INDIAN INSTITUTE OF TECHNOLOGY
MATERIALS MANAGEMENT DIVISION
Powai, Mumbai 400076

PR No. 1000051464 **RFQ No. 3000014861**

Technical Specifications and Terms & Conditions for Servers, Storage and Switches

The following are the technical specifications for the Servers, Storage and Switches.

S/N	Item Description	Parameters	Total Qty
1	**Server:**		**4**
1	Chassis	2U Rack Mountable	
2	CPU	Two numbers of Processors as below: AMD Epyc/Intel XEON latest generation CPU With at least 64 Cores, 256M L3 Cache, 2.3 GHz base clock, PCIe 4.0x128 per CPU.	
3	Motherboard	2 socket server board (compatible with item 1) with the following characteristics: a) Total 32 DIMM slots. b) Memory is upgradable up to 2TB per CPU with RDIMM. c) Hot-swap support for SATA, SAS, SSD, and NVMe. d) Minimum of 2 numbers of internal usb 3.1 ports. e) At least Primary and Secondary risers installed. f) Minimum 8 PCI-Express 4.0 slots, out of which at least two x16 PCIe slots and at least two x8 PCIe slots. g) Must have an integrated server management system. h) support upto 8 single wide GPUs	
4	Memory	At-least 1024 GB memory DDR5 or higher Registered DIMM (RDIMM) operating at 4800 MT/s	
5	Bus Slots	Server should support upto eight or more PCI-Express 5.0 x16 slots. Additional 2 x 8 or higher PCIe 5.0 slots	
6	BOOT optimized storage	960GB or more SAS 12G Read Intensive HDD * 2 Nos	
7	HDD Bays	Upto 30 SFF SAS/SATA/SSD/NVMe or Upto 16 LFF SAS/SATA/SSD or Upto 36 1T EDSFF or 18 2T EDSFF (FUTURE) (Required min. 4 TB SAS x 4 with Raid 5)	

8	Controller	Server should support one of the below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously: a) Embedded / PCIe based x16 RAID controller with 8GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60. Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe. or b) Embedded / PCIe based x16 RAID controller supporting RAID 0, 1, 5, 6, 10. Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe. or c) Embedded / PCIe based RAID controller with 4GB Flash backed write cache supporting RAID 0, 1, 5, 6, 10, 50, 60 s Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe. d) Above mentioned controller must support following: i) Hardware root of trust and secure encryption and decryption of critical drive data ii) Online Capacity Expansion (OCE) iii) Configurable stripe size up to 1 MB iv) Global and dedicated Hot Spare with Revertible Hot v) Instant Secure Erase vi) Migrate RAID/Stripe Size vii) Modifying Cache Write Policy viii) Move Logical Drive ix) Re-enable Failed Logical Drive or e) PCIe based x32 RAID controller with 8GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60, 1T, 10T supporting up to 32 direct-connected storage devices (SAS/SATA/NVMe). Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 24G SAS, 16G NVMe. Controller must support following: i) Expand Logical Drive ii) Instant Secure Erase iii) Migrate RAID/Stripe Size iv) Modifying Cache Write Policy v) Move Logical Drive vi) Re-enable Failed Logical Drive	

9	Networking features	Server should support below networking cards: a) 1Gb 4-port network adaptors b) 10Gb 2-port Ethernet adaptor c) 10GBaseT 2-port Ethernet adaptor d) 10/25Gb 2-port SFP28 Ethernet adaptor e) 10/25Gb 4-port SFP28 Ethernet adaptor f) 100Gb 2-port QSFP28 Ethernet g) 100Gb 1-port QSFP56 Ethernet h) 100Gb 2-port QSFP56 Ethernet i) 200Gb QSFP56 Ethernet (Required 25G x 4 with trancereceiver)	
10	Interfaces	a) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. b) 1GbE Dedicated management port	
11	Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	
12	Fans	Redundant hot-plug system fans	
13	Industry Standard Compliance	a) ACPI 6.3 Compliant b) PCIe 5.0 Compliant c) WOL Support d) Microsoft® Logo certifications e) PXE Support f) Energy Star g) SMBIOS 3.2 h) UEFI 2.7 i) Redfish API j) IPMI 2.0 k) Secure Digital 4.0 l) Advanced Encryption Standard (AES) m) Triple Data Encryption Standard (3DES) n) SNMP v3 o) TLS 1.2 p) DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) q) Active Directory v1.0 r) ASHRAE A3/A4	

14	System Security	a) UEFI Secure Boot and Secure Start support b) Tamper-free updates - components digitally signed and verified c) Immutable Silicon Root of Trust d) Ability to rollback firmware e) FIPS 140-2 validation f) Secure erase of NAND/User data g) Common Criteria certification h) TPM (Trusted Platform Module) 1.2 option i) Configurable for PCI DSS compliance j) TPM (Trusted Platform Module) 2.0 option k) Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser l) Bezel Locking Kit option m) Support for Commercial National Security Algorithms (CNSA) n) Chassis Intrusion detection option o) Secure Recovery - recover critical firmware to known good state on detection of compromised firmware	
15	Operating Systems and Virtualization Software Support	a) Windows Server. b) Red Hat Enterprise Linux (RHEL) c) SUSE Linux Enterprise Server (SLES) d) VMware ESXi. e) Canonical Ubuntu f) Oracle Linux and Oracle VM g) Citrix	
16	Provisioning	a) Should support tool to provision server using RESTful API to discover and deploy servers at scale b) Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
17	Firmware security	a) For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable b) Should maintain a repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	
18	Embedded Remote Management and firmware security	a) System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication b) Server should have dedicated 1Gbps remote management	

		port c) Server should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware d) Server should support agentless management using the out-of-band remote management port e) The server should support monitoring and recording changes in the server hardware and system configuration. It should assist in diagnosing problems and delivering rapid resolution when system failures occur f) Two factor Authentication g) Local or Directory-based user accounts with Role based access control h) Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality.Should provide support for Java free graphical remote console. i) Should support managing multiple servers as one via j) Group Power Control k) Group Power Capping l) Group Firmware Update m) Group Configuration n) Group Virtual Media and Encrypted Virtual Media o) Group License Activation p) Should support RESTful API integration q) System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support r) Server should have a security dashboard: displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. s) One-button Secure Erase designed to decommission/repurpose servers t) NVMe wear level display u) Workload Performance Advisor - Provides server tuning recommendations to improve server performance	
19	Server Management	a) Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources the user is authorized to view.	

		b) The Dashboard minimum should display a health summary of the following: i. Server Profiles ii. Server Hardware iii. Appliance alerts	
		c) The Systems Management software should provide Role-based access control	
		d) Zero Touch Provisioning (ZTP) using SSDP with remote access	
		e) Management software should support integration with popular virtualization platform management software like Vmware Center & Realize Operations, and Microsoft System Center & Admin Center	
		f) Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
		g) Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalised dashboard to monitor device health, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
		h) Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		i) Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline	
		j) The Server Management Software should be of the same brand as the server supplier.	

