN encapsulation.
	BPDU Tunneling	Transparent STP BPDUs.
	Port Mirroring	Minimum 4 mirroring groups.
	STP	IEEE 802.1D STP, 802.1w RSTP, 802.1s MSTP.
	IGMP	Control multicast packet flooding.
Layer 3 Routing	BGP	IPv4/IPv6 routing, Multi-protocol BGP for IPv6 routes.
	ECMP	Multiple equal-cost links for redundancy and bandwidth scaling.
	OSPF	OSPFv2 (IPv4), OSPFv3 (IPv6) for faster convergence.
	Static Routing	Manually configured IPv4/IPv6 routes.
	PBR	Policy-based routing with classifier.

	IP Optimization	Directed broadcasts, TCP parameters, ICMP error packets.
	Dual Stack	Separate IPv4/IPv6 stacks for transition.
Security	TPM	Integrated TPM for platform integrity.
	ACL	IPv4/IPv6 filtering based on Layer 2/3 headers.
	ACL Filtering	Filter by IP field, source/destination IP address/subnet, TCP/UDP port number (per-VLAN/port).
	Authentication	RADIUS, TACACS+.
	Control Plane	Control Plane Policing for DOS protection.
	Authentication Methods	IEEE 802.1X, Web, MAC, up to 32 sessions per port.
	DHCP Protection	Block unauthorized DHCP servers.
	Secure Access	SSHv2, SSL, SNMPv3.
	Protection	CPU protection, ICMP throttling, identity-driven ACL, STP BPDU protection, Dynamic IP lockdown, Dynamic ARP protection, STP root guard, port security, MAC address lockout, source-port filtering, Secure Shell, SSL, Secure FTP, Critical Authentication Role, MAC Pinning.
	Management Security	Management Interface Wizard, security banner.
	Compliance	RoHS (EN 50581:2012), WEEE regulations.
Certification	Standards	EN 60950-1, IEC 60950-1, EN61000, EN 60825.
Warranty and Support	Warranty	Limited Lifetime warranty from OEM.

ToR Switch (Quantity: 2)

Category	**Specification**	**Details**
Architecture	Ports	24x 1/10-Gigabit BaseT slots with transceivers, 4x 1/25/50G SFP+ ports with DACs, dual hot-swap PSUs (2).
	Form Factor	19" rack-mountable, mounting kit included.
	Processor/Memory	Quad-core CPU, 8 GB DRAM, 32 GB eMMC/flash, 8 MB packet buffer, 32,000 MAC address entries.
	ASICs	Programmable ASICs for optimized performance.
	Performance	800 Gbps switching capacity, 550 Mpps forwarding rate.
	Stacking	Frontplane or backplane stacking, minimum 200 Gbps stacking performance, minimum 8 switches in stack.
	Routing/ACL	64K IPv4 Unicast Routes, 32K IPv6 Unicast Routes, 8K IPv4/IPv6 Multicast Routes, 8K IGMP Groups, 4K MLD Groups, 4K/1.25K/5K IPv4/IPv6/MAC ACL ingress entries, 2K/0.5K/2K IPv4/IPv6/MAC ACL egress entries.
IPv6 Features	Management	IPv6 host management, dual stack (IPv4/IPv6).
	MLD Snooping	Forward IPv6 multicast traffic.
	ACL/QoS	Support ACL and QoS for IPv6 traffic.
	Routing	Static and OSPFv3 protocols.

	Security	RA guard, DHCPv6 protection, dynamic IPv6 lockdown, ND snooping.
High Availability and Resiliency	BFD	Bidirectional Forward Detection for sub-second failure detection.
	VRRP	Support for highly available routed environments in IPv4/IPv6.
	UDLD	Uni-directional Link Detection to prevent STP loops.
	LACP	IEEE 802.3ad LACP, up to 256 LAGs, 8 links per LAG, static/dynamic groups, user-selectable hashing.
	Spanning Tree	IEEE 802.1s Multiple Spanning Tree, legacy support for 802.1d, 802.1w.
	Port Trunking	Static/dynamic trunks, up to 8 links per trunk.
Management	API/ZTP	Built-in REST API, Zero Touch Provisioning (ZTP).
	Management Options	On-premises, cloud-based, 3rd-party NMS support.
	Monitoring	Scalable ASIC-based wire-speed monitoring, sFlow (RFC 3176).
	Security	Restrict access to critical commands, multiple privilege levels, password protection, syslog.
	SNMP	SNMP v2c/v3, industry-standard MIB, private extensions.
	RMON	Support events, alarms, history, statistics, private alarm extensions.
	Configuration	TFTP, SFTP for configuration updates.
	Utilities	Ping, traceroute for IPv4/IPv6.
	NTP	Network Time Protocol for time synchronization.
	Flash Images	Dual flash images, multiple configuration files.
	Port Monitoring	Ingress/egress port monitoring.
	IP SLA	Support IP SLA for Voice (UDP Jitter, VoIP tests).
Multicast	IGMP Snooping	Reduce IPv4 multicast traffic.
	MLD	Discovery of IPv6 multicast listeners (MLD v1, v2).
	PIM	PIM Sparse Mode (SM), Dense Mode (DM) for IPv4/IPv6.
	IGMP/ASM	Manage IPv4 multicast (IGMPv1, v2, v3).
	MSDP	Route multicast traffic through core networks.
Layer 2 Switching	VLANs	4094 VLAN IDs.
	Jumbo Packets	Support frame size up to 9198 bytes.
	Protocol VLANs	IEEE 802.1v for non-IPv4 protocols.
	RPVST+	Rapid Per-VLAN Spanning Tree.
	MVRP	Automatic VLAN learning and assignment.
	VXLAN	Support VXLAN encapsulation.
	BPDU Tunneling	Transparent Upper STP BPDUs.
	Port Mirroring	Minimum 4 mirroring groups.
	STP	IEEE 802.1D STP, 802.1w RSTP, 802.1s MSTP.

	IGMP	Control multicast packet flooding.
Layer 3 Routing	BGP	IPv4/IPv6 routing, Multi-protocol BGP for IPv6 routes.
	ECMP	Multiple equal-cost links for redundancy and bandwidth scaling.
	OSPF	OSPFv2 (IPv4), OSPFv3 (IPv6) for faster convergence.
	Static Routing	Manually configured IPv4/IPv6 routes.
	PBR	Policy-based routing with classifier.
	IP Optimization	Directed broadcasts, TCP parameters, ICMP error packets.
	Dual Stack	Separate IPv4/IPv6 stacks for transition.
Security	TPM	Integrated TPM for platform integrity.
	ACL	IPv4/IPv6 filtering based on Layer 2/3 headers.
	ACL Filtering	Filter by IP field, source/destination IP address/subnet, TCP/UDP port number (per-VLAN/port).
	Authentication	RADIUS, TACACS+.
	Control Plane	Control Plane Policing for DOS protection.
	Authentication Methods	IEEE 802.1X, Web, MAC, up to 32 sessions per port.
	DHCP Protection	Block unauthorized DHCP servers.
	Secure Access	SSHv2, SSL, SNMPv3.
	Protection	CPU protection, ICMP throttling, identity-driven ACL, STP BPDU protection, Dynamic IP lockdown, Dynamic ARP protection, STP root guard, port security, MAC address lockout, source-port filtering, Secure Shell, SSL, Secure FTP, Critical Authentication Role, MAC Pinning.
	Management Security	Management Interface Wizard, security banner.
	Compliance	RoHS (EN 50581:2012), WEEE regulations.
Certification	Standards	EN 60950-1, IEC 60950-1, EN61000, EN 60825.
Warranty and Support	Warranty	Limited Lifetime warranty from OEM.

Access Switch (Quantity: 25)

Category	**Specification**	**Details**
Architecture	Form Factor	19" rack-mountable, 24x 10/100/1000 BASE-T ports, 4x 10G SFP ports.
	Ports	Dedicated Console Port.
	Performance	128 Gbps switching capacity, 95 Mpps throughput.
	Memory	4 GB SDRAM, 16 GB flash, 12 MB packet buffer, 8,000 MAC addresses.
	Routing/ACL	512 IPv4/IPv6 Unicast Routes, 512 IGMP/MLD Groups, 512 IPv4/IPv6/MAC ACL ingress entries.
IPv6 Features	Management	IPv6 host management.
	Dual Stack	Support IPv4/IPv6 connectivity.

	MLD Snooping	Forward IPv6 multicast traffic.
	ACL/QoS	Support ACL and QoS for IPv6 traffic.
	Routing	IPv6 Static routing.
	Security	RA guard, DHCPv6 protection, dynamic IPv6 lockdown, ND snooping.
High Availability and Resiliency	UDLD	Uni-directional Link Detection to prevent STP loops.
	LACP	IEEE 802.3ad LACP, up to 8 LAGs, static/dynamic groups, user-selectable hashing.
	Spanning Tree	IEEE 802.1s Multiple Spanning Tree, legacy support for 802.1d, 802.1w.
	QoS	Strict priority queuing, IEEE 802.1p, CoS, IP ToS, Layer 3 protocol, TCP/UDP port number, DiffServ, rate limiting, per-queue minimums, large buffers for congestion management.
Management	API	Built-in programmable REST API.
	Management Options	On-premises, cloud-based management.
	Monitoring	Scalable ASIC-based wire-speed monitoring, sFlow (RFC 3176).
	CLI	Industry-standard CLI with hierarchical structure.
	Security	Restrict access to critical commands, multiple privilege levels, password protection, syslog.
	SNMP	SNMP v2c/v3, industry-standard MIB, private extensions.
	RMON	Support events, alarms, history, statistics, private alarm extensions.
	Configuration	TFTP, SFTP for configuration updates.
	Utilities	Ping, traceroute for IPv4/IPv6.
	NTP	Network Time Protocol for time synchronization.
	LLDP	IEEE 802.1AB LLDP for network mapping.
	Flash Images	Dual flash images, multiple configuration files.
Multicast	IGMP Snooping	Reduce IPv4 multicast traffic.
	MLD	Discovery of IPv6 multicast listeners (MLD v1, v2).
	IGMP	Support IGMPv1, v2, v3.
Layer 2 Switching	VLANs	4094 VLAN IDs, 512 VLANs simultaneously.
	Jumbo Packets	Support frame size up to 9198 bytes.
	RPVST+	Rapid Per-VLAN Spanning Tree.
	MVRP	Automatic VLAN learning and assignment.
	Port Mirroring	Minimum 4 mirroring groups.

