Tender Guidelines

RFP Reference: UHS/IT/TENDER/003/2026 **10th February 2026**
RFP Closing Date: 26th February 2026 before 12:30 PM.

No.	Description
1	**SERVER AND STORAGE INFRASTRUCTURE UPGRADE**

University Hospital Sharjah. **(UHS)** Management has decided to invite vendors for a Request for Proposal (RFP). You, as a vendor are requested to participate in the RFP process by submitting your offer to provide the services as described in this document.

The RFP should comply with the following terms & conditions:

1. The proposal shall be clear, informative & include as per the requirement described in the RFP.
2. The financial offer should be on your company letterhead containing the authorized signatory and must be sent to the attention of the Director of Finance, **University Hospital Sharjah, PO Box 72772, Sharjah in a sealed document**.

3. The price quoted is as mentioned in the technical requirement listed below (RFP) to UHS.

4. All deliveries should be made for the ordered quantity in full, without partial shipments, to our Main Warehouse, located in UHS vicinity or as specified on the Purchase Order/ Contract. Failure to comply with the agreed delivery schedule or any shortfall in quantity may result in penalties or contract termination, as per the Purchase Agreement Terms and Conditions.

5. As a part of the RFP document, the Vendors are requested to provide their valid Trade License, Name, and Designation of the Managing Director/General Manager/Sr. Manager having the authority to bind their company for the business relationship. Also, the vendors are required the provide licenses, certificate confirming that the vendor is legalized to operate the proposed business activity. As well as the following documents:

    a) Valid Trade License

    b) Updated Company Profile

    c) Tax Registration Certificate (TRN)

    d) Full Company Address & Contact Details

    e) Memorandum of Association (MOA) and Power of Attorney (POA) for authorized signatory (if applicable)

    f) An official Authorization Letter/Agency Certificate, confirming the vendor's legal authorization to supply the specified items on behalf of the manufacturer or principal company.

    g) Any additional approvals or compliance documents mandated by government authorities for the supply of the specified equipment.

    h) Non-Liability Letter and Legal Clearance Confirmation.

    i) Insurance Policies (General Liability, Professional Indemnity, etc.).

j) Declaration of No Ongoing Legal Disputes.

k) Vendor Code of Conduct Acknowledgment.

6. Standard payment terms are 90 days from the date of completion of delivery of supplies/ services or as specifically agreed in purchase contract/ agreement.

7. Any delays or non-conformance may result in the termination of Services agreement and/or imposition of penalty for delayed services as per the Services Agreement terms and conditions. **A performance bond may be required to ensure commitment to the agreed timelines and quality standards**.

8. The proposed services shall be evaluated & approved by UHS's before confirmation. Once the agreement is signed off, the services will have to correspond to the required services with specific time-frame, and as originally proposed, agreed and any deviations shall be considered a breach of service contract/agreement.

9. The specified brand and manufacturer must remain unchanged throughout the contract period unless otherwise approved by UHS in writing.

10. UHS will be constantly evaluating the compliance of Contract/Agreement Terms and consistency in performance of the services throughout the duration of the agreement.

11. Vendors are required to submit regular progress reports at agreed intervals detailing progress, challenges, and actions to address any delays or issues. Should Vendors not meet the requirements of UHS, UHS reserves the right to terminate the agreement if the vendor is not able to rectify during the time allotted by UHS's representative.

12. Vendor Contact details (landline, mobile, emails) of the authorized representatives should be mentioned.

13. **Tenders should be submitted in two sealed envelopes and submitted to the Administration Office Finance Department- UHS:**

    a. **The Technical Specification details (PLEASE DO NOT INDICATE ANY FINANCIAL VALUE IN THIS).** If requested for additional clarifications and details these need to be submitted to **(Administration Office Finance Department- UHS).**

        i. The offer should must conform to the RFP Document as per the attachment.
        ii. The offer shall be submitted (hard copy and soft copy saved in USB).
        iii. Reference Project/Hospital where similar work was performed.

    b. **The Financial Offer** addressed to UHS's Director of Finance, with **tender reference**.

    All above documents should be submitted before the tender expiry date, all documents submitted after the expiry date will not be accepted.