20	Cloud Enabled Monitoring and Management	a) Secure connection from customer sites to HPE cloud service b) Unified Identity & Access Management c) Manages and controls servers regardless of physical location d) Subscription-based entitlement e) Efficient Device Onboarding f) Firmware Update Awareness with Intelligent delta-only based updates g) Set Group firmware Baseline and Compliance monitoring and notification h) Group based firmware management that can be scheduled or on-demand i) Remote Site management with low bandwidth/high latency network connectivity j) Role-based access and views for managed customer environments k) GUI and Rest APIs for core features	
21	Installation, commissioning and testing	The charges of installation, commissioning and testing should be done at no additional cost	

2	**Network Fibre Switch:**		**2**
A	**ToR-48 port:**		
1	Form Factor	1U or 2U or Chassis based, Rack mountable Ethernet switch with 1RU form	
2	Architecture	Non-Blocking architecture. Should support Modular Operating system.	
3	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.	
4	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
5	Latest OS version	The switch shall be supplied with the latest OS version.	
6	Feature Availability	All the specified features/parameters/certifications must be available on the Technical Bid opening date. Features /parameters /certifications proposed to be available in near future / on roadmap shall not be considered.	
7	Advance Layer 3 Support	PIM DM/SM/SSM, OSPF, BGP, MBGP, IS-IS should be supported on IPv4 and IP V6 platform,	
8	Data Center Features	Switch should support DCBx Data Center Bridging Exchange Protocol,Priority Flow Control (PFC),Enhanced Transmission Selection (ETS)	
9	Interface Specifications:		

10	Ports	Should support at least 48 x 1Gb/10Gb/25Gb SFP28 ports with min 8 x 40Gb/ 100Gb QSFP28 ports should be available from day 1. Stacking should be supported upto 6 or more switches.	
11	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/make of the switches only.switch should support 10GBASE-T models	
12	Port status display	Each port must have a dedicated LED for status display.	
13	Telecom standard	MTCTE Certified	
B	**Hardware Specifications:**		
1	Switching Capacity	4 Tbps or more	
2	Forwarding rate and latency	1000 Mpps or more, Average Latency: 800 ns or better	
3	MAC Addresses	280K or more,	
4	VLANs (802.1q tagged VLAN)	4000 or more	
5	IPv4 Routes/Entries/Scale	250K or more	
6	IPv6 Routes/Entries/Scale	100K or more	
7	IP Multicast Entries (S,G)	90K or more	
8	Memory and peripheral capacity	16GB RAM or more, 128GB SSD or more	
9	Packet Buffers	32MB or more	
C	**Standards and Protocols**		
1	L2 Loop Protection	IEEE 802.1d Spanning tree protocol	
		802.1s MSTP (Multiple instances of STP)	
		802.1w RSTP (Rapid spanning tree)	
2	Link Aggregation	802.3ad Link Aggregation	
3	QOS Support	At least 8 nos of 802.1p Priority Queues per port and 802.1BA	
4	IP Multicast	IGMP Snooping, MLD v1/v2 support	
5	Port Mirroring / Span port	Port mirroring must be available.	

D	**Routing Features**		
1	Routing Protocols:	The switch shall have hardware based forwarding for IPv4 & IPv6.	
		Following protocols shall be supported with IPv4/IPv6: Static routing, PBR, RIPv2, OSPFv2/v3, BGP	
		The switch shall have Dual stack mode to run both IPv4 & IPv6	
		Generalized Precision Time Protocol (GPTP) , Multiple VLAN Registration Protocol (MVRP) , Multiple Stream Registration Protocol (MSRP).	
2	Router redundancy	Shall support VRRP all versions, for IPV4 and IPV6.	
3	Network Login	MAC and 802.1 X based Login must be available	
4	Port Security	MAC Address based Lockdown and Limited Learning or equivalent	
5	Access Control Lists:	L2/L3/L4 IP based, Source port, destination port, MAC based	
6	AAA (authentication, authorization and accounting)	AAA using RADIUS and TACACS+ must be available	
E	**Management and Monitoring:**		
1	Management	Following in-band management methods shall be available:	
		Secure Web based management (On https)	
		SSH based management (SSH v2).	
2	Out-of-band management	Following out-of-band management methods shall be available:	
		Serial console port	
		Management ethernet port. Dedicated OOB port	
3	Role based Administration	The switch shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges.	
4	Remote Monitoring	Should support RMON, ITU- Y.1731, IEEE 802.1ag	
		Ability of VM-based applications to extract data without disrupting forwarding or control plane traffic.Should support integrated application hosting on the switch.	
5	Network Management	The switch should support SNMP V2c and V3, XML API	
6	Log Management	Syslog shall be supported with multiple syslog destinations.	

7	Flow export	Shall support Netflow/IPFIX/sflow for flow exports.	
8	Time synchronization	Time synchronization using Network time protocol must be available.	
9	Configuration backup & restore	The switch shall have the feature of backing up the configuration & restoring a backed- up configuration. Multiple Configuration files must be supported.	
10	TFTP/FTP upload and download	Config/image upload and download from TFTP/FTP server shall be available.	
F	**Other Requirements:**		
1	Interface cables and other features	Should be supplied with Indian power cords along with all stacking accessories.	
		switch should support VxLAN Tunneling End Point (VTEP),DCBx Data Center Bridging Exchange Protocol,Priority Flow Control (PFC), Enhanced Transmission Selection (ETS), switch should support MPLS as future scalability.	
2	Power Supply & FAN	Hot -swappable modular power and fans,AC and DC power supply options should be supported on the same switch.	
3	Regulatory and Safety	Should support regulatory and safety standards,EMI/EMC standards and Environmental Compliance/standards.	
4	Environmental conditions	The offered equipment must be able to operate in the following environmental conditions	
		Operating temperature: 0°C to 45°C	
		Relative Humidity: 5% to 95% Non-condensing	
5	Electromagnetic interference	The Offered equipment shall have FCC certification.	
6	OEM Criteria and Support	All the switches, the fiber modules should be from the same OEM. The OEM should have R&D center in India. should have a Toll-free number with India TAC center to provide L1/L2/L3 support. Switch should be seamlessly integrated with existing Extreme switches.	
7	Premier license	Perpetual premier license	
8	Installation, commissioning and testing	The charges of installation, commissioning and testing should be done at no additional cost	

3	**Storage:**		**6**
1	Data Availability and All Flash	The offered storage shall be a Unified Enterprise Class Storage Array supporting both Block and File Natively providing enterprise class resiliency & 100% data availability along with all NVMe controllers.	
2	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms & clustering including Windows Server 2019 / 2022, VMware ESX 8.x hypervisor, HPE Morpheus VM essentials hypervisor. Red hat enterprise Linux and SUSE Enterprise Server (SLES) etc.	
3	Capacity & Scalability	a) Offered storage shall be scalable to 184TB raw capacity using 7.68TB NVMe TLC drives. b) Offered Storage array shall be supplied minimum with 33TiB RAID6 Physical Usable Capacity using minimum 8 x 7.68TB TCL NVMe encrypted drives and shall be configured in Raid 6. Vendor shall not use more than 10D+2P while sizing the array. c) Offered Storage shall be able to protect against at-least 2 drives failure simultaneously within a given raid group.	
4	Storage Encryption	a) Vendors shall offer only encrypted drives with appropriate encryption licenses. Vendor shall not offer any controller based or Software based encryption. b) The offered Storage array shall support at-least external key managers from Utimaco ESKM and Thales Cipher Trust Manager. Vendor shall also offer internal Key manager engine for key management.	
5	No. of Controllers	Storage array shall be offered with at least dual controllers, having dual encrypted NVMe boot drives per controller.	
6	Memory and CPU Processing Power	a) Offered Storage array should have at-least 512GB memory across both controllers. b) After a complete power failure, the host acknowledged writes must be restored without the need for battery backed mirrored write caches. c) Offered storage controller shall be based upon at-least PCI 4.0 technology with at-least 8 number of CPU cores.	
7	Architecture & Processing Power	a) Offered storage array shall be true Active-active so that every logical disk is striped across all offered drives and all drives shall be able to contribute the IOs to both controllers simultaneously. b) Offered storage array shall have native virtualization support so that RAID can be carved out from a logical space instead of dedicating separate physical disks for each application.	