	STP	IEEE 802.1D STP, 802.1w RSTP, 802.1s MSTP.
	IGMP	Control multicast packet flooding.
Layer 3 Routing	Static Routing	Static IP routing, dual stack IPv4/IPv6 routes.
	Dual Stack	Separate IPv4/IPv6 stacks for transition.
Convergence	LLDP-MED	Support Media Endpoint Discovery for QoS, VLAN configuration.
	Auto VLAN	Support RADIUS VLAN, LLDP-MED for IP phone configuration.
Security	TPM	Integrated TPM for platform integrity.
	ACL	IPv4/IPv6 filtering based on Layer 2/3 headers.
	ACL Filtering	Filter by IP field, source/destination IP address/subnet, TCP/UDP port number (per-VLAN/port).
	Authentication	RADIUS, TACACS+.
	Control Plane	Control Plane Policing for DOS protection.
	Authentication Methods	IEEE 802.1X, Web, MAC, up to 32 sessions per port.
	Secure Access	SSHv2, SSL, SNMPv3.
	Protection	CPU protection, ICMP throttling, identity-driven ACL, STP BPDU protection, Dynamic IP lockdown, STP root guard, port security, MAC address lockout, source-port filtering, Secure Shell, SSL, Critical Authentication Role, MAC Pinning.
	Security Banner	Display customized security policy on login.
	Compliance	RoHS (EN 50581:2012), WEEE regulations.
Certification	Standards	EN 60950-1, IEC 60950-1, EN 60825, CAN/CSA C22.2 No. 60950, UL 60950-1.
Warranty and Support	Warranty	Limited Lifetime warranty from OEM.

SFP Modules (Quantity: 65)

Specification	**Details**
Type	Single mode Fiber SFP Transceiver.
Specification	10G SFP+ LC LR 10km, from same OEM as network switches.

Network Monitoring Software (Quantity: 1)

Specification	**Details**
Functionality	WLAN, wired LAN, VPN management.
License	Perpetual license, accommodate up to 125 networking devices, deployed on-prem as virtual appliance.
Features	- Zero Touch Provisioning. - User and application visibility/control. - Multivendor and third-party integration. - Wi-Fi connectivity health analytics. - Role-based access.

	- Stage-based connectivity health.
Support	5-year support from OEM.

Server Specification (Quantity: 4)

Category	**Specification**	**Details**
Processor	CPU	2x 4th or latest generation Intel Xeon Gold Processor, minimum 32 physical cores per socket, 2.1 GHz base clock frequency .
Memory	RAM	Minimum 512 GB DDR5 4800 MT/s Registered DIMM, expandable to 4 TB.
Network/Storage	Adapters	Dual Port 10G Base T Network Adapter, Dual Port 32G FC HBA Card.
	RAID Controller	Internal 12G SAS RAID Controller supporting RAID 1, 5, 6.
	Storage	2x 960 GB Enterprise SSD or higher, configured in RAID 1 for OS/Hypervisor.
	Disk Bays	Minimum 8 SFF disk bays supporting SAS SSD.
Power/Fans	Redundancy	Internal hot-plug redundant power supply units, hot-plug redundant fan units.
PCI Slots	PCIe	Support PCIe 5.0 cards.
Hypervisor	OS	VMware vSphere Enterprise Plus 7.x or higher, fully licensed for populated processor/core.
Management Features	Systems Management	- Role-based access control. - Dynamic USB port management. - Real-time out-of-band hardware performance monitoring & alerting, predictive failure monitoring. - Monitor CPU, RAM, HD, fans, BIOS, power supplies, HBA, NICs. - Automatic hardware configuration/license restoration during system board replacement. - Automated hardware configuration and OS deployment to multiple servers. - HTML5 graphical remote virtual console & virtual media without Java/ActiveX. - Dedicated 1G remote management port/controller with full remote management functionality, IPMI 2.0 compliant, SSL/TLS encryption. - Storage space for firmware/drivers/software, rollback/patch support, zero-touch repository manager, self-updating firmware. - Agent-free monitoring/management, driver updates, configuration, telemetry streaming.
	Remote Management	Fully integrated remote console, virtual KVM, GUI-based, virtual media support.
Ports	USB	Minimum 2x USB 3.0 or higher.
Form Factor	Rack	1U or 2U rack-mountable, rack mounting kit for standard 42U rack.
Cables	Power	Power cables C13-C14.

Certification	VMware	VMware certified for vSphere Enterprise Plus, verified at VMware Compatibility Guide portal.
Warranty and Support	Warranty	5-year comprehensive OEM warranty, 24x7x365 support, patches/updates for hardware/software, including hypervisor. OEM must be VMware Global OEM Alliance-Premier partner or provide letter from VMware for support authorization.

Storage Specification (Quantity: 1)

Category	**Specification**	**Details**
Architecture	Type	Hybrid block storage array with dual hot-swappable active/active controllers.
	Capacity	240 TB raw capacity.
	RAID	Support RAID 1, 5, 6, 10 or equivalent.
Connectivity	Ports	- 4x 32G FC ports for host connectivity. - 4 host ports per controller, 8 host ports per array. - 16G FC transceivers and patch cords for minimum 4 host ports. - FC protocol for sharing LUNs as block devices to servers running virtualization.
	Management Port	Ethernet management port for storage array management.
Cache/Memory	Cache	Minimum 48 GB read/write cache and system memory per array (excluding SSD/HDD capacity).
Scalability	Capacity	Maximum raw capacity of 2.88 PB with/without additional enclosures.
	Drives	Support 24 SFF drives per array, minimum 120 LFF HDD/SSD per array.
	Enclosures	Support minimum 9 enclosures with 12Gb SAS expansion slots.
	SSD Cache	Support SSD read cache extension.
	Volumes/Snapshots	Up to 512 volumes, 512 snapshots per array, volume copy.
	Hosts/Initiators	Up to 512 hosts, 1024 initiators.
Features	Thin Provisioning	Support thin provisioning.
	Redundancy	No Single Point of Failure (SPOF), all components redundant and hot-swappable (power supply, fans, etc.).
	Performance	Deliver at least 700,000 IOPS random reads, 200,000 random writes with additional disks.
	OS Support	Support VMware vSphere, Windows Server 2022, RedHat Enterprise Linux, etc.
	Tiering	Auto Tiering (Performance, Standard, Archive tiers).
	Replication	Array-based asynchronous local and remote replication, available from day 1.
	Management	Browser-based/web-based management over IP.
	Upgrades	Non-disruptive online controller code upgrade.

	VAAI	Support vStorage API for Array Integration (VAAI).
Form Factor	Rack	Rack-mountable, rack mounting kit for standard 42U rack.
Accessories	Connectivity	All accessories for SPOF-free connectivity provided by supplier.
Warranty and Support	Warranty	5-year comprehensive OEM warranty, 24x7x365 support, patches/updates for hardware/software.

Server Virtualization Software (Licensing as Per Server Core/Sockets)

Category	**Specification**	**Details**
Platform	Hypervisor	Based on stable, open-source hypervisor platform.
	Virtualization Types	Support full virtualization (hardware-assisted) and container-based virtualization.
Management	Interface	Centralized web-based user interface.
	Migration	Support live migration of virtual machines and containers.
	RBAC	Role-based access control.
	Networking	Support VLANs, bridges, software-defined networking (SDN).
	Security	Integrated firewalling, network segmentation, two-factor authentication (2FA), secure web access.
	Monitoring	Built-in logging and monitoring.
	Dashboard	Centralized dashboard for performance, usage, health metrics.
	Notifications	Email/alert notifications for critical events.
	User Management	User role management with access auditing.
	Portal	Web-based management portal over HTTPS.
	API	API access for automation and scripting.
High Availability	Failover	High-availability with automatic failover.
	Synchronization	Central configuration synchronization across nodes.
Storage	Support	Shared or distributed storage for live migration and HA.
	Protocols	Compatibility with NFS, iSCSI, ZFS, Ceph-like protocols.
	Redundancy	Redundant storage paths, data integrity protection.
	Tiering	Optional tiered storage (SSD + HDD) or all-flash arrays.
Security	Hardening	Secure boot, system hardening.
	Encryption	Encrypted backup, data-in-transit protection.
	Updates	Regular software update and patch capability.
	Isolation	Isolation between virtual machines and networks.
	Authentication	Multi-factor authentication for admin access.
Services	Installation	Installation and configuration of virtualization platform and cluster.
	Integration	Integration with existing IT infrastructure (network/storage).
	Testing	Testing and validation of HA, backup, migration.
	Training	Basic and advanced training for IT administrators.
	Documentation	Setup, admin guides, operational procedures.

	Support	5-year post-deployment support and maintenance.
Eligibility Criteria	Experience	Minimum 3 years’ experience in deploying virtualization solutions.
	Deployments	At least 3 similar deployments completed successfully.
	Support	Ability to provide local support and training.

Racks & UPS

Category	**Specification**	**Details**
Racks (Quantity: 2)	Type	Floor standing, 42U, 800x1200 mm with PDU, all required accessories.
	Material	Steel frame with powder-coated finish.
	Load Capacity	Minimum 1500 kg static.
	Cooling	Compatible with fan module (supplied).
	PDU	2x 12-socket 15A/230V PDU (horizontal/vertical mount).
	Ingress Protection	IP20.
UPS (Quantity: 1)	Rating	10kVA/10kW, online double conversion.
	Input	230V/400VAC.
	Bypass	Automatic and manual.
	Interface	LCD or LED panel with status indicators.
	Communication	RS-232, USB, SNMP slot.
	Alarms	Audible alarms for battery mode, low battery, fault, overload.
	Battery	10x 12V 120Ah Sealed Maintenance-Free (SMF) VRLA batteries.
	Battery Rack	Suitable rack for housing batteries with insulation and cable connections.
	Cabling	Interlink cables with lugs and terminations included.

Passive Networks

Category	**Specification**	**Details**
Optical Fiber Cables	6 Core OFC	1500m, indoor/outdoor, multi-tube, gel-filled, ECCS armored, FRP central strength member, tensile strength 2500N, crush resistance 4000N/10cm, operating temperature -20°C to +70°C, anti-rodent, anti-termite, UV protected.
	12 Core OFC	900m, same specifications as 6 Core OFC.
LIU	24 Port LIU (Server Room)	Sliding type, OS2, expandable to 72 fibers, loaded with 2x 12F LC modular cassette, 12 colored pigtails, CRS material, direct OFC termination, RoHS compliant, includes splice trays and glands.
	24 Port LIU (Backbone)	Sliding type, OS2, lockable with key, expandable to 96 fibers, loaded with 1x 24F LC adapter, 12 colored pigtails, CRS material, direct OFC termination, RoHS compliant, includes splice trays and glands.
Patch Cords	Single Mode	25x 2.5m single mode fiber patch cords.

Services	Cabling	Cable laying, termination/splicing, Fluke/OTDR/OLTS testing, digging for outdoor cabling, 25-year performance warranty certificate.
	Conduits	ISI PVC/GI conduit pipes as per site requirements.