14. UHS shall have no obligation to accept any tender proposal submitted by any vendor. UHS may at its sole discretion and without providing any reason, accept or reject any or all

proposals, in whole or in party. Such rejection shall not give rise to any claim, liability, or cause of action of any king by the vendor against UHS.

15. Submission of a tender proposal shall not create and agreement, legal or other relationship between the vendor and UHS. No vendor shall acquire any rights, interests, or claims against UHS by submitting a proposal, participating in the tender process or relying on any communications related to the tender.
16. In the event UHS accepts a tender proposal of a vendor, the parties agree any such tender award will be subject to a Services Agreement and separate agreement outlining the specific terms and conditions of the project and services agreed.
17. All costs, expenses or losses incurred by the vendor in connection with the preparation, submission of presentation of its proposal shall be borne sole by the vendor. UHS shall have no liability, under any circumstances to reimburse, compensate or indemnify the vendor whether in part or in whole for such costs or expenses.
18. The vendors acknowledge and agree that they have not relied on any statement, representation, warranty, or promise made by UHS, whether oral or written, in preparing their tender proposal and all decisions and judgements regarding the submission of their proposal are made at their own discretion and risk.
19. UHS may at any time without liability, amend, suspend, or withdraw the tender invitation in whole or in part. UHS may also request additional information, clarifications or documents from any vendor and may reject any proposal that is incomplete, unclear or does not comply with the tender requirements as outlined in this document.
20. Quality, Price, and sale services are combined parameters for tender evaluation. Once a vendor has been selected, a negotiation period will follow to allow both parties to review the agreement terms thoroughly. This will ensure that all deliverables, KPIs, and expectations are clearly outlined before the final agreement is signed.
21. . Vendors must submit a risk management plan, identifying potential risks to the project, such as security and confidentiality breaches, system failures, and disruptions to delivery schedules. Vendors should outline how they intend to address these risks, including their disaster recovery and business continuity plans.
22. Vendors are encouraged to adhere to ethical practices and sustainability standards in their operations. This includes providing energy-efficient equipment and adopting environmentally friendly practices in their supply chain and delivery.
23. The Vendor, its employees, its subsidiaries, and everyone who has a direct or indirect relationship with implementing and securing the works and Services included within the scope of this tender, shall be obligated to inform UHS and disclose in writing any case of conflict of interest or any private interest that has arisen, will arise, or may arise. For any transaction related to the activities of UHS, in accordance with UHS policies.
24. The vendor, its employees, and subsidiaries shall be obligated to maintain confidentiality of any data, drawings, documents, or information related to the tender - written or oral. Vendors must ensure that any data shared is protected by encryption standards and secure transfer protocols. Additionally, vendors are required to notify UHS of any data breaches immediately. Compliance with relevant data privacy regulations (e.g., GDPR, UAE Data Protection Law) is mandatory. This includes all dealings, affairs, or secrets related to UHS they may have encountered during the tender process. Vendors shall not be allowed to disclose any information related to the tender through any media outlet without obtaining prior written approval from UHS.

25. The copyright, rights and ownership of any documents, materials and information submitted by UHS within this tender is owned by UHS, and accordingly, these documents and materials

may not be copied, in whole or in part, or reproduced, distributed, made available to any third party, or used without obtaining prior written approval from UHS. If the vendor develops any custom software or systems for UHS as part of this tender, UHS will retain ownership of the intellectual property or have clear licensing terms for its continued use. All documents submitted by the UHS in connection with the request for proposals shall be returned upon request without any copies being retained by the bidder or any other person.

26. The vendors shall indemnify, defend and hold harmless UHS, its officers, employees and agents from and against any and all claims, liabilities, losses, damage costs, or expenses arising out of or in connection with:

    a. the vendors participation in the tender process
    b. any errors, omissions, misrepresentations or inaccuracies in the proposal
    c. any breach of the vendors' obligations under this tender invitation

27. To the maximum extent permitted by law, UHS expressly excludes any liability for:
    a. Any direct, indirect, incidental, consequential or special losses
    b. Loss of profits, revenue, goodwill or business opportunities
    c. Any claims by third parties arising from a vendor's proposal
    d. Any loss or damage caused by errors, omissions or delays in the tender process
28. This tender invitation and all matters relating to it shall be governed by any construed in accordance with the laws of the United Arab Emirates. The competent courts of Sharjah, United Arab Emirates shall have exclusive jurisdiction over any disputes arising from or in connection with this tender.
29. This document and clauses therein constitute the entire understanding between UHS and any vendor regarding liability, proposal submission, and the tender process. No other communication, agreement or understanding, whether oral or written shall be deemed to modify, supersede, or expand these clauses.