8	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of failure configuration including Array Controller card, Cache memory, FAN, Power supply etc.	
9	Host Ports and Back-end Ports	a) The offered Storage array shall have a minimum of 8 x 10Gb SFP+ IP ports and shall be scalable to 16 x 10Gb SFP+ Ports. b) For maximizing the overall performance and NVMe SSD endurance, offered storage array shall support full RAID stripe write to backend disk drives for eliminating the white space issues of NVMe SSD drives.	
10	Global Hot Spare	a) offered Storage Array shall support distributed Global hot Sparing Capacity for offered Disk drives. b) Global hot sparing capacity should be atleast one drive worth of capacity.	
11	Quality of service	a) Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units. b) Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array. c) It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time.	
12	Capacity efficiency	a) Offered storage array shall support inline data efficiency engine (Supporting Thin Zero detect and re-claim, De-duplication and Compression) and shall be enabled by default. b) Vendor shall have flexibility to enable / disable the data efficiency engine at the time of Volume creation. c) Storage subsystem shall be supplied with Thin Provisioning, Thin Re-claim, Snapshot, remote replication, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1 for the supplied capacity of the array.	
13	Firmware Upgrade	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.	

14	Integration - Vmware	The offered storage system shall also be provided with VMware vCenter integration pack so that following day to day operations can be performed directly from the vCenter itself: a. Adding, deleting, expanding the datastore b. Scheduling and restoring datastore and VM snapshot. c. Mounting and applying QOS policy to datastore. d. Creation of VMs. e. RDM migration from VMFS to VVOL f. A common dashboard for providing the number of Storage subsystems, Volumes, Datastore, Virtual Machines, host and Clusters. g. Dashboard shall also provide IOPS, Latency and bandwidth information for Storage subsystem as well as Volumes. h. Dashboard shall also provide top 5 issues which are most recent and based upon the severity of the issue.	
15	Ransomware Detection	a) The offered storage shall have in-built inline data-adaptive ransomware detection engine for Block Volumes. b) Ransomware detection engines shall be completely based upon dynamic calculation of trigger thresholds using in-built training periods and by analysing the write data path instead of using traditional approaches like measuring CPU utilization, change of data rate, data reduction efficiency ratios and data entropy. c) It shall be possible to select a specific set of volumes or group of volumes to be enabled for Ransomware detection for block data. d) It shall also be possible to adjust the balance between sensitivity of detection process and false positives events for effective detection process. Vendor shall provide required configurable parameters or handlers for the same. e) Ransomware detection engine shall be truly intelligent by creating an immediate creation of alert snapshots after noticing the suspicious event. f) It shall also be possible to export the ransomware detection logs to a remote server, such as a SIEM or XDR and Call home support.	

16	Snapshot / Point in time copy, No. of Volumes and tamer-proof protection (Ransomware Protection)	a) The storage array should have support for controller-based snapshots (At-least 1024 copies for a given volume). b) The system must provide the capability to create immutable, read-only snapshots, that cannot be modified. c) The system shall provide the capability to create compliant, read-only snapshots, which makes it impossible to modify or delete the snapshot and its base volume by the user, a system administrator, and the manufacturer. d) The protection period of the above snapshots must be individually configurable between 1 minute and several years. Changing the system clock must not allow the tampering of protection. e) Offered Storage array shall support more than 60000 base volume on the storage array without snapshot and clone.	
17	Remote Replication	a) The storage array should support hardware based data replication at the array controller level across all models of the offered family. b) Offered Storage array shall support both Synchronous and Asynchronous replication across 2 storage arrays natively without using any third party or software based solution. c) Offered storage array shall have capability to create the application consistency group for replication operations. Shall have flexibility to have more than 256 volumes per consistency group. d) Offered storage subsystem shall support incremental replication after resumption from Link Failure situation or during failback operations.	
18	Active / Active Stretch Clustering	a) Offered Storage array shall have capability to provide true Active / Active Replication and Stretch clustering at metro distances for Zero RPO and RTO so that a given volume pair between primary and DR location can have concurrent access to both read and write operations simultaneously. b) Active / Active replication shall be supported for all well-known OS like VMware, Redhat, Windows etc.	
19	Support	Offered storage array shall be configured and support for 5YRS (24 x 7) to be provided.	
20	Installation, commissioning and testing	The charges of installation, commissioning and testing should be done at no additional cost.	

Additional Terms and Conditions:

GENERAL TERMS AND CONDITIONS:

Bidders are advised to read all the clauses mentioned in the tender carefully. Submitting your bid implies that you agree to act as per the terms and conditions mentioned in the tender.

1. The bidder shall bear all the costs during the preparation and submission of the proposal, site visit (if required), etc.
2. The bidders may be requested to come to IIT Bombay and present the solution proposed in their technical bids.
3. IIT Bombay may ask for clarifications, if required, on submitted information in order to evaluate the bid. The bidder should respond to such a clarification request within 2 working days.
4. The bidder has to quote for all the items mentioned in the specification. On failing to do the same, IITB may invalidate the bid and disqualify the bidder.
5. The quoted product must be the most recent or currently supported models, and that they incorporate all recent improvements in design and materials. On failing to do the same, IITB may invalidate the bid and disqualify the bidder.
6. Due to a stringent deadline for incurring the expenditure, IIT Bombay has the right to cancel the PO or charge the penalty if the delivery, installation, and acceptance testing is not completed within the stipulated timeline. Specifically
    a. Delivery should be within 8 weeks of issuing of PO.
    b. Installation, commissioning, and acceptance testing should complete within two weeks of the delivery.
7. The purchase committee will make the final decision on the quantity of purchase after evaluating the proposals. The actual quantity purchased could be lower or higher up to 25% of indicated quantity.
8. At the time of installation, if it is found that some additional hardware or software items are required to meet the operational requirement of the configuration but not included in the OEM's original list of deliverables, the OEM shall supply such items to ensure the completeness of the configuration at no additional cost.
9. Bidders should submit only the necessary documentation related to this tender with a proper index highlighting the required technical specs in the product documentation that matches the tender specs or asked by the purchaser with page numbers. Failure to do the same will invalidate the bid and result in disqualification.
10. Bidder is not allowed to outsource any work mentioned in the scope of work for this tender to a third party.
11. Along with the technical bid, the bidder has to submit the compliance sheet as per the given format in Annexure-X and complete bill of material (BoM). Failure to do the same will invalidate the bid and result in disqualification.
12. The bidder has to submit an Undertaking as acceptance of all terms & conditions along with the technical bid on the company's letterhead as per the format given in Annexure-IX. Failure to do the same will invalidate the bid and result in disqualification.
13. The bidder has to give an undertaking of authenticity along with the technical bid on the company's letterhead as per the format mentioned in Annexure-VII. Failure to do the same will invalidate the bid and result in disqualification.
14. IIT Bombay reserves the right to accept or reject, all the offers if a) Seller/OEM fails to comply with any material term of the contract; b) Seller/OEM fails to deliver the material(s) or any part thereof within the stipulated delivery period and /or fails to replace/ rectify any rejected or defective material(s) promptly; c) Seller/OEM becomes bankrupt or goes into liquidation; d) Seller/OEM has misrepresented to buyer.
15. IIT Bombay also reserves the right to re-issue the tender. The bidders will not have any right to object to such re-issue of tender.