Data Center Civil Works and Other Acessories

Category	**Specification**	**Details**
Fire Extinguisher	Type	Automatic modular, ceiling-mounted, full room coverage.
	Specifications	Hazard-free clean agent or seal fire foam, 5 kg capacity, 15 bar working pressure, clear instruction label, no maintenance.
	Preferred Make	Kanex, Ceasefire, Supermex.
Split AC (2 Nos)	Capacity	2 Ton, inverter type, 5-star energy rating, 230V/50Hz/single phase.
	Preferred Make	Bluestar, Mitsubishi, Carrier.
	Timer	Microcontroller-based, LCD display, user-friendly settings, equal operation time for both ACs, wall-mounted, programmable time settings (2, 4, 8, 10, 12 hours), manual/automatic operation, auto-switchover on unit failure/overtemperature.
Fire Retardant Door	Specifications	Equipped with vision panel, rockwool/honeycomb infill. Length: 1 Meter, Depth: 2.1 Meter
Rodent Repellant	System	VHFO system, high-frequency sound waves (>20 kHz), inaudible to humans, painful to pests.
	Components	One master console, satellite/transducers covering 380 sq.ft (open floor, raised floor, false ceiling).
	Sound Waves	Linear sine waves with constantly varying frequencies.
	Power	230V AC, 50 Hz, 800 milliwatt per satellite.
Room Biometric	System	Biometric fingerprint and proximity card readers at data center entrance, FCC/CE/UL-294 rated.
	Accessories	20 proximity cards, all necessary hardware/software/cabling.
Thermal Insulation	Specifications	13 mm thickness, one side aluminum foil faced XLPE, nitrile rubber (Arm Flex/Kflex). Area: 67.58 sq.mt (Length : 21.8 Meter, Breadth: 3.1 Meter)
Room Lighting	Specifications	40W LED fitting, 2x2 feet, square, cool white, 4 connected to UPS for emergency lighting.
Water Leak Detection	System	Cable sensors, water leak detection modules, I/O modules, control panel with minimum 4 zones, single-zone modules resistant to oxidation/erosion, relay output for controller connection, one serial interface.

Fire Retardant Paint	Specifications	Approved make, even shade over primer coat, painting putty for leveling, 2 coats of fire-retardant paint, base coating as per manufacturer’s recommendation. Area: 67.58 sq.mt (Length : 21.8 Meter, Breadth: 3.1 Meter)
Raised Floor	Specifications	Steel cementitious, 450-600 mm height, 600x600x35 mm, point load 450 kg, UDL 1350 kg/sq.m, M1000 panel type, edge support rigid grid, wear resistance <0.08 g/cm², hemispherical bottom profile, all-steel silver zinc-plated pedestal, grommets for cable entry. Area: 26.98 sq.mt (Length : 7.1 Meter, Breadth: 3.8 Meter)
False Ceiling	Specifications	Metal grid, powder-coated 0.5 mm thick hot-dipped galvanized steel tiles, 595x595 mm, regular edge (10 mm), suitable for 25 mm grid, powder-coated galvanized steel grid as per manufacturer’s specification. Area: 26.98 sq.mt (Length : 7.1 Meter, Breadth: 3.8 Meter)

Note: The bidder must provide the Make & Model for components where specified and ensure compliance with all listed specifications. All components must meet the required certifications, warranties, and support terms as outlined. **Plan of Proposed area for centralised data centre is attached with the Tender Documen**t

<u>Place of Supply and Installation/Upgradation :</u>

Thavakkara Campus, Kannur Civil Station P.O, Kannur – 670002

<u>Documents to be Scanned and upload</u>

Sl NO	Parameter Specific requirements	Documents
1	All Tenderers should fill and submit the compliance statement Attached	Compliance statement to be submitted (Annexure 6)
2	The Bidder must be a company registered in India Shall have been in operation for a period of at least 5 years as on bid submission date.	Valid documentary proof of: Certificate of incorporation Company registration certificate. Valid GST registration certificate attached
3	The bidder should submit Manufacturer Authorization Form (MAF) from the OEM for the quoted products/items along with the technical bid.	Manufacturer Authorization Form to be submitted
4	The bidder must have a valid ISO 9001:2015 and ISO 27001:2013 or later certificate	Certificate copy to be enclosed
5	The Bidder should have implemented 3 Network and Server Storage Infra Project, Bidder Should have at least 5 Network/Server Engineer in the Payroll	One order of minimum 100 Lakhs/ two order Copy of work order(s) of 50Lakhs / Purchase Order/ Completion Certificate/ Project ongoing certificate/contract agreement to be attached

6	The Bidder/OEM should have been actively engaged in the field and shall have a registered office in Kerala for the last five years.	Copy of audited profit and loss account/ balance sheet of the last three financial years, highlighting the requisite figure related to positive net worth and profitability.
7	The Bidder/OEM should have positive net worth for the last three audited Financial Year.	Copy of audited profit and loss account/ balance sheet of the last three financial years, highlighting the requisite figure related to positive net worth and profitability.
8	The Bidding entity should not have been black listed for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice, breach of contract or restrictive practice by any Central/ State Government/PSU/Semi- Government bodies as on bid submission date	Self-Certification/ Declaration duly signed by authorized signatory on company letter head.
9	Detailed Bill of Materials for all the required components should be mentioned else the bidder will be disqualified.	BOM should be Submitted, Any Additional Materials required for successful completion of the Project must be include and supply by the Bidder without any additional charges .
10	OEM Should be the Leaders in Gartner for last 5 Years	Certificate/Report copy to be enclosed
11	Details of Site Visit	Sign off document for site survey should submitted along with the Technical Proposal
12	Copy of GST Payment Receipt	Copy of payment to Kerala GST Department (18% of tender fee). (MSME firms should upload MSME certificate/UDAYAM registration certificates)
13	Bidder Profile	As format mentioned in Annexure 1
14	Bid Particulars	As format mentioned in Annexure 2
15	Form of Tender	As format mentioned in Annexure 3
16	Completion Period Certificate	As format mentioned in Annexure 4
17	Integrity pact	As format mentioned in Annexure 5
18	Scanned copy of preliminary Agreement in Kerala Stamp Paper worth Rs.200/-	As per format Given in Annexure 7

Terms and Conditions

1. The tender should be submitted in two cover system (Technical bid & Financial bid).
2. Bidders shall keep their tendered rate firm for a period of 120 days from the date of opening of the tender.

3. The bidder shall quote their rates in the standard Indian currency in the BOQ provided, indicating the breakup details and the total rate tendered should be inclusive of all taxes, transportation, installation, supply, support charges & other Charges if any.
4. Tender fee and EMD for each item as given below should be remitted online (SBI MOPS) as indicated in the e-Tender website. However, 18% GST of the Tender Fee should be remitted to GST Department directly and upload the receipt in the e-procurement portal.

Sl. No	Item	Tender Fee	18% GST	Tender Fee including GST	EMD
1.	Supply, Installation/ Upgradation, Testing and Commissioning of Centralised Data Centre at Thavakkara Campus, Kannur University.	₹25,000/-	₹4,500/-	₹29,500/-	₹3,90,000/-

5. **All the MSMEs with Udyog Aadhar Registration or any other body specified by the Ministry of Micro, Small and Medium Enterprises working within the state of Kerala will be exempted from the payment of Tender Fee and EMD. Under MSME category, only Manufactures for Goods and Service Providers for Services are eligible for EMD/Tender fee exemptions.**
6. . Forfeiture of EMD:

   (i) If any bidder withdraws from his tender before the expiry of the bid validity period specified or

   (ii) in case after being successful bidder, he/firm fails to sign the contract, and to furnish the performance security
7. The bidder should upload along with the tender a preliminary agreement executed and signed in Kerala Stamp Paper of value of Rs.200/- as per format given as Annexure 7.
8. The successful bidder shall, before signing the agreement and within the period specified in the letter of acceptance of his tender, deposit a sum equivalent to **5% of the value of the contract** by way of Security Deposit or Demand Draft or bank guarantee drawn in favour of the **Finance Officer, Kannur University** payable at SBI Kannur Branch or Kannur Branch of other Nationalized or Scheduled bank, **as performance security** for the satisfactory fulfilment of the contract.
9. All bid/tender documents are to be submitted online only and in the designated cover(s)/envelope(s) on the website. Tenders/bids shall be accepted only through online mode on the website and no manual submission of the same shall be entertained.
10. Profile of Bidder as per Annexure 1 shall be provided.
11. Data sheet of the product(s) offered in the bid, are to be uploaded along with the bid documents. Buyers can match and verify the Data Sheet with the product specifications offered. In case of any unexplained mismatch of technical parameters, the bid is liable for rejection.
12. Bidders shall produce copy of the valid GST Registration and PAN card.
13. All the damages to the walls, floors, articles, etc.during the execution, shall be repaired and

modified/ replaced by the Firm at its own cost.

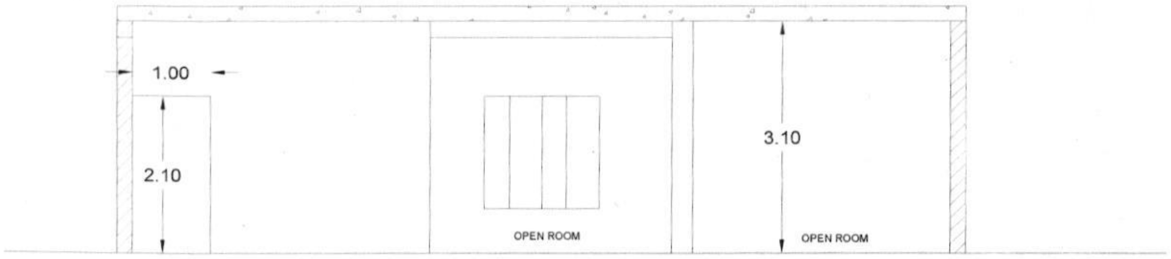
14. The bids shall be opened online at Kannur University on the date mentioned in Invitation Bid. If the date fixed for opening happens to be a holiday/ due to technical issue, the tenders will be opened on the next working day, at the same time.
15. Tenderers shall invariably specify in their tenders the delivery conditions including the time required for the supply of articles tendered for.
16. The final acceptance of the tenders rests entirely with the University who do not bind themselves to accept the lowest or any tender. But the tenderers on their part should be prepared to carry out such portion of the supplies included in their tenders as may be allotted to them.
17. Warranty of equipment not specifically mentioned in the Technical Specification will be 3 years.
18. The supplier shall guarantee to repair/replace without any extra cost, the items supplied or part thereof, if found defective due to bad designing, workmanship or substandard materials, within the warranty period. The entire expenditure towards replacement/repair in this regard shall be borne by the supplier. The period of warranty for the repaired/replaced item will recommence from the date of replacement/repair.
19. Payment will be made after the receipt and successful Installation, Testing, Commissioning of the System. No advance payment will be made to the Contractor/Supplier.
20. The financial bid of those bidders who qualify the technical evaluation after opening of Technical bid shall only be opened.
21. Dedicated/ toll free Telephone No. for service support, Escalation Matrix for Service support shall be provided.
22. Any attempt on the part of the tenderers or their agents to influence the University/Department in their favour by personal canvassing with the Officers concerned will disqualify the tenderers.
23. Registrar, Kannur University reserves the right not to process the tender , cancel the contract, supply order, hold the payment and to trade or not to trade the old stores without assigning any reason.
24. The tenderer shall have to pay all stamp duty, lawyers charges and other expenses incidental to the execution of the agreement.
25. The successful bidder has to execute an agreement within 15 days on receipt of the Purchase order. In cases where a successful bidder, after having made partial supplies fails to fulfil the contract in full, all or any of the materials not supplied may at the discretion of the Registrar, be purchased by means of another tender/ quotation or by negotiation or from the next higher bidder who had offered to supply already and the loss, if any caused to the University shall there by together with such sums as may be fixed by the University towards the damage be recovered from the defaulting bidder.
26. The Kannur University reserves the right to cancel the contract of the selected bidder and recover expenditure incurred by the Kannur University if the selected bidder commits a breach of any of the terms and conditions of the bid/contract.
27. Failure to supply and install the items within the specified time period as per the agreement will attract a penalty at the rate as specified in Kerala Stores Purchase Manual/ KPWD Manual.
28. Custom clearance of the consignment including all the stages of custom clearance will be under the purview of the supplier.