University Hospital Sharjah

Request for Proposal (RFP)

Server and Storage Infrastructure Upgrade

1. Introduction

University Hospital Sharjah invites qualified and experienced vendors to submit proposals for the supply, installation, configuration, and support of a **Server and Storage Infrastructure Upgrade**. The objective is to modernize the existing data center environment to improve performance, availability, scalability, security, and manageability while supporting future growth.

2. Background & Current Environment

- Existing on-premises data center supporting mission-critical applications
- A mix of physical and virtual workloads deployed on a converged infrastructure across the Main and DR sites.
- There is a dedicated dark fiber between Main Site and the DR with a round-trip latency <1millisecond.
- Current challenges may include capacity constraints, aging hardware, performance bottlenecks.

3. Scope of Work and Detailed Technical Requirements

- The solution is primarily based on converged infrastructure (CI); however, vendors may propose a hyper-converged infrastructure (HCI) solution (e.g., Nutanix) that fully meets the RFP scope. Converged infrastructure is preferred, but HCI solutions will be evaluated if they provide equivalent or superior capabilities.
- The current backup and recovery platform is Veeam. While continuing with Veeam is preferred, vendors may propose alternative solutions that enhance or optimize backup and recovery performance, reliability, or efficiency.

The selected vendor shall be responsible for, but not limited to, the following:

3.1 Server Infrastructure

Virtualization (VMware ESXi) Infrastructure Servers (Qty:8):

- Each server shall be equipped with two (2) AMD EPYC 9275F processors, each with 24 cores.
- Each server shall be configured with a minimum of 1.5 TB RAM using high-speed memory modules.
- Each server shall include two (2) M.2 NVMe SSDs configured in RAID-1 for VMware ESXi deployment.
- Each server shall have two (2) dual-port 10/25 Gbps network interface cards, populated with appropriate transceiver modules.
- Each server shall have two (2) dual-port 32 Gbps HBA cards, populated with appropriate transceiver modules.
- Each server shall be supplied with fully redundant power supplies.

- Each server shall be provided with two (2) power extension cables (C13 to C14).
- The proposed servers shall be fully compatible with and officially supported by latest VMware for ESXi.

SAP HANA Servers (TDI compliant infrastructure) Qty:3:

- Three (3) servers shall be proposed for SAP HANA workloads.
- Two (2) servers shall be equipped with two (2) Intel Xeon Gold processors, each with 28 cores and high clock speed, and one (1) server shall be equipped with (2) Intel Xeon Gold processors, each with 20 cores and high clock speed, certified for SAP HANA.
- Two (2) servers shall be configured with a minimum of 1,152 GB RAM, and one (1) server shall be configured with a minimum of 576 GB RAM, as per SAP HANA memory sizing requirements.
- Each server shall include two (2) 512 GB NVMe SSDs configured in RAID-1.
- Each server shall be equipped with two (2) dual-port 10/25 Gbps network interface cards, populated with appropriate transceiver modules.
- Each server shall include two (2) dual-port 32 Gbps HBA cards, populated with appropriate transceiver modules.
- Each server shall be supplied with fully redundant power supplies.
- Each server shall be provided with two (2) power extension cables (C13 to C14).
- Each server shall support the deployment of SUSE Linux Enterprise Server for SAP Applications, versions 15 and 16 (latest editions).