BIDDER ELIGIBILITY CRITERIA:

S.No.	Qualifying Criteria	Mandatory Document proof to be furnished
1.	The bidder should be an Indian Company registered under the Companies Act / Partnership/ LLP and should have presence atleast from the last 3 to 5 years in a similar line of business, i.e., installation, configuration, and commissioning of Enterprise series IT equipment. In case the Bidding Company is the result of a merger/acquisition, at least one of the merging companies should have been in operation for atleast 3 to 5 years as on the date of submission of the bid.	Copy of the Partnership deed/Bye Law/Certificate of Incorporation issued by Registrar of Companies and Memorandum & Articles of Association and full address of the registered office.
2.	The bidder should have supplied at least three orders of Enterprise storage from a reputed OEM like HPE, DELL-EMC, Hitachi, Infortrend or substantially equivalent to State/Central Government/PSUs or any listed corporate company in the last three years.	Purchase order copies along with satisfactory work completion certificate/ Final Acceptance certificate issued by Client. Relevant Purchase Orders received in the last three years.
3.	The bidder should have at least two qualified and experienced Storage Engineers/professionals on its payroll with a minimum experience of 5 years in handling storage devices from reputed brands.	Bio-data of the personnel proposed to be deployed for the project.
4.	Bidder has to be an OEM or partner authorized by OEM for this tender.	Bidders should furnish a letter of authorization (MAF) from OEM for this tender as per the format given in Annexure-V.
5.	The Bidder should have an average annual turnover of ₹ 3 Crores and should be a positive net worth company for the last three financial years.	The Audited Financial Statements (Profit and loss statement, Balance sheet) for the last three years and CA certificate should be furnished/ uploaded.
		Solvency certificate for the value of ₹4 Crores issued by Scheduled Banks to be furnished.
6.	The bidder should be an ISO 9001 certified company at least for the last three years.	The ISO certificate should be enclosed.
7.	Bidders should have an office/branch in the MMR region.	Any government-approved proof should be provided.
8.	The bidder should not have been blacklisted by any department of IIT Bombay, or by any other IIT, or by any state or central government body or organization, or by an autonomous body governed by state or central government during the past 3 years.	Self-declaration should be given on companies' letterhead as per the format provided in the Annexure-VIII

OEM QUALIFICATION CRITERIA:

S.No.	Qualifying Criteria	Mandatory Document proof to be furnished
1.	The OEM should be in the Gartner leader's magic quadrant for all-flash storage, at least for the last three years.	URLs of OEM and Gartner website should be provided or the OEM should submit a self-declaration with all the details mentioned on the company letterhead.
2.	The OEM of quoted products should preferably have its own corporate office or parts warehouse and service centre or RMA depot in the MMR region with fully qualified engineers.	Should submit any government authorized document which will prove this or should provide the OEM website URLs where this information is published.
3.	The OEM should be well equipped and located to honor 4 hours of response time in case of failures.	The OEM should submit a self-declaration with all the details mentioned on the company letterhead.
4.	The OEM should be well established at least from the last 20 years in enterprise series of storage devices and should have a global footprint.	Should submit any government authorized document which will prove the establishment of OEM/Brand and or copy of PO needs to be attached.
5.	The OEM should have a direct presence in India at least from the last 10 years.	Should submit any government authorized document which will prove the establishment of OEM/Brand and or copy of PO needs to be attached.
6.	The OEM should have at least 25 Crores average annual turnover from the last 3 consecutive years.	The Audited Financial Statements (Profit and loss statement, Balance sheet) for the last three years and CA certificate should be furnished/ uploaded OR a duly signed and stamped self-declaration on company letterhead.
7.	The OEM should have their own 24x7 technical support center in India and the technical support resources should be on direct rolls with the OEM.	Should submit any government authorized document which will prove this or should provide the OEM website URLs where this information is published or The OEM should submit a self-declaration with all the details mentioned on his letterhead.
8.	The OEM should not be from a country that shares a land border with India.	Declaration to be submitted as per Annexure-III (Certificate of Compliance)
9.	The OEM should not have been blacklisted by any department of IIT Bombay, or by any other IIT, or by any state or central government body or organization, or by an autonomous body governed by state or central government during the past 5 years.	Self-declaration should be given on company letterhead as per the format provided in the Annexure-VIII

TENDER EVALUATION:
The competent authority will evaluate all the proposals to determine whether these are complete in all respects as specified in the tender document. Evaluation of the proposal shall be done in two stages as

(a) Stage - I (Technical Evaluation):

1. The competent authorities will evaluate the technical bid(s) to determine whether they are meeting the essential eligibility criteria, whether the tenderer has submitted the EMD undertaking, whether any computational errors have been made, whether all the documents have been appropriately signed & stamped, whether all the documents as mentioned / or required to be submitted with technical bid are submitted and whether a bid is complete and generally is in order. There will not be any further technical evaluation in case of incomplete bid, and the bidder will be disqualified.
2. After completing the technical evaluation of proposed switches, and references, the competent authority will qualify bidder(s) who have complied with all the tender specifications.

(b) Stage- II (Financial evaluation):

1. The bidders who have cleared /qualified the technical evaluation only their commercial bid will be opened.
2. The details of the commercial bid opening will be informed to the short-listed bidder(s) at a later date.
3. Bidders should quote a single figure which includes all the cost of the project only in INR. The successful bidder will submit the item-wise bifurcation of the single figure quoted and an item-wise cost breakup within 24 hours from latest email communication.

EVALUATION MATRIX:

In Annexure-X, a set of attributes pertaining to the equipment have been given in the form of a compliance sheet. The purchase committee at IIT Bombay will check the quoted product is matching with the tender specifications. The evaluation will be done based on the documentation, details, and remarks given by the bidder and from the OEM website. The bidder/OEM will be disqualified if the quoted product is not complying with any of the tender specifications.