29. The provisions of Kerala Stores Purchase Manual/ KPWD Manual Rules are applicable to this tender and further proceedings.
30. No tender received after the specified date and time will be accepted on any account.
31. No representation for enhancement of rates once accepted will be considered.
32. Further Information and inquiries can be obtained from the Director, IT Directorate, Kannur University during working hours of the University. **Phone: 0497 2715468**

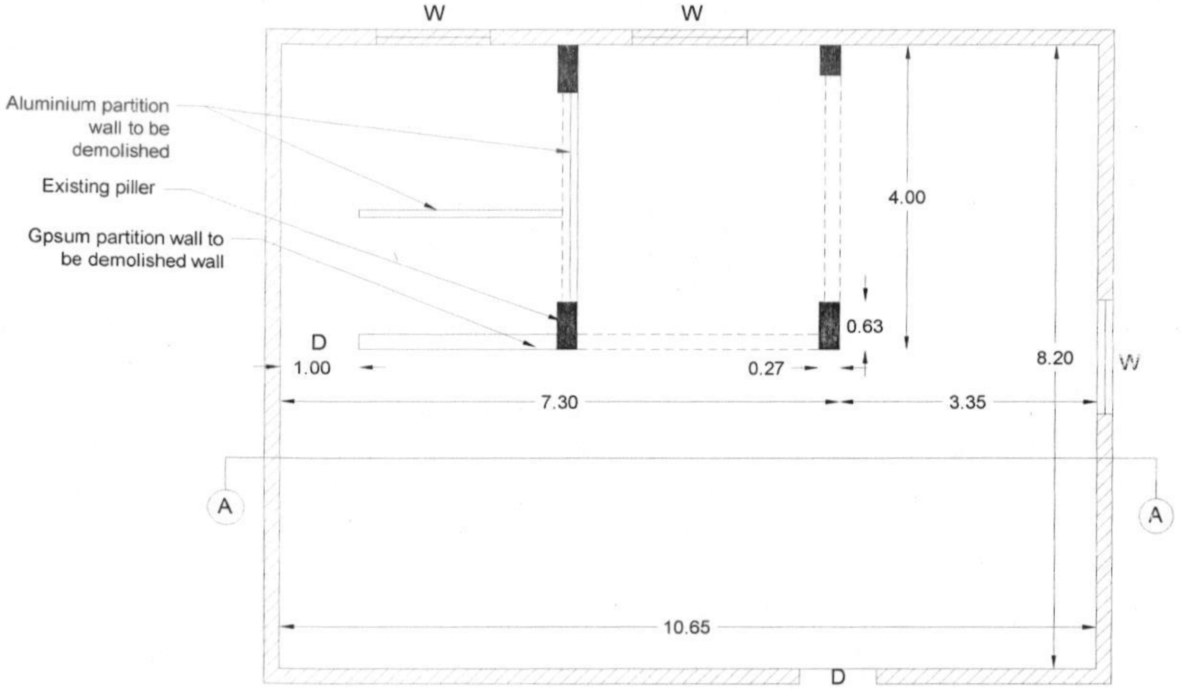
GST No of Kannur University : 32AAAGK0152J1ZT

sd/-
Registrar
Prof. (Dr.) Joby K Jose

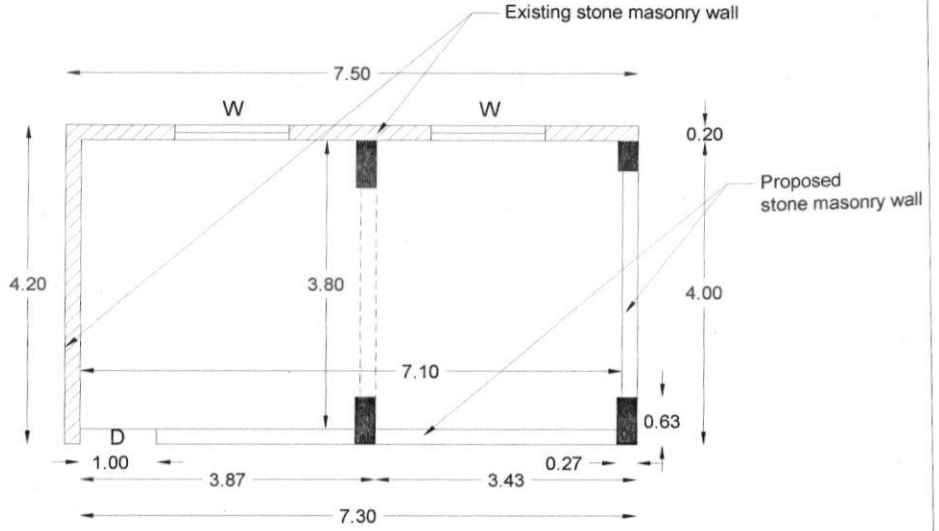
CENTRALISED DATA CENTRE AT THAVAKKARA CAMPUS,KANNUR UNIVERSITY



SECTION A-A


W
W
Aluminium partition wall to be demolished
Existing piller
Gpsum partition wall to be demolished wall
4.00
0.63
D
1.00
0.27
8.20
W
7.30
3.35
A
A
10.65
D

EXISTING PLAN OF IT CENTER



PLAN OF PROPOSED AREA FOR CENTRALISED DATA CENTRE

SCALE 1:100
ALL DIMENSIONS ARE IN M

Assistant Executive Engineer
Kannur University

ANNEXURE 1

BIDDER PROFILE

Sl.No.	Particulars	
Details of bidder (Firm/Company)		
1	Name	
2	Address	
3	Telephone & Mobile Number	
4	Email & website	
Details of Authorized Person		
5	Name	
6	Address	
7	Telephone & Email	
Information about the company		
8	Status of Company (Public Ltd. / Pvt. Ltd)	
9	Details of Registration of Firm (Provide Ref.)	
10	Number of Professionals	
11	Location and address of offices (in India & overseas)	
12	Service Tax Registration Number	
13	Income Tax Registration Number(PAN)	
14	GST Registration Number	

Signature of the Bidder

ANNEXURE 2
TECHNICAL BID (BID PARTICULARS)

1. Tender Number :---

2. Name of the Bidder :---

3. Full Address of the Bidder :---
----

4. Name of the actual signatory of the
product(s) offered :--

5. Bidder’s proposal number and date :--

6 . Name & Address of the officer to
whom all references shall be made
regarding the Tender :---

Telephone :--------------------------

Mobile **:** --------------------------

E-mail :--------------------------

Bidder Signature Name **-**-------------------

Designation -------------

Company ----------------

Date -------------

ANNEXURE – 3

FORM OF TENDER

Name of Work: Supply**,** Installation/ Upgradation, Testing and Commissioning of Centralised data Centre at Thavakkara Campus, Kannur University under PM-USHA Scheme.

From,

………………………………..

…………………………………

…………………………………

To,

The Registrar,
Kannur University,
Thavakkara, Kannur.

Sir,

I/We do hereby tender to execute the works enumerated in the Schedule accompanying in accordance the terms in your tender Notification…………………………..date…………..and specifications and conditions of contract in the bidding document.

In consideration I/We being invited to tender, I/We agree to keep the tender open for acceptance 120 days from the date of submission thereof and not to make any modifications in its terms and conditions which are not acceptable.

I/We agree that the tender inviting authority shall, without prejudice to any other right or remedy be at liberty to forfeit the earnest money/ Bid security absolutely and also recover from me/us the entire loss that may be caused to the Kannur University by the retender or rearrangement of the work or otherwise under the provision of the Revenue Recovery Act or otherwise.

Signature :

Full Name & Address of Bidder :

ANNEXURE – 4

COMPLETION PERIOD

(To be submitted in the letter pad of the firm indicating full name and address,
telephone no. & E-mail etc.)

Supply**,** Installation/Upgradation, Testing and Commissioning of Centralized Data Centre at Thavakkara Campus, Kannur University as per the Schedule of Work shall be completed within a period of **90 Days** from the date of receipt of Purchase Order.

SIGNATURE OF THE BIDDER WITH SEAL

Annexure- 5

Integrity Pact

CERTIFICATE

I/We…………………………………………undertake that the tender submitted by us is downloaded from the website www.etenders.kerala.gov.in and any deviation, of detected, at any stage, would entitle the Employer to reject our bidding/offer without assigning any reason or recourse to any penal action and would be legally binding on us.