Backup Server:

- Server shall be equipped with two (2) AMD EPYC 9175F processors, each with 16 cores.
- Server shall be configured with a minimum of 128 GB RAM using high-speed memory modules.
- The server shall be equipped with two (2) 512 GB NVMe SSDs configured in RAID-1 for the operating system. Additionally, the server shall include five (5) 7.68 TB enterprise-grade SSDs configured in RAID-5 (4+1 spare) dedicated for backup storage. All SSDs shall meet enterprise endurance specifications and provide a minimum operational service life of five (5) years.
- Server shall have two (2) dual-port 10/25 Gbps network interface cards, populated with appropriate transceiver modules.
- Server shall have two (2) dual-port 32 Gbps HBA cards, populated with appropriate transceiver modules.
- Server shall be supplied with fully redundant power supplies.
- Server shall be provided with two (2) power extension cables (C13 to C14).

3.2 Storage Infrastructure

The purpose of this RFP is to procure an **enterprise-grade datacenter storage solution** capable of supporting **virtualized, physical, and mission-critical workloads**. The solution must provide **high availability, scalability, performance, and security** to meet current and future business requirements.

- Two (2) all-flash, end-to-end NVMe/FC unified storage systems supporting both block and file protocols (FC/iSCSI/NVMe for block, NFS/SMB for file), each with a dual-controller architecture and populated with enterprise-grade NVMe SSDs rated for a minimum five (5)-year endurance, shall be deployed in an active-active stretched cluster configuration across

the Main Site and the Disaster Recovery (DR) Site, and Self-Encrypting Drive (SED) technology shall ensure that data at rest is always protected.

- The stretched cluster shall provide active-active high availability, ensuring continuous operations and minimizing downtime.
- The storage solution shall provide true active-active LUN access across the stretched cluster, enabling concurrent read/write I/O to the same LUN from hosts at both the Main Site and DR Site with automatic path management and no performance degradation during site or controller failover.
- The solution shall ensure zero RPO (Recovery Point Objective) and zero RTO (Recovery Time Objective) for all critical workloads through active-active high availability.
- The storage platform shall provide always-on data-at-rest encryption, inline compression, and inline deduplication, enabled by default, with no impact on performance, availability, or data accessibility.
- A dedicated existing dark fiber link shall connect the Main Site and DR site, providing a round-trip latency of less than 1 millisecond to support synchronous replication and high-speed data access.
- The storage solution shall provide space-efficient, immutable, read-write snapshots with consistency group support, ensuring application-consistent point-in-time recovery across multiple volumes, fully supported in active-active stretched cluster configurations.
- The solution shall provide policy-based automated snapshot scheduling for Virtual Machines (VMs), Windows and Linux file servers, Microsoft Exchange, Microsoft SQL Server, SAP HANA, and Oracle databases. Snapshots shall support application-consistent and crash-consistent options with configurable frequency (hourly, daily, weekly) and retention policies as per business requirements. The system shall enable granular restore capabilities including full VM recovery, individual files and folders, mailboxes and emails (Exchange), databases and point-in-time recovery (SQL, SAP HANA, Oracle), and transaction/log management where applicable. The solution shall support centralized management, snapshot replication (if required), encryption at rest and in transit, and successful testing of full and granular restore procedures.
- The storage solution shall provide a centralized management and monitoring platform with role-based access control, real-time and historical performance analytics, and proactive alerting with integration to email, SNMP, and third-party monitoring systems, ensuring full visibility across all nodes in an active-active stretched cluster configuration.
- The storage solution shall support the creation of multiple independent logical storage arrays or pools on the same physical infrastructure, each with isolated management, performance, and data protection policies, fully supported in active-active stretched cluster deployments.
- The storage platform shall provide granular, volume-level QoS with configurable minimum, maximum, and burst IOPS/throughput, including monitoring, alerting, and reporting, ensuring strict performance isolation across all volumes in active-active stretched cluster configurations.
- The storage platform shall provide automated thin provisioning with dynamic, real-time volume expansion and contraction, integrated with monitoring, alerting, and reporting,

ensuring optimal utilization across all volumes in active-active stretched cluster configurations, with no service disruption.