SCOPE OF WORK:

1. The selected Bidder has to supply the listed items within the stipulated time.
2. The selected Bidder has to deploy, install, configure and test the storage boxes as per specification mentioned in the tender at Computer Centre's Data Centre in accordance with the technical team of Computer Centre IITB. The scope of the work at this phase would include but not restricted to the following:
   A. Site Inspection and Bill of Material Verification.
   B. Rack Mounting and Stacking of the Storage devices.
   C. Structured cabling of OFC, CAT6a/CAT7 and power and any other required cabling and enclosing via flexible pipes wherever necessary with design approval from Technical staff assigned by Computer Centre IIT Bombay.
   D. Labelling for each and every cable and its diagram and documentation.
   E. Storage Power on Self/Burn-In/Stress Test activity –Minimum 48 Hours
   F. Replacement of hardware if any fault is observed.
   G. License installation.
   H. Firmware upgradation.
   I. Management IP and user configuration.
   J. Explanation of the configuration, and providing howtos and best practices on various configurations.

K. Final acceptance from the technical team of the purchaser.

3. The Bidder has to ensure that the proposed equipment/components must not be declared "End of Life" or "End of Support" for the next 6 years from the date of purchase. Suppose the supplied equipment is declared End of Support/End of Life during the warranty period of 5 years. In that case, the bidder/OEM has to replace the equipment having equivalent or higher configurations without any additional cost to the purchaser.
4. The Bidder should have a back to back contract with the OEM so that the purchaser will be able to log a call with the OEM directly for the contract period of 7 years.
5. Single Point of Contact: The selected Bidder shall appoint a single point of contact, with whom IIT Bombay will deal with any activity pertaining to the requirements of this Tender. The Bidder has to award all the necessary authority to this person at its own expense.

Payment Terms:

Servers, Storage and Switches: The payment will be made after successful installation of these equipment.

AMC for 2 years: The payment for AMC will be released bi-annually based on the performance.

WARRANTY & SLA:

1. Each and every component of the supplied equipment, security keys, accessories, and licenses should have an on-site comprehensive 24x7x365 days warranty for 5 years and AMC of 2 years with 4 hours of response time. No parts, accessories, licenses of the systems should be excluded from such warranty.
2. The said warranty will begin from the date of acceptance and sign-off from the technical team of IIT Bombay.
3. The bidder should also provide the cost of an annual maintenance contract (AMC) within the bifurcation document mentioned above which starts at the end of the warranty period with back-to-back, onsite support from the OEM. The quoted price of the AMC should be valid for 24 months after the end of the warranty period. The payment of the AMC will be released bi-annually based on the performance, and if there is any penalty, it will be deducted from the payment of the next half.
4. The bidder will be fully responsible for getting support from OEM in respect of each and every Hardware part, Software, Licenses, and technical support for the equipment mentioned in this tender. In case the bidder fails to provide the support, OEM has to provide technical support for the period mentioned in the contract. The bidder has to attach a confirmation letter from the OEM.
5. The said warranty and the AMC should not be considered violated if the IIT Bombay buys any other compatible supplemental hardware from a third party and installs it in the machines with an intimation to the Bidder.
6. Mean time between failures (MTBF): If during the warranty period, any storage fails four or more occasions and caused downtime in a period of less than three months or six times in a period of less than twelve months, it shall be replaced by equivalent or better configured and robust new storage device by the Bidder/OEM at no additional cost to the IIT Bombay.
7. The Bidder will depute an experienced engineer as and when required to visit the site and assist the staff during the initial configuration and/or during the failure and ensure the system's proper functioning.
8. The Root Cause Analysis (RCA) faced for any issues related to the system should be provided by the OEM within 3 Business Days.
9. If any component supplied by the Bidder/OEM is inoperative, which renders the entire system useless, then it will be treated as system downtime.
10. Any hardware issues should be resolved/rectified within 24 hours. It is the responsibility of Bidder to coordinate with the OEM to provide a replacement.
11. Along with the technical bid, the OEM should submit a letter of commitment for **7 years (60 months of warranty and 24 months of AMC)** from the installation date, with respect to Hardware, Software, and Firmware support. The bid will be rejected if not accompanied by the letter from the OEM.
12. In case of merger/sale of business by the OEM, the above-said warranty, AMC and SLA will be

applicable to the new OEM. If the new OEM does not honor the said warranty, AMC, and SLA, the IIT Bombay reserves the right to debar the bidder or the OEM (whosoever participate in the tender) and reserve the right to take proper legal action. The OEM has to accept this clause in the commitment letter. Failure of the same may result in disqualification of the bid.

PENALTY:

1. Delivery of all equipment should be within 8 weeks from the date of Purchase Order. In the event of any or all equipment(s) not being delivered, installed, tested, and commissioned within a period of 10 weeks from the date of Purchase Order, a penalty of 0.5 percent of the total cost of equipment for each week of the delay will be charged to the bidder. The maximum penalty will be 10%. This amount of penalty so calculated shall be deducted at the time of making final payment after successful installation and commissioning of hardware.
2. Penalty during the warranty period and AMC period:
   The PBG being submitted will be forfeited against the penalty and the bidder will be debarred for the period as per procurement rule.
3. The IIT Bombay reserves the right to publish the information about the unsatisfactory service by the bidder/OEM and action taken by the institute on their website and in the national newspaper (s).

Annexure VII

(To be given on the company's letterhead)

Date:

To,
Dy. Registrar (MM)
Indian Institute of Technology Bombay,
Powai, Mumbai – 400076.

Sub: Undertaking of Authenticity for Hardware and/or Software Supplies Tender Reference No.: _____

Dear Sir,

With reference to the equipment being quoted to you vide our Quotation No: _____ dated _____, we hereby confirm that all the components, parts, assembly, software, etc. used in the equipment to be supplied shall be original new components/parts/assembly/software and of the most recent or current supported models, and that they incorporate all recent improvements in design and materials, only from respective OEMs of the products and that no refurbished / duplicate / second-hand components /parts/assembly/software shall be supplied or shall be used.

1. We also undertake to produce a certificate from the Original Equipment Manufacturers (if required by you) to support the above statement at the time of delivery/installation.
2. We also confirm that in respect of licensed operating systems and other software utilities to be supplied, the same will be procured from authorized sources and provided with an Authorized License Certificate
3. In case of default and the purchaser finds that the above conditions are not complied with, we agree to take back the equipment supplied and return the money paid by you, in full within seven days of intimation of the same by the purchaser, without demur or any reference to a third party and without prejudice to any remedies the purchaser may deem fit.
4. In case of default and we are unable to comply with the above at the time of delivery or during installation, for the IT Hardware / Software already billed, we agree to take back the equipment without demur if already supplied and return the money if any paid to us by you in this regard.
5. We also take full responsibility for both parts & Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI.

Dated this ..... day of 202…

_____

(Signature) (Name) (In the capacity of)

Duly authorised to sign Bid for and on behalf of _____

Annexure-VIII

Self declaration non blacklisting
(To be given on company's letterhead)

Date:

To,
Dy. Registrar (MM)
Indian Institute of Technology Bombay,
Powai, Mumbai – 400076.

Sub: Declaration of Non-Blacklisting.
Tender Reference No.: _____

Dear Sir,

With reference to the equipment being quoted to you vide our Quotation No:____ dated _____ , we hereby declare that neither we nor our Start-up or a parent, subsidiary, or associate Company under direct or indirect common parent is/are presently not placed on any Blacklist or Holiday list by any department of IIT Bombay, or by any other IIT, or by any state or central government body or organization, or by any PSU's, or by an autonomous body governed by state or central government for any kind of fraudulent practice(s)/activity(s).