Signature ....(of tenderer)

Seal ……………………………

Annexure 6

Compliance Statement

NETWORK FIREWALL

SN	Minimum Technical Specification- Quantity:02	Compliance (Y/N)
	General Requirements	
	The OEM of the network gateway and security appliance must have at least 20 years of experience in the security market.	
	The OEM must be capable of serving the entire scope of security gateway requirements, including throughput, connection rate and next generation security application enablement for all network deployments, from small office to data center in a single hardware appliance.	
	The OEM must have a virtualized security gateway solution that can support the enablement of all next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus, all managed from a central platform.	
	Features and applications requirements	
	The appliance must be capable of supporting next generation security applications listed below on a unified platform. These applications must be exclusively supplied by and managed by the OEM. a) Stateful Inspection Firewall b) Intrusion Prevention System c) Application Control and URL Filtering d) Anti-Bot and Antivirus e) IPSec VPN f) Logging and Status g) Event Correlation and Reporting	
	The security gateway must use Stateful Inspection based on granular analysis of communication and application state to track and control the network flow.	
	The firewall should be based on x64 architecture and should not be of any proprietary or ASIC based architecture.	
	Shall have minimum of 1.5 Gbps of Threat Prevention throughput, measured with Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and Zero-Day protection with logging enabled.	
	Shall have minimum of 3.5 Gbps of NGFW Throughput, measured with Firewall, IPS and Application Control with logging enabled.	
	Shall have minimum of 4.5 Gbps IPS throughput	
	Shall have minimum 17 Gbps Firewall (1518B UDP) throughput	
	Shall have minimum 65000 Connections per Second	
	Shall have minimum 4 million concurrent sessions at day 1 and expandable to 8 million with the addition of RAM in future.	
	Shall have minimum 1 CPU with 2 Physical Cores	

	Shall have minimum 16GB RAM	
	Shall have minimum 200GB SSD storage	
	Shall support configuring minimum 20 Virtual Systems	
	Shall support event logging and maintain for a minimum of 180 days with or without a management appliance.	
	Shall have Redundant AC power supplies	
	The communication between the management servers and the appliance must be encrypted and authenticated with PKI Certificates.	
	The following user authentication schemes must be supported by the appliance and VPN module: SecureID, TACACS, RADIUS and digital certificates	
	Appliance must support DHCP server and DHCP relay	
	Appliance must have the ability to work in Transparent/Bridge mode	
	Shall support Firewall, IPS, Application control, URL filtering, Antivirus, Anti-bot, Threat Emulation and Threat Extraction from day 1.	
	Shall support Active/Active and Active/Passive HA configuration.	
	IPv6 Support and features	
	Appliance must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface	
	Appliance must support IPv6 traffic handling on IPS and App module, Firewall, Identity Awareness, URL Filtering, Antivirus and Anti-Bot	
	Appliance must Support 6 to 4 NAT, or 6 to 4 tunnels	
	Appliance must log and show ipv6 traffic	
	Appliance shall support displaying IPv6 routing table	
	Intrusion Prevention System	
	IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection.	
	IPS and firewall module must be integrated on one platform.	
	IPS must have options to create profiles for either client or server-based protections, or a combination of both.	
	IPS must provide at least two pre-defined profiles/policies.	
	IPS must have a software-based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage.	
	IPS must provide an automated mechanism to activate or manage new signatures from updates.	
	IPS must support network exceptions based on source, destination, service or a combination of the all.	
	IPS application must have a centralized event correlation and reporting mechanism.	

	The administrator must be able to automatically activate new protections, based on configurable parameters (performance impact, threat severity, confidence level, client protections, server protections)	
	For each protection the solution must include protection type (server-related or client related), threat severity, performance impact, confidence level and industry reference.	
	IPS must be able to collect packet capture for specific protections.	
	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP.	
	IPS and/or Application Control must include the ability to detect and block P2P & evasive applications.	
	The administrator must be able to define network and host exclusions from IPS inspection	
	Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses.	
	IPS and/or Application Control must detect and block remote controls applications, including those that are capable tunneling over HTTP traffic	
	IPS must have a mechanism to convert SNORT signatures	
	Total solution must allow the administrator to easily block inbound and/or outbound traffic based on countries, without the need to manually manage the IP ranges corresponding to the country.	
	Application Control and URL Filtering	
	Application control database must contain a minimum of 6000 known applications.	
	Solution must have a URL categorization that exceeds 200 million URL's.	
	Solution must allow to create a filtering rule with multiple categories.	
	Solution should inspect HTTPS based URL Filtering without requiring SSL decryption.	
	Solution should allow to create a filtering for single site being supported by multiple categories.	
	Solution must have users and groups granularity with security rules.	
	Solution must have an easy to use, searchable interface for applications and URLs.	
	Solution must categorize applications and URLs and applications by Risk Factor.	
	The solution must have unified application control and URL security rules.	
	The solution must provide a mechanism to limit application usage based on bandwidth consumption.	
	Solution must include a Black and White lists mechanism to allow the administrator to deny or permit specific URLs regardless of the category.	
	Solution must provide an override mechanism on the categorization for the URL database.	
	Anti-Bot and Anti-Virus features	
	OEM must have an integrated Anti-Bot and Anti-Virus application on the appliance.	
	Anti-bot application must be able to detect and stop suspicious abnormal network behaviour.	
	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications.	

	Anti-Bot protections must be able to scan for bot actions	
	The solution should have mechanisms to protect against spear phishing attacks.	
	Anti-Bot and Anti-Virus policy must be administered from a central console.	
	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism.	
	Anti-virus application must be able to prevent access to malicious websites.	
	Anti-virus application must be able to inspect SSL encrypted traffic.	
	Anti-Virus must be able to stop incoming malicious files.	
	Anti-Virus must be able to scan archive files.	
	Anti-Virus and Anti-Bot policies must be centrally managed with granular policy configuration and enforcement.	
	The Anti-Virus should support scanning for links inside emails.	
	The Anti-Virus should Scan files that are passing on CIFS protocol.	
	Security Management	
	Management and Firewall should be two separate systems. Management can be virtual appliance or bare metal hardware installation.	
	NGFW appliances must be managed from a centralized dedicated management system separate from the NGFW appliance.	
	Device Management system includes Centralized Management, logging, reporting and basic event correlation functionality in the single box.	
	Device Management system should provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.	
	Management platform should provide autonomous threat prevention security policy.	
	Solution must be able to segment the rues base in favour of delegation of duties in which changes in one segment will not affect other segments on the same autonomous system.	
	The device must provide a minimum basic statistic about the health of the firewall and the amount of traffic traversing the firewall.	
	Solution must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant policy segment for an autonomous system.	
	Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks.	
	Solution must have capabilities for multi-domain management and support the concept of global security policy across domains.	

WAN SWITCH

Sr. No	Minimum Technical Specification- Quantity:02	Compliance (Yes/No)
1	**Architecture**	
	Shall be 19" Rack Mountable and must have 24x ports 10/100/1000 BASE-T PoE+ ports and 4x 10G SFP+ ports with 370W POE power.	
	The switch should have 1x USB-C Console Port , 1x OOBM and 1x USB Type A Host port and 8GB SDRAM and 16 MB flash and 8 MB Packet buffer size	
	The swith should support stacking on uplink port or dedicated stack module and should suppot minimum 8 switch in stack	
	The Switch should support 16000 MAC address	
	The switch should have minimum 2K Ipv4 Unicast Routes ,1K Ipv6 Unicast Routes ,1K Igmp Groups ,1K Mld Groups ,5K Ipv4 ingress Entries and 2K Ipv4 egress ACL Entries.	
	The switch should have 128 Gbps of Switching Capacity and 95 Mpps Throughput Capacity	
	The switch support High availability with always-on PoE.	
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 routing supports Static and OSPFv3 protocols	
	RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
3	**High Availability And Resiliency**	
	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 32 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	
4	**Management**	
	The Switch should support Built-in programmable and easy to use REST API interface. It must support ZTP simplifies installation of switching infrastructure using DHCP-based	
	The Switch should support On-premises and cloud- based management and 3rd party NMS solution	
	The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	

	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	
	The Switch should support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests	
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 IEEE 802.1v protocol VLANs to isolate select non-IPv4 protocols automatically into their own VLANs	
	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 VXLAN encapsulation (tunnelling) protocol for overlay network that enables a more scalable virtual network deployment	
	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 Open shortest path first (OSPF) to deliver faster convergence.	
	The Switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing	
	The Switch should support Static IP routing provides manually configured routing	
	The Switch should support Static IPv4 and IPv6 routing to provide simple manually configured IPv4 and IPv6 routes	
	The Switch should support IP performance optimization to provide a set of tools to improve the performance of IPv4 networks including directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities	
	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	
9	**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 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	
	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	
	The Switch should support Green initiative for RoHS (EN 50581:2012) and WEEE regulations	
10	**Certification**	
	EN 60950-1:2006 EN 62368-1 UL 60950-1 CAN/CSA-C22.2 No. 60950-1-07 IEC 60950-1:2005 IEC 62368-1:2014 CNS-14336-1	
11	**Warranty and Support**	
	The switch shall be offered with Limited Lifetime warranty from OEM directly	

CORE SWITCH

	Minimum Technical Specifications of Items	
Sr. No	**Minimum Technical Specification- Quantity:02**	**Compliance (Yes/No)**

1	**General Features**	
	The switch should be Gigabit Layer 2 and Layer 3 switch with console, OOBM ports, USB ports along with all accessories.	
	Switch should have hot swappable redundant Power Supply and fan tray from day-1.	
	Switch should have non-blocking throughput from day 1.	
	Software upgrades, updates shall be included as part of the warranty	
	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software to optimize performance and capacity	
	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source	
	Operating temperature of 0°C to 40°C and 15% to 95% Operating Relative Humidity	
	All mentioned features (above & below) should be available from day 1. Any license required to be factored from day 1	
2	**Performance**	
	Should have 16GB DRAM and 32 GB Flash memory.	
	The switch will have at up to 1.28 Tbps switching capacity.	
	Forwarding rates: The switch should have 900 Mpps forwarding rates.	
	IPv4 unicast routes support : 24K or more.	
	IPv6 unicast routes support : 12K or more.	
	IPv4 and IPv6 Multicast Routes : 4K or more.	
	MAC addresses support: 140K or more.	
	VLANs ID: Min 1K VLANs simultaneously.	
	ACL /QOS entry support : 4K or more.	
	Packet buffer : 32 MB or more	
	The device should be IPv6 ready from day one.	
	Should support the ability to configure backup of the previous configuration automatically.	
3	**Functionality:**	
	The proposed switch should support distributed and redundant architecture by deploying two switches with each switch maintaining independent control and synchronized during upgrades or failover and should support upgrades during live operation.	
	The Switch should support long distance across the Rack and Floor Switch Stacking.	
	Must support RIPv2, RIPng, EVPN, BGP, BGP4, MP-BGP, VRF, VXLAN, EVPN, OSPFv2 and v3 Routed Access, Policy-Based Routing (PBR), PIM SM, DCBX, PFC, ETS, PIM-DM, PIM-SSM and Virtual Router Redundancy Protocol (VRRP) from Day 1	
	The switch should support IEEE 802.3ad link-aggregation control protocol (LACP) and port trunking	
	The switch should support IEEE 802.1s Multiple Spanning Tree	