- The proposed solution shall be capable of delivering sub-1 millisecond latency while sustaining a minimum **throughput of 2 GBps** and up to 500,000 IOPS, based on an **8 KB block size**, with **deduplication and compression** enabled and a guaranteed **3:1 data reduction ratio**. The workload profile shall consist of **65% reads and 35% writes**, applicable to both **sequential and random I/O** patterns, ensuring consistent performance across **mixed workloads**. In addition, the storage media shall provide enterprise-class endurance with a minimum operational lifespan of five (5) years, suitable for sustained, high-intensity workloads.

Storage Requirements (Usable Capacity):

Workload Type	**Current Usable Capacity**
VMware (Windows, Red Hat, SUSE)	13 TB
Databases (SQL, IRIS, Oracle)	42 TB
NAS (SMB, NFS)	8 TB
Total Existing	**63 TB**
Required Usable Capacity (3-year horizon)	**100 TB**

Notes:

- Deduplication ratio: 2.5:1 from the exiting storage
- RAID overhead: Dual parity
- Usable capacity calculated after compression, deduplication, and RAID
- Vendors must ensure that the recommended disk size supports the required IOPS, throughput, deduplication/compression efficiency, RAID overhead, power/cooling, and total cost of ownership.

3.3 Backup Appliance

- The solution shall provide **immutable and tamper-resistant backups** that cannot be altered, deleted, or encrypted by ransomware or malicious insiders.
- Support **air-gapped or logical isolation** mechanisms to protect backup data from production network compromise.
- Include **built-in ransomware detection** and anomaly analysis to identify suspicious behavior, abnormal encryption patterns, or unauthorized changes.
- Support **role-based access control (RBAC)**, multi-factor authentication (MFA), and audit logging for all administrative activities.
- The appliance shall support high-throughput backup and restore operations without performance degradation, scalable capacity for future growth, and global deduplication and compression to optimize storage utilization.
- The solution shall use a scale-out architecture to enable cost-effective growth, prevent product obsolescence, and maintain a consistent backup window as data volumes increase.
- The solution shall provide a robust, tiered backup storage architecture and support offsite tape copies for long-term retention.
- The storage system shall use RAID 6 to protect against up to two simultaneous disk failures, and Self-Encrypting Drive (SED) technology shall ensure that data at rest is always protected.

- The solution shall fully support the Veeam data platform as well as all other market-leading backup software, ensuring seamless integration and compatibility for backup, replication, and restore operations.
- The solution shall provide a centralized management console for monitoring, reporting, and administration, support automated backup policies with scheduling, retention, and lifecycle management, and include alerting and reporting for backup status, failures, security events, and capacity utilization.

Backup Appliance Requirements:

	Day 1 (Data)	Capacity	Progressive Synthetic Backup	Retention
VM Backup	27	TB	Weekly	180 Days
DB Backup	28	TB	Daily	
DB Trans Logs	200	GB	10 minutes	
Exchange On-prem	11.25	TB	Daily	
File Server	1.25	TB	Daily	
DMS Files	2.2	TB	Daily	
AD Backup	140	GB	Daily	
VDI USER DATA	10	TB	Daily	
Total of First Backup	80	TB		
Data Growth per year (25%)	20	TB		
Back Appliance Total Capacity for 3 years including 180 Days retention	140	TB		
Backup Appliance Total Capacity for 3 years including 180 Days retention after Deduplication and Compression	TBD			
Cache Layer capacity	TBD			

3.4 Softwares (Support and Subscription)

VMware Virtualization:

- The proposed solution shall be fully compatible with the VMware ESXi hypervisor infrastructure.
- UHS has an existing VMware Cloud Foundation (VCF) subscription covering 416 cores with production support, valid until 29 April 2027. As per the new requirements, the VCF subscription shall be limited to 384 cores with the same level of production support. The proposed solution shall utilize the existing VCF licenses with the new servers until the current subscription expiry. The VCF renewal subscription shall be considered from the date of the existing subscription expiry, and a further three (3) years of VCF subscription with production support for 384 cores shall be included in the new proposal.

Note: **VMware SITE ID - 15908074**

SUSE Linux Enterprise Server for SAP Applications:

- UHS has an existing Qty: 6 SUSE Linux Enterprise Server for SAP Applications with Live Patching, x86-64, 1-2 Sockets with Unlimited Virtual Machines, L3-Priority Subscription