It is understood that, if this declaration is found to be incorrect, then without prejudice to any other action that may be taken, my/ our security may be forfeited in full, and the tender, if any to the extent accepted, may be canceled.

Dated this ..... day of 202…

_____

(Signature) (Name) (In the capacity of)

Duly authorised to sign Bid for and on behalf of _____

Annexure-IX

TENDER / CONDITIONS ACCEPTANCE LETTER

(To be given on company's letterhead)

Date:

To,
Dy. Registrar (MM)
Indian Institute of Technology Bombay,
Powai, Mumbai – 400076.

Sub: Acceptance of Terms & Conditions of Tender.
Tender Reference No.:

Dear Sir,

1. I/We have downloaded/obtained the tender document(s) for the above-mentioned 'Tender/Work.'
2. I/We hereby certify that I/We have read the entire terms and conditions of the tender documents (including all documents like annexure), schedule(s), etc.,) and I/We shall abide by the terms/conditions/clauses contained therein.
3. The corrigendum(s) issued from time to time by your department/organization has also been taken into consideration while submitting this acceptance letter.
4. I/We hereby unconditionally accept the tender conditions of the above-mentioned tender document(s)/corrigendum(s) in totality/entirely.
5. In case any provisions of this tender are found violated, your department/ organization shall be at liberty to reject this tender/bid, including the forfeiture of the full said earnest money deposit absolutely, and we shall not have any claim/ right against the department in satisfaction of this condition.

Dated this _____ day of 202_

_____

(Signature) (Name) (In the capacity of)

Duly authorised to sign Bid for and on behalf of _____

Annexure-X

COMPLIANCE SHEET

S/N	Item Description	Parameters	Bidder Compliance/ Remark
1	**Server:**		
1	Chassis	2U Rack Mountable	
2	CPU	Two numbers of Processors as below: AMD Epyc/Intel XEON latest generation CPU With at least 64 Cores, 256M L3 Cache, 2.3 GHz base clock, PCIe 4.0x128 per CPU.	
3	Motherboard	2 socket server board (compatible with item 1) with the following characteristics: i) Total 32 DIMM slots. j) Memory is upgradable up to 2TB per CPU with RDIMM. k) Hot-swap support for SATA, SAS, SSD, and NVMe. l) Minimum of 2 numbers of internal usb 3.1 ports. m) At least Primary and Secondary risers installed. n) Minimum 8 PCI-Express 4.0 slots, out of which at least two x16 PCIe slots and at least two x8 PCIe slots. o) Must have an integrated server management system. p) support upto 8 single wide GPUs	
4	Memory	At-least 1024 GB memory DDR5 or higher Registered DIMM (RDIMM) operating at 4800 MT/s	
5	Bus Slots	Server should support upto eight or more PCI-Express 5.0 x16 slots. Additional 2 x 8 or higher PCIe 5.0 slots	
6	BOOT optimized storage	960GB or more SAS 12G Read Intensive HDD * 2 Nos	
7	HDD Bays	Upto 30 SFF SAS/SATA/SSD/NVMe or Upto 16 LFF SAS/SATA/SSD or Upto 36 1T EDSFF or 18 2T EDSFF (FUTURE) (Required min. 4 TB SAS x 4 with Raid 5)	

8	Controller	Server should support one of the below controllers, must support Mixed Mode which combines RAID and HBA mode operation simultaneously: f) Embedded / PCIe based x16 RAID controller with 8GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60. Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe. or g) Embedded / PCIe based x16 RAID controller supporting RAID 0, 1, 5, 6, 10. Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe. or h) Embedded / PCIe based RAID controller with 4GB Flash backed write cache supporting RAID 0, 1, 5, 6, 10, 50, 60 s Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe. i) Above mentioned controller must support following: i) Hardware root of trust and secure encryption and decryption of critical drive data ii) Online Capacity Expansion (OCE) iii) Configurable stripe size up to 1 MB iv) Global and dedicated Hot Spare with Revertible Hot v) Instant Secure Erase vi) Migrate RAID/Stripe Size vii) Modifying Cache Write Policy viii) Move Logical Drive ix) Re-enable Failed Logical Drive or j) PCIe based x32 RAID controller with 8GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60, 1T, 10T supporting up to 32 direct-connected storage devices (SAS/SATA/NVMe). Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 24G SAS, 16G NVMe. Controller must support following: i) Expand Logical Drive ii) Instant Secure Erase iii) Migrate RAID/Stripe Size iv) Modifying Cache Write Policy v) Move Logical Drive vi) Re-enable Failed Logical Drive	

9	Networking features	Server should support below networking cards: j) 1Gb 4-port network adaptors k) 10Gb 2-port Ethernet adaptor l) 10GBaseT 2-port Ethernet adaptor m) 10/25Gb 2-port SFP28 Ethernet adaptor n) 10/25Gb 4-port SFP28 Ethernet adaptor o) 100Gb 2-port QSFP28 Ethernet p) 100Gb 1-port QSFP56 Ethernet q) 100Gb 2-port QSFP56 Ethernet r) 200Gb QSFP56 Ethernet (Required 25G x 4 with trancereceiver)	
10	Interfaces	a) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. b) 1GbE Dedicated management port	
11	Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	
12	Fans	Redundant hot-plug system fans	
13	Industry Standard Compliance	a) ACPI 6.3 Compliant b) PCIe 5.0 Compliant c) WOL Support d) Microsoft® Logo certifications e) PXE Support f) Energy Star g) SMBIOS 3.2 h) UEFI 2.7 i) Redfish API j) IPMI 2.0 k) Secure Digital 4.0 l) Advanced Encryption Standard (AES) m) Triple Data Encryption Standard (3DES) n) SNMP v3 o) TLS 1.2 p) DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) q) Active Directory v1.0 r) ASHRAE A3/A4	

14	System Security	a) UEFI Secure Boot and Secure Start support b) Tamper-free updates - components digitally signed and verified c) Immutable Silicon Root of Trust d) Ability to rollback firmware e) FIPS 140-2 validation f) Secure erase of NAND/User data g) Common Criteria certification h) TPM (Trusted Platform Module) 1.2 option i) Configurable for PCI DSS compliance j) TPM (Trusted Platform Module) 2.0 option k) Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser l) Bezel Locking Kit option m) Support for Commercial National Security Algorithms (CNSA) n) Chassis Intrusion detection option o) Secure Recovery - recover critical firmware to known good state on detection of compromised firmware	
15	Operating Systems and Virtualization Software Support	a) Windows Server. b) Red Hat Enterprise Linux (RHEL) c) SUSE Linux Enterprise Server (SLES) d) VMware ESXi. e) Canonical Ubuntu f) Oracle Linux and Oracle VM g) Citrix	
16	Provisioning	a) Should support tool to provision server using RESTful API to discover and deploy servers at scale b) Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
17	Firmware security	a) For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable b) Should maintain a repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	
18	Embedded Remote Management and firmware security	a) System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication b) Server should have dedicated 1Gbps remote management port c) Server should have storage space earmarked to be used	

		as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware d) Server should support agentless management using the out-of-band remote management port e) The server should support monitoring and recording changes in the server hardware and system configuration. It should assist in diagnosing problems and delivering rapid resolution when system failures occur f) Two factor Authentication g) Local or Directory-based user accounts with Role based access control h) Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. i) Should support managing multiple servers as one via j) Group Power Control k) Group Power Capping l) Group Firmware Update m) Group Configuration n) Group Virtual Media and Encrypted Virtual Media o) Group License Activation p) Should support RESTful API integration q) System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support r) Server should have a security dashboard: displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. s) One-button Secure Erase designed to decommission/repurpose servers t) NVMe wear level display u) Workload Performance Advisor - Provides server tuning recommendations to improve server performance	
19	Server Management	a) Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources the user is authorized to view.	