	The switch should support STP, Trunking, Q-in-Q, Deficit Weighted Round-Robin(DWRR) or equivalent scheduling, Committed Information Rate (CIR)/Equivalent and eight egress queues per port	
	Switch shall support rolled back to the previous successful configuration	
	The switch should support SNMPv1, v2, and v3, SSL, SSHv2, Telnet, ping, traceroute	
	The switch should support Zero-Touch Provisioning (ZTP). The switch shall support IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests	
	The switch should be manageable from cloud NMS and On-premises NMS solution	
	The switch should provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number	
	The switch should support Source-port filtering	
	The switch should support IEEE 802.1X	
	The switch should support RADIUS/TACACS+, Dynamic ARP protection, Port Security, STP route guard, BPDU guard.	
	OS should have support for Management automation via REST-API, Python or equivalent technology	
	Should support Sflow, Port mirroring or equivalent technology	
4	**Interface Requirement**	
	i) 24 ports of 1G/10G SFP+ Ports Cables/Transceivers shall be populated as per the design	
	ii) 4 ports of 40GbE/100GbE (QSFP+/QSFP28). Cables/ Transceivers shall be populated as per the design	
5	**Regulatory Compliance**	
	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standard like IS-13252:2010 or better for Safety requirements of Information Technology Equipment.	
	Switch shall conform to EN 55022/55032 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standard like IS 6873 (Part 7): 2012 or better for EMC (Electro Magnetic Compatibility) requirements.	
6	**OEM qualification criteria, Warranty and Support**	
	The switch shall be offered with minimum five years hardware warranty with NBD Shipment and software updates/upgrades from OEM directly	
	Switch or Switch's Operating System on different hardware plateform should be tested for EAL 2/NDPP or above under Common Criteria Certification.	

DISTRIBUTION SWITCH

Sr. No	Minimum Technical Specification- Quantity:04	Compliance (Yes/No)
1	**Architecture**	

	24-Port 10-Gigabit SFP+ slots populated with required Transceivers, 4 x 1/10/25 SFP28 slots with DACs for interconnectivity, dual hot-swap PSUs (2 Nos.)	
	19" Rack mountable (Mounting kit should be included)	
	Quad core processor/CPU with minimum 8GB DRAM, 32GB eMMC/Flash memory and 8MB of packet buffer memory. Must have min 32000 entries of MAC Address	
	Switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software to optimize performance and capacity	
	Switching Capacity of 800 Gbps and 600 Mpps forwarding rate.	
	The swith should support front plane stacking on uplink port or Backplane stacking and should have Stacking Performance of minimum 200 Gbps. The switch should suppot minimum 8 switch in stack	
	The switch should have minimum 64,000 Ipv4 Unicast Routes ,32K Ipv6 Unicast Routes ,8K Ipv4 Multicast Routes,8K Ipv6 Multicast Routes,8K Igmp Groups ,4K Mld Groups 4,000 ,Ipv4/Ipv6/MAC ACL Entries (Ingress) 5000/1250/5000 and Ipv4/Ipv6/MAC ACL Entries (Egress) 2000/500/2000	
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	
	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 routing supports Static and OSPFv3 protocols	
	RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
3	**High Availability And Resiliency**	
	The Switch should support Bidirectional Forward Detection (BFD) to enable sub-second failure detection for rapid routing protocol re-balancing	
	The Switch should support Virtual Router Redundancy Protocol (VRRP) to allow groups of two routers to dynamically create highly available routed environments in IPV4 and IPV6 networks	
	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 256 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 IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking supports static and dynamic trunks where each trunk supports up to eight links (ports) per static trunk	

4	**Management**	
	The Switch should support Built-in programmable and easy to use REST API interface. It must support ZTP simplifies installation of switching infrastructure using DHCP-based	
	The Switch should support On-premises and cloud- based management and 3rd party NMS solution	
	The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	
	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 Dual flash images provides independent primary and secondary operating system files for backup while upgrading and 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 IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests	
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 Protocol Independent Multicast (PIM) defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information and support PIM Sparse Mode (SM) and Dense Mode (DM) for both IPv4 and IPv6	
	The Switch should support Internet Group Management Protocol (IGMP) and Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3	

	The Switch should support Multicast Service Discovery Protocol (MSDP) to efficiently routes multicast traffic through core networks	
6	**Layer 2 Switching**	
	The Switch should support VLAN and tagging for IEEE 802.1Q (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 IEEE 802.1v protocol VLANs to isolate select non-IPv4 protocols automatically into their own VLANs	
	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 VXLAN encapsulation (tunnelling) protocol for overlay network that enables a more scalable virtual network deployment	
	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 Border Gateway Protocol (BGP) provides IPv4 and IPv6 routing.	
	The Switch should support Equal-Cost Multipath (ECMP) enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth	
	The Switch should support Multi-protocol BGP (MP-BGP) enables sharing of IPv6 routes using BGP and connections to BGP peers using IPv6	
	The Switch should support Open shortest path first (OSPF) delivers faster convergence.	
	The Switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing	
	The Switch should support Static IP routing provides manually configured routing	
	The Switch should support Policy-based routing and usesa classifier to select traffic that can be forwarded based on policy set by the network administrator	
	The Switch should support Static IPv4 and IPv6 routing to provide simple manually configured IPv4 and IPv6 routes	
	The Switch should support IP performance optimization to provide a set of tools to improve the performance of IPv4 networks including directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities	

	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	
9	**Security**	
	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source	
	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 RADIUS and 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 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 DHCP protection blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks	
	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	
	The Switch should support Green initiative for RoHS (EN 50581:2012) and WEEE regulations	
10	**Certification**	
	EN 60950-1, EC 60950-1,EN 61000,EN 60825	
11	**Warranty and Support**	
	The switch shall be offered with Limited Lifetime warranty from OEM directly	

TOR SWITCH

Sr. No	Minimum Technical Specification- Quantity:02	Compliance (Yes/No)
1	**Architecture**	
	24-Port 1/10-Gigabit BaseT slots populated with required Transceivers, 4 x 1/25/50G SFP+ Ports with DACs for interconnectivity, dual hot-swap PSUs (2 Nos.)	
	19" Rack mountable (Mounting kit should be included)	

	Quad core processor/CPU with minimum 8GB DRAM, 32GB eMMC/Flash memory and 8MB of packet buffer memory. Must have min 32000 entries of MAC Address	
	Switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software to optimize performance and capacity	
	Switching Capacity of 800 Gbps and 550 Mpps forwarding rate.	
	The swith should support front plane stacking on uplink port or Backplane stacking and should have Stacking Performance of minimum 200 Gbps. The switch should suppot minimum 8 switch in stack	
	The switch should have minimum 64,000 Ipv4 Unicast Routes ,32K Ipv6 Unicast Routes ,8K Ipv4 Multicast Routes,8K Ipv6 Multicast Routes,8K Igmp Groups ,4K Mld Groups 4,000 ,Ipv4/Ipv6/MAC ACL Entries (Ingress) 5000/1250/5000 and Ipv4/Ipv6/MAC ACL Entries (Egress) 2000/500/2000	
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	
	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 routing supports Static and OSPFv3 protocols	
	RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
3	**High Availability And Resiliency**	
	The Switch should support Bidirectional Forward Detection (BFD) to enable sub-second failure detection for rapid routing protocol re-balancing	
	The Switch should support Virtual Router Redundancy Protocol (VRRP) to allow groups of two routers to dynamically create highly available routed environments in IPV4 and IPV6 networks	
	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 256 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 IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking supports static and dynamic trunks where each trunk supports up to eight links (ports) per static trunk	
4	**Management**	
	The Switch should support Built-in programmable and easy to use REST API interface. It must support ZTP simplifies installation of switching infrastructure using DHCP-based	

	The Switch should support On-premises and cloud- based management and 3rd party NMS solution	
	The Switch should have Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance.	
	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 Dual flash images provides independent primary and secondary operating system files for backup while upgrading and 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 IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests	
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 Protocol Independent Multicast (PIM) defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information and support PIM Sparse Mode (SM) and Dense Mode (DM) for both IPv4 and IPv6	
	The Switch should support Internet Group Management Protocol (IGMP) and Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3	
	The Switch should support Multicast Service Discovery Protocol (MSDP) to efficiently routes multicast traffic through core networks	
6	**Layer 2 Switching**	
	The Switch should support VLAN and tagging for IEEE 802.1Q (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 IEEE 802.1v protocol VLANs to isolate select non-IPv4 protocols automatically into their own VLANs	
	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 VXLAN encapsulation (tunnelling) protocol for overlay network that enables a more scalable virtual network deployment	
	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 Border Gateway Protocol (BGP) provides IPv4 and IPv6 routing.	
	The Switch should support Equal-Cost Multipath (ECMP) enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth	
	The Switch should support Multi-protocol BGP (MP-BGP) enables sharing of IPv6 routes using BGP and connections to BGP peers using IPv6	
	The Switch should support Open shortest path first (OSPF) delivers faster convergence.	
	The Switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing	
	The Switch should support Static IP routing provides manually configured routing	
	The Switch should support Policy-based routing and usesa classifier to select traffic that can be forwarded based on policy set by the network administrator	
	The Switch should support Static IPv4 and IPv6 routing to provide simple manually configured IPv4 and IPv6 routes	
	The Switch should support IP performance optimization to provide a set of tools to improve the performance of IPv4 networks including directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities	
	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	
9	**Security**	

	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source	
	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 RADIUS and 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 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 DHCP protection blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks	
	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	
	The Switch should support Green initiative for RoHS (EN 50581:2012) and WEEE regulations	
10	**Certification**	
	EN 60950-1, EC 60950-1,EN 61000,EN 60825	
11	**Warranty and Support**	
	The switch shall be offered with Limited Lifetime warranty from OEM directly	

ACCESS SWITCH

Sr. No	Minimum Technical Specification- Quantity:25	Compliance (Yes/No)
1	**Architecture**	
	Shall be 19" Rack Mountable and it must have 24x ports 10/100/1000 BASE-T ports and 4x 10G SFP ports	
	The switch should have dedicated Console Port and should have 128 Gbps of Switching Capacity and 95 Mpps Throughput Capacity	
	4GB SDRAM and 16GB flash and 12 MB Packet buffer size and 8000 MAC address	
	The switch should have minimum 512 Ipv4 Unicast Routes and 512 Ipv6 Unicast Routes ,512 Igmp Groups ,512 Mld Groups ,512 Ipv4 /512 IPv6 /MAC ACL ingress Entries.	