		b) The Dashboard minimum should display a health summary of the following: i. Server Profiles ii. Server Hardware iii. Appliance alerts	
		c) The Systems Management software should provide Role-based access control	
		d) Zero Touch Provisioning (ZTP) using SSDP with remote access	
		e) Management software should support integration with popular virtualization platform management software like Vmware Center & Realize Operations, and Microsoft System Center & Admin Center	
		f) Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
		g) Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalised dashboard to monitor device health, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
		h) Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		i) Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline	
		j) The Server Management Software should be of the same brand as the server supplier.	

20	Cloud Enabled Monitoring and Management	a) Secure connection from customer sites to HPE cloud service b) Unified Identity & Access Management c) Manages and controls servers regardless of physical location d) Subscription-based entitlement e) Efficient Device Onboarding f) Firmware Update Awareness with Intelligent delta-only based updates g) Set Group firmware Baseline and Compliance monitoring and notification h) Group based firmware management that can be scheduled or on-demand i) Remote Site management with low bandwidth/high latency network connectivity j) Role-based access and views for managed customer environments k) GUI and Rest APIs for core features	
21	Installation, commissioning and testing	The charges of installation, commissioning and testing should be done at no additional cost	

2	**Network Fibre Switch:**		**Bidder Compliance/ Remark**
A	**ToR-48 port:**		
1	Form Factor	1U or 2U or Chassis based, Rack mountable Ethernet switch with 1RU form	
2	Architecture	Non-Blocking architecture. Should support Modular Operating system.	
3	IPV6 Compliance	All Functionalities of Switch shall be IPV4 and IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.	
4	End of sale	OEM End-of-sale declaration shall not have been released for the quoted model at the time of the bid submission.	
5	Latest OS version	The switch shall be supplied with the latest OS version.	
6	Feature Availability	All the specified features/parameters/certifications must be available on the Technical Bid opening date. Features /parameters /certifications proposed to be available in near future / on roadmap shall not be considered.	
7	Advance Layer 3 Support	PIM DM/SM/SSM, OSPF, BGP, MBGP, IS-IS should be supported on IPv4 and IP V6 platform,	
8	Data Center Features	Switch should support DCBx Data Center Bridging Exchange Protocol, Priority Flow Control (PFC), Enhanced Transmission Selection (ETS)	
9	Interface Specifications:		
10	Ports	Should support at least 48 x 1Gb/10Gb/25Gb SFP28 ports with min 8 x 40Gb/ 100Gb QSFP28 ports should be available from day 1. Stacking should be supported upto 6 or more switches.	

11	SFP Transceivers	All the Transceivers/Modules used to connect the Switches should be from the same OEM/make of the switches only. Switch should support 10GBASE-T models	
12	Port status display	Each port must have a dedicated LED for status display.	
13	Telecom standard	MTCTE Certified	
B	**Hardware Specifications:**		
1	Switching Capacity	4 Tbps or more	
2	Forwarding rate and latency	1000 Mpps or more, Average Latency: 800 ns or better	
3	MAC Addresses	280K or more,	
4	VLANs (802.1q tagged VLAN)	4000 or more	
5	IPv4 Routes/Entries/Scale	250K or more	
6	IPv6 Routes/Entries/Scale	100K or more	
7	IP Multicast Entries (S,G)	90K or more	
8	Memory and peripheral capacity	16GB RAM or more, 128GB SSD or more	
9	Packet Buffers	32MB or more	
C	**Standards and Protocols**		
1	L2 Loop Protection	IEEE 802.1d Spanning tree protocol 802.1s MSTP (Multiple instances of STP) 802.1w RSTP (Rapid spanning tree)	
2	Link Aggregation	802.3ad Link Aggregation	
3	QOS Support	At least 8 nos of 802.1p Priority Queues per port and 802.1BA	
4	IP Multicast	IGMP Snooping, MLD v1/v2 support	
5	Port Mirroring / Span port	Port mirroring must be available.	
D	**Routing Features**		
1	Routing Protocols:	The switch shall have hardware based forwarding for IPv4 & IPv6. Following protocols shall be supported with IPv4/IPv6: Static routing, PBR, RIPv2, OSPFv2/v3, BGP The switch shall have Dual stack mode to run both IPv4 & IPv6 Generalized Precision Time Protocol (GPTP) , Multiple VLAN Registration Protocol (MVRP) , Multiple Stream Registration Protocol (MSRP).	
2	Router redundancy	Shall support VRRP all versions, for IPV4 and IPV6.	
3	Network Login	MAC and 802.1 X based Login must be available	
4	Port Security	MAC Address based Lockdown and Limited Learning or equivalent	
5	Access Control Lists:	L2/L3/L4 IP based, Source port, destination port, MAC based	

6	AAA (authentication, authorization and accounting)	AAA using RADIUS and TACACS+ must be available	
E	**Management and Monitoring:**		
1	Management	Following in-band management methods shall be available:	
		Secure Web based management (On https)	
		SSH based management (SSH v2).	
2	Out-of-band management	Following out-of-band management methods shall be available:	
		Serial console port	
		Management ethernet port. Dedicated OOB port	
3	Role based Administration	The switch shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges.	
4	Remote Monitoring	Should support RMON, ITU- Y.1731, IEEE 802.1ag	
		Ability of VM-based applications to extract data without disrupting forwarding or control plane traffic.Should support integrated application hosting on the switch.	
5	Network Management	The switch should support SNMP V2c and V3, XML API	
6	Log Management	Syslog shall be supported with multiple syslog destinations.	
7	Flow export	Shall support Netflow/IPFIX/sflow for flow exports.	
8	Time synchronization	Time synchronization using Network time protocol must be available.	
9	Configuration backup & restore	The switch shall have the feature of backing up the configuration & restoring a backed- up configuration. Multiple Configuration files must be supported.	
10	TFTP/FTP upload and download	Config/image upload and download from TFTP/FTP server shall be available.	
F	**Other Requirements:**		
1	Interface cables and other features	Should be supplied with Indian power cords along with all stacking accessories.	
		switch should support VxLAN Tunneling End Point (VTEP),DCBx Data Center Bridging Exchange Protocol,Priority Flow Control (PFC), Enhanced Transmission Selection (ETS), switch should support MPLS as future scalability.	
2	Power Supply & FAN	Hot -swappable modular power and fans,AC and DC power supply options should be supported on the same switch.	
3	Regulatory and Safety	Should support regulatory and safety standards,EMI/EMC standards and Environmental Compliance/standards.	
4	Environmental conditions	The offered equipment must be able to operate in the following environmental conditions	
		Operating temperature: 0°C to 45°C	

		Relative Humidity: 5% to 95% Non-condensing	
5	Electromagnetic interference	The Offered equipment shall have FCC certification.	
6	OEM Criteria and Support	All the switches, the fiber modules should be from the same OEM. The OEM should have R&D center in India. should have a Toll-free number with India TAC center to provide L1/L2/L3 support. Switch should be seamlessly integrated with existing Extreme switches.	
7	Premier license	Perpetual premier license	
8	Installation, commissioning and testing	The charges of installation, commissioning and testing should be done at no additional cost	

3	**Storage:**		**Bidder Compliance/ Remark**
1	Data Availability and All Flash	The offered storage shall be a Unified Enterprise Class Storage Array supporting both Block and File Natively providing enterprise class resiliency & 100% data availability along with all NVMe controllers.	
2	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms & clustering including Windows Server 2019 / 2022, VMware ESX 8.x hypervisor, HPE Morpheus VM essentials hypervisor. Red hat enterprise Linux and SUSE Enterprise Server (SLES) etc.	
3	Capacity & Scalability	a) Offered storage shall be scalable to 184TB raw capacity using 7.68TB NVMe TLC drives. b) Offered Storage array shall be supplied minimum with 33TiB RAID6 Physical Usable Capacity using minimum 8 x 7.68TB TCL NVMe encrypted drives and shall be configured in Raid 6. Vendor shall not use more than 10D+2P while sizing the array. c) Offered Storage shall be able to protect against at-least 2 drives failure simultaneously within a given raid group.	
4	Storage Encryption	a) Vendors shall offer only encrypted drives with appropriate encryption licenses. Vendor shall not offer any controller based or Software based encryption. b) The offered Storage array shall support at-least external key managers from Utimaco ESKM and Thales Cipher Trust Manager. Vendor shall also offer internal Key manager engine for key management.	
5	No. of Controllers	Storage array shall be offered with at least dual controllers, having dual encrypted NVMe boot drives per controller.	

6	Memory and CPU Processing Power	a) Offered Storage array should have at-least 512GB memory across both controllers. b) After a complete power failure, the host acknowledged writes must be restored without the need for battery backed mirrored write caches. c) Offered storage controller shall be based upon at-least PCI 4.0 technology with at-least 8 number of CPU cores.	
7	Architecture & Processing Power	a) Offered storage array shall be true Active-active so that every logical disk is striped across all offered drives and all drives shall be able to contribute the IOs to both controllers simultaneously. b) Offered storage array shall have native virtualization support so that RAID can be carved out from a logical space instead of dedicating separate physical disks for each application.	
8	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of failure configuration including Array Controller card, Cache memory, FAN, Power supply etc.	
9	Host Ports and Back-end Ports	a) The offered Storage array shall have a minimum of 8 x 10Gb SFP+ IP ports and shall be scalable to 16 x 10Gb SFP+ Ports. b) For maximizing the overall performance and NVMe SSD endurance, offered storage array shall support full RAID stripe write to backend disk drives for eliminating the white space issues of NVMe SSD drives.	
10	Global Hot Spare	a) offered Storage Array shall support distributed Global hot Sparing Capacity for offered Disk drives. b) Global hot sparing capacity should be atleast one drive worth of capacity.	
11	Quality of service	a) Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units. b) Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array. c) It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time.	

12	Capacity efficiency	a) Offered storage array shall support inline data efficiency engine (Supporting Thin Zero detect and re-claim, De-duplication and Compression) and shall be enabled by default. b) Vendor shall have flexibility to enable / disable the data efficiency engine at the time of Volume creation. c) Storage subsystem shall be supplied with Thin Provisioning, Thin Re-claim, Snapshot, remote replication, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1 for the supplied capacity of the array.	
13	Firmware Upgrade	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.	
14	Integration - Vmware	The offered storage system shall also be provided with VMware vCenter integration pack so that following day to day operations can be performed directly from the vCenter itself: a) Adding, deleting, expanding the datastore b) Scheduling and restoring datastore and VM snapshot. c) Mounting and applying QOS policy to datastore. d) Creation of VMs. e) RDM migration from VMFS to VVOL f) A common dashboard for providing the number of Storage subsystems, Volumes, Datastore, Virtual Machines, host and Clusters. g) Dashboard shall also provide IOPS, Latency and bandwidth information for Storage subsystem as well as Volumes. h) Dashboard shall also provide top 5 issues which are most recent and based upon the severity of the issue.	
15	Ransomware Detection	a) The offered storage shall have in-built inline data-adaptive ransomware detection engine for Block Volumes. b) Ransomware detection engines shall be completely based upon dynamic calculation of trigger thresholds using in-built training periods and by analysing the write data path instead of using traditional approaches like measuring CPU utilization, change of data rate, data reduction efficiency ratios and data entropy. c) It shall be possible to select a specific set of volumes or group of volumes to be enabled for Ransomware detection for block data. d) It shall also be possible to adjust the balance between sensitivity of detection process and false positives events for effective detection process. Vendor shall provide required configurable parameters or handlers for the same. e) Ransomware detection engine shall be truly intelligent by creating an immediate creation of alert snapshots after noticing the suspicious event. f) It shall also be possible to export the ransomware detection logs to a remote server, such as a SIEM or	

		XDR and Call home support.	
16	Snapshot / Point in time copy, No. of Volumes and tamer-proof protection (Ransomware Protection)	a) The storage array should have support for controller-based snapshots (At-least 1024 copies for a given volume). b) The system must provide the capability to create immutable, read-only snapshots, that cannot be modified. c) The system shall provide the capability to create compliant, read-only snapshots, which makes it impossible to modify or delete the snapshot and its base volume by the user, a system administrator, and the manufacturer. d) The protection period of the above snapshots must be individually configurable between 1 minute and several years. Changing the system clock must not allow the tampering of protection. e) Offered Storage array shall support more than 60000 base volume on the storage array without snapshot and clone.	
17	Remote Replication	a) The storage array should support hardware based data replication at the array controller level across all models of the offered family. b) Offered Storage array shall support both Synchronous and Asynchronous replication across 2 storage arrays natively without using any third party or software based solution. c) Offered storage array shall have capability to create the application consistency group for replication operations. Shall have flexibility to have more than 256 volumes per consistency group. d) Offered storage subsystem shall support incremental replication after resumption from Link Failure situation or during failback operations.	
18	Active / Active Stretch Clustering	a) Offered Storage array shall have capability to provide true Active / Active Replication and Stretch clustering at metro distances for Zero RPO and RTO so that a given volume pair between primary and DR location can have concurrent access to both read and write operations simultaneously. b) Active / Active replication shall be supported for all well-known OS like VMware, Redhat, Windows etc.	
19	Support	Offered storage array shall be configured and support for 5YRS (24 x 7) to be provided.	
20	Installation, commissioning and testing	The charges of installation, commissioning and testing should be done at no additional cost.	