2	**IPv6 feature**	
	Switch should support IPv6 host enables switches to be managed in an IPv6 network	
	Switch should support Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols	
	Switch should support MLD snooping forwards IPv6 multicast traffic to the appropriate interface	
	Switch should support IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic	
	Switch should support IPv6 Static routing	
	Switch should support RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping	
3	**High Availability And Resiliency**	
	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 IIEEE 802.3ad LACP supports up to 8 LAGs and 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,Rate limiting ,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 have Scalable ASIC-based wire speed network monitoring and accounting using sFlow (RFC 3176) 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.	
	The Switch should support Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Switch should support events, alarms, history, and statistics groups as well as a private alarm extension group.	
	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 to facilitate 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. Switch should support Multiple configuration files which can be stored to a flash image	
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 supports IGMPv1, v2, and v3	
6	**Layer 2 Switching**	
	The Switch should support 4094 VLAN IDs and 512 VLANs simultaneously	
	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 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 Dual stack 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 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 and use standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones	
9	**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 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 Remote Authentication Dial-In User Service (RADIUS) and minal Access Controller Access-Control System (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 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 Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port and accepts up to 32 Concurrent 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 CPU protection to provide automatic protection against malicious network traffic trying to shut down the switch.	
	The Switch should support ICMP throttling.	
	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 and prevent forged BPDU attacks	
	The Switch should support Dynamic IP lockdown to block traffic from unauthorized hosts, preventing IP source address spoofing	
	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 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 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. UL 60950-1.	
11	**Warranty and Support**	
	The switch shall be offered with Limited Lifetime warranty from OEM directly	

SFP MODULES

	Minimum Technical Specification	Compliance(Y/N)
	Single mode Fiber SFP Transciever– Quantity: 65	
	Make & Model (To be filled by bidder)	
	10G SFP+ LC LR 10km , Transceiver must be from same OEM of Network Switches	

NETWORK MONITORING SOFTWARE

SN	Minimum Technical Specification	Compliance(Y/N)
	Network Monitoring Software – Quantity: 01	
	Make & Model (To be filled by bidder)	

	WLAN, wired LAN, and VPN management	
	Perpetual license can accommodate up to 125 Networking devices , Should be deployed on-prem as virtual appliance.	
	Zero Touch Provisioning	
	Should have User and application visibility and control	
	Should have Multivendor and third-party integration	
	Should have Wi-Fi connectivity health analytics	
	Should have Role-based access	
	Should have Stage-based connectivity health	
	5 Year support from OEM	

SERVER STORAGE

	Minimum Technical Specification	Compliance(Y/N)
	Server Specification – Quantity: 04	
	Make & Model (To be filled by bidder)	
	Shall have 2 x 4th or Latest generation Intel Xeon Gold Processor with A) minimum 32 Physical Cores Per Socket B) minimum 2.1 GHz Base Clock frequency	
	Shall have Minimum 512GB Memory with DDR5 4800 MT/s Registered DIMM Memory Modules, expandable up to 4TB	
	Shall have A) Dual Port 10G Base T Network Adapter B) Dual Port 32G FC HBA Card	
	Shall have Internal 12G SAS RAID Controller supporting Raid 1,5and 6	
	Shall have Internal Hard Disks of	
	A) Minimum 2 x 960GB Enterprise SSD or higher configured in RAID1 for OS/Hypervisor.	
	Shall have internal hot plug Redundant Power Supply Units	
	Shall have hot plug Redundant Fan Units	
	Shall support Internal PCI Slots: Shall support PCIe 5.0 cards	
	Shall support Minimum 8 SFF Disk Bays supporting SAS SSD	
	Shall provide Hypervisor OS: VMware vSphere Enterprise Plus 7.x or higher edition fully licensed for the processor/core populated	
	Shall have following features: a) The Systems Management software should provide Role- based access control. b) Shall support Dynamic USB Port management. c) Real-time out-of-band hardware performance monitoring & alerting, Predictive failure monitoring. d) Should be able to monitor all system health and systems components (CPU,	

	RAM, HD, FANs, BIOS, Power Supplies, HBA's, NICs). e) Automatically restore hardware configuration and license information during system board replacement and return system to production in minutes using the in-chassis backup with configuration. Automatically restore hardware configuration and license information during system board replacement and return system to production in minutes using the in-chassis backup with configuration. f) Automated hardware configuration and Operating System deployment to multiple servers. g) HTML5 graphical remote virtual console & virtual media without using Java or ActiveX plugins. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder. h) Should have dedicated 1G remote management port and controller with necessary software and licenses for full remote management functionally. Should support IPMI 2.0 compliant configuration, out of band management over Ethernet with SSL and TLS encryption. i) Should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized to rollback/patch faulty firmware. Zero-touch repository manager and self-updating firmware system. Support for quick sync. j) The Server Management Software should be of the same brand as of the server OEM. Agent-free monitoring & management; driver updates & configuration; Support for Telemetry Streaming for log analysis. k) License shall be enabled to fully manage the server from remote location, fully integrated remote console, virtual keyboard, video, and mouse (KVM), GUI based, support Virtual media etc.	
	Shall have A) Ports: Minimum 2 x USB 3.0 or Higher	
	Shall supply Rack Mounting Kit to mount the server on a standard 42U Rack	
	Shall provide Power Cables C13-C14	
	Server form factor shall be 1U or 2U rack mountable.	
	Proposed Server model should be VMware certified for running vSphere Enterprise Plus edition. This should be verified at the VMware Compatibility Guide portal.	
	5Yrs comprehensive Single OEM warranty including 24x7x365 support, patches and updates for all Hardware components and Software components including Hypervisor. Server OEM providing support should be VMware Global OEM Alliance-Premier partner or should provide a letter from VMware to substantiate they are authorized to provide support for VMware vSphere hypervisor.	
	Storage Specification – Quantity: 01	
	Make & Model (To be filled by bidder)	

	The Storage System shall be a hybrid block storage array with Dual hot-swappable active/active controllers.	
	Shall supply with A) 240TB Raw Capacity	
	The Storage shall support RAID1, RAID 5, RAID 6, RAID10 OR Equivalent RAID Levels	
	A) Storage shall have minimum 4 x 32G FC ports for host connectivity for FCcommunication. B) Shall support 4 host ports per controller, 8 host ports per array. C) Shall provide 16G FC transceivers and patch cords for connecting minimum 4 host ports of the Storage D) FC protocol shall be used to share the LUNS as block device to the proposed Server running Virtualization.	
	Storage shall have an Ethernet management port to manage the storage array.	
	A) The storage system shall have minimum 48 GB of Read/Write cache and system memory Per array. B) SSD/HDD capacity shall not be considered for Cache calculation.	
	A) Array shall support a maximum raw capacity of 2.88 PB with/without additional enclosures. B) Shall support 24 SFF drives per array.	
	A) Shall support at minimum 9 enclosures to expand storage capacity. B) Expansion slots shall be of 12Gb SAS.	
	Shall support SSD read cache extension.	
	Storage shall support minimum 120 LFF HDD/SSD per array	
	Storage shall support up to 512 volumes and 512 snapshots per array and volume copy.	
	Storage shall support up to 512 hosts.	
	Storage shall support up to 1024 initiators.	
	Storage shall support Thin provisioning.	
	The storage shall be with No Single Point of Failure (SPOF). All the components shall be redundant and hot swappable including power supply, fans etc.	
	Storage shall support delivering at least 7,00,000 IOPS Random Reads and 200,000 Randon Writes with additional disks.	
	Storage shall support multiple operating systems such as VMware vSphere, Windows Server 2022, RedHat Enterprise Linux etc.	
	Storage shall support Auto Tiering, like Performance tier, standard tier, archive tier.	
	Storage shall support array based asynchronous local and remote replication and shall be available from day 1.	
	Storage management software shall be browser-based/web based, which shall be accessible over IP.	
	Storage shall support non-disruptive online controller code upgrade.	
	Storage shall support vStorage API for Array Integration (VAAI)	

	A) Storage and Enclosures, if any, shall be rack mountable form factor. B) Shall supply Rack Mounting Kit to mount the server and/or enclosures on a standard 42U Rack	
	All accessories to connect and configure the storage without single point of failure to be provided by Supplier/Bidder.	
	5Yrs comprehensive Single OEM warranty including 24x7x365 support, patches and updates for all Hardware components and Software components.	

SERVER VIRTUALIZATION SOFTWARE

	Server Virtualization Software Specification – Licensing as Per Server Core/Sockets	**Compliance(Y/N)**
	Make & Model (To be filled by bidder)	
	The solution must:	
	Be based on a stable, open-source hypervisor platform	
	Support both full virtualization (hardware-assisted) and container-based virtualization.	
	Include a centralized web-based user interface for management.	
	Support live migration of virtual machines and containers.	
	Provide role-based access control (RBAC).	
	Include integrated firewalling and network segmentation features.	
	Support VLANs, bridges, and software-defined networking (SDN).	
	Enable two-factor authentication (2FA) and secure web access.	
	Provide built-in logging and monitoring features.	
	High-availability support with automatic failover.	
	Central configuration synchronization across nodes.	
	Shared or distributed storage support for live migration and HA	
	Optional integration with lightweight load balancing.	
	Support for distributed, shared, or centralized storage.	
	Compatibility with common storage protocols: NFS, iSCSI, ZFS, or Ceph-like.	
	Redundant storage paths and data integrity protection.	
	Optional tiered storage (SSD + HDD) or all-flash arrays.	
	Management and Monitoring	
	Centralized dashboard for performance, usage, and health metrics.	
	Email or alert notification for critical events.	
	User role management with access auditing.	
	Web-based management portal accessible over HTTPS.	

	API access for automation and scripting.	
	Security	
	Secure boot and system hardening.	
	Encrypted backup and data-in-transit protection.	
	Regular software update and patch capability.	
	Isolation between virtual machines and networks.	
	Multi-factor authentication for admin access.	
	Services Required	
	Installation and configuration of virtualization platform and cluster.	
	Integration with existing IT infrastructure (network/storage).	
	Testing and validation of HA, backup, and migration.	
	Basic and advanced training for IT administrators.	
	Documentation: setup, admin guides, operational procedures.	
	Post-deployment support and maintenance (5 years).	
	Eligibility Criteria for Bidders	
	Minimum 3 years' experience in deploying virtualization solutions.	
	At least 3 similar deployments completed successfully.	
	Ability to provide local support and training.	

RACKS & UPS

	Minimum Technical Specification	Compliance(Y/ N)
	RACK – 2 qty	
	Make & Model (To be filled by bidder)	
	Rack Type Floor standing	
	42U 800x1200 with PDU and all required Accessories	
	Material Steel frame with powder-coated finish	
	Load Capacity Minimum 1500 kg static	
	Cooling Provision Compatible with fan module (to be supplied)	
	Power Distribution Unit (PDU) 2 x 12-socket 15A/230V PDU (horizontal or vertical mount)	
	Ingress Protection IP20	
	UPS- Rack Mountable -1 Qyt	
	Make & Model (To be filled by bidder)	
	UPS Rating: 10kVA / 10kW	
	Type: Online Double Conversion	
	Input Voltage: 230V/400VAC	
	Bypass Automatic & Manual	

	Interface/Display LCD or LED panel with status indicators	
	Communication Ports RS-232, USB, SNMP slot	
	Audible Alarms For battery mode, low battery, fault, overload	
	Battery bank: 10 units of 12V 120Ah Sealed Maintenance-Free (SMF) VRLA batteries	
	Battery Type Sealed Maintenance-Free (SMF), VRLA	
	Battery Rating 12V 120AH	
	Battery Rack Suitable rack for housing batteries with proper insulation and cable connections	
	Cabling Interlink cables with lugs and terminations included	

PASSIVE NETWORKS

	Minimum Technical Specification	Compliance(Y/N)
	Passive Components	
	Make & Model (To be filled by bidder)	
	Supply ,laying, testing & commissioning of 6 Core, Indoor/Outdoor Multi-Tube Gelfilled OFC for Backbone, ECCS Armoured, Fiber Reinforced Plastic Central Strength Member , Tensile Strength Min: 2500N , Crush Resistance Min : 4000N/10CM, Operating Temperature range : -20°C to +70° , Anti-Rodent, Anti-Termite and UV Protected - 1500m	
	Supply ,laying, testing & commissioning of 12 Core, Indoor/Outdoor Multi-Tube Gelfilled OFC for Backbone, ECCS Armoured, Fiber Reinforced Plastic Central Strength Member , Tensile Strength Min: 2500N , Crush Resistance Min: 4000N/10CM, Operating Temperature range : -20°C to +70° , Anti-Rodent, Anti-Termite and UV Protected - 900m	
	Supply ,installation, testing & commissioning of 24 Port Sliding Type for Server Room, OS2 LIU Expandable Upto 72 Fibers, loaded with - 2 x 12F LC Modular Casette, 12 Coloured Pigtails ,LIU Material: Cold Rolled Steel (CRS) ,:Direct OFC Termination, RoHS Compliant - Should include Splice Trays and Glands as required. - 1 Qty	
	Supply ,installation, testing & commissioning of 24 Port Sliding Type OS2 LIU Lockable with Key to prevent unauthorized access to Backbone , Expandable Upto 96 Fibers, Loaded with - 1 x 24F LC Adapter,12 Coloured Pigtails ,LIU Material: Cold Rolled Steel (CRS) ,:Direct OFC Termination, RoHS Compliant - Should include Splice Trays and Glands as required.-1 Qty	
	Single mode 2.5 Mtr Patch cords fiber - 25Qty	

	Cable laying , Termination/Splicing, Fluke/Otdr/Olts Testing including digging and other Services for Outdoor Cabling, 25 Year Performance warranty Certificate	
	ISI PVC/GI Conduits Pipes as per Site Requirements	

DC CIVIL WORKS

	ROOM INTERIOR	**Compliance YES/NO**
	Automatic Modular Types Fire Extinguisher: The datacenter should be equipped with automatic modular fire extinguisher for suppressing any chance of fire. The Extinguishers should be ceiling mounted. Extinguishers should to be placed in the datacenter to get the full coverage of the room. The fire extinguisher should have the following specifications.	
	Filling Hazard-Free Clean Agent Or Seal Fire Foam	
	Capacity 5 Kg	
	Working Pressure 15 Bar	
	Labels Clear Instruction Label & No Maintenance	
	Mounting type Ceiling Mounted	
	Preferred Make: Kanex/Cease fire/Supermex	
	Split AC- 2 Nos 2 Numbers of split AC should be considered for the room cooling. The operation of the AC will be in such a way that only one AC will be working at a time. This should be achieved with the help of a sequential timer. The timer should be capable of switching the AC at equal intervals which can be set by the user. The specification of AC and Timer is as follows.	
	Capacity : 2 Ton	
	Technology : Invertor Type	
	Energy Rating : 5 Star	

	Voltage / Frequency/ Phase : 230V/50Hz/Single	
	Preferred Make : Bluestar/Mitsbushi/Carrier	
	Type : Latest Micro Controller Based Technology	
	Display : LCD Fully Display Digital Model	
	Settings : User Friendly Setting	
	Operation time Both Ac Works Equal time	
	Mounting Type : Wall Mounting	
	Time setting Option : Option to Set Time Programmable 2Hrs,4Hrs,8Hrs,10hrs, 12Hrs	
	Operating Type : Facility of Set AC-1 Manual/ AC-2 manual Facility of Set AC-1 Automatic/ AC-2 Automatic	
	Other feature : Auto Switch over feature for the AC unit at the time of Unit failure or over temperature	
	Fire retardant door for the Data center room entrance: The entrance of the datacenter should be equipped with a fire retardant door. The specifications is as follows. The size should be selected as per the site condition The door should be equipped with a vision panel Infill should be Rockwool/Honeycomb Length: 1 Meter, Depth: 2.1 Meter	
	Rodent repellant for the room The datacenter should be protected from any rodents infestation for this the room should be equipped with rodent repellent system with Very High Frequency Operated System. The system should have the following specifications.	
	Operation Type : VHFO system shall transmit high frequency sound waves (above the 20 KHZ frequency) which are inaudible and harmless to humans but audible and painful to pests thus driving them away.	
	System Type : VHFO system shall consist of one Master Console and Satellites / Transducers.	
	Covering area : Satellite unit shall cover an open floor area of approximately 380 Sqft Satellite unit shall cover Raised floor area of approximately 380 Sqft Satellite unit shall cover false ceiling area of approximately 380 Sqft	
	Sound Wave type : The sound waves propagated shall be linear sine waves with constantly varying frequencies	

	Operating frequency: Above 20 KHz (Variable)	
	Power supply: 230 V AC, 50 H	
	Power output: 800 mill watt per Satellite	
	Room Biometric: Biometric finger print and proximity card readers shall be installed at the entrance of Datacenter, to restrict entry of unauthorized persons and to enforce access Biometric finger print with proximity card readers at the entrance of Datacenter The reader should have certifications like FCC/CE/UL-294 rated 20 Numbers of Proximity Cards compatible with the system shall be provided All the necessary hardware, software with its cabling are to be supplied and installed	
	Thermal Insulation To protect the room from thermal insulation the base floor and ceiling to be fixed with thermal insulation material with following specification Thickness: 13mm Design: One Side aluminum foil faced XLPE Material : Nitrile rubber of Arm Flex/Kflex Area: 67.58 sq.Meter (Length: 21.8 Meter, Breadth : 3.1 Meter)	
	Room light: The Data canter to be equipped with LED light fittings as part of the data center lighting system to remove ambient heat from the data center and reduce energy consumption. Four no's of the Room light should be connected to UPS as an emergency light. Following parameter to be considered while selecting the light	
	Power: 40W LED fitting	
	Size : 2x2 feet	
	Shape : Square	
	Colour : Cool White	
	Size : 2x2 feet	
	Water leak Detection System Water leak detection system shall be installed in the Server Room to detect and raise alarm regarding presence of water. The technical specifications of water leak detection system are given below:	

	The WLD system shall comprise of Cable sensors, Water leak detection modules, I/O modules connected to a control panel The control panel shall have a minimum of 4 zones The WLD system shall have one serial interface The WLD module shall be a single zone type. The module shall be resistant to oxidation and erosion. The module shall have relay output for connection to the controller	
	Fire retardant paint for the room Providing and applying Fire retardant paint of approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint. For all vertical Plain surface Area: 67.58 sq.Meter (Length: 21.8 Meter, Breadth : 3.1 Meter)	
	Raised Floor Providing & fixing steel cementations raised access floor of Finished Floor with antistatic high-pressure laminate and Tile lifter with 3 Prongs for maintenance purpose with following specification Height up to 450mm to 600mm finished in Size 600 x 600 mm x 35 mm Point load 450 kg Uniform distribution load (UDL) 1350 kg per sq. metre Panel Type - M 1000 Under structure- Edge Support Rigid Grid, Wear resistance (g /cm2) - < 0.08, Bottom profile - Hemispherical shape, Pedestal -all steel construction & silver zinc plated Grommets for cable entry. Area: 26.98 Sq.Meter (Length: 7.1 Meter, Breadth : 3.8 Meter)	
	False Ceiling Providing and fixing metal false ceiling with following specification Type: Metal Grid with powder coated 0.5mm thick hot dipped galvanized steel Tiles Size 595 x 595 mm with regular edge (10mm) suitable for 25mm grid. Support: suitable powder coated galvanized steel grid as per manufacturer specification. Area: 26.98 Sq.Meter (Length: 7.1 Meter, Breadth : 3.8 Meter)	

Annexure-7

AGREEMENT

Articles of agreement executed on this the ……… day of …………………………………… ……………………………. between the Registrar, Kannur University (hereinafter referred to as "the University") of the one part and Shri………………………………………… ……………………………………………………. (H.E. name and address of the tenderer) (hereinafter referred to as "the bounden") of the other part.

WHEREAS in response to the Notification No……………….. dated ………………… the bounden has submitted to the University a tender for the ……………………… specification therein subject to the terms and conditions contained in the said tender;

WHEREAS the bounden has also deposited with the University a sum of Rs……………… `…………………………….. as earnest money for execution of an agreement undertaking the due fulfillment of the contract in case his tender is accepted by the University

NOW THESE PRESENTS WITNESS and it is hereby mutually agreed as follows:

1. In case the tender submitted by the bounden is accepted by the University and the contract for ………………………… is awarded to the bounden, the bounden shall within ……………days of acceptance of his tender execute an agreement with the University incorporating all the terms and conditions under which the University accepts his tender.

2. In case the bounden fails to execute the agreement as aforesaid incorporating the terms and conditions governing the contract, the University shall have power and authority to recover from the bounden any loss or damage caused to the University by such breach as may be determined by the University by appropriating the earnest money deposited by the bounden if the earnest money is found to be inadequate the deficit amount may be recovered from the bounden his properties movable and immovable in the manner hereinafter contained.
.

3. All sums found due to the University under or by virtue of this agreement shall be recoverable from the bounden and his properties movable and immovable under the provisions of the Revenue Recovery Act for the time being in force as though such sums are arrears of land revenue and in such other manner as the University may deem fit.

In witness where of Shri……………………………………………………….. (name and designation) for and on behalf of the University and Shri. …………………………………………… Bounden have hereunto set their hands the day and year shown against their respective signatures.

Signed by Shri. ………………………………….. (date) ……………………………………..
In the presence of witnesses:
1. ………………………………………………
2. ………………………………………………

Signed by Shri. ………………………………….. (date) ……………………………………..
In the presence of witnesses:
1. ………………………………………………

2. ………………………………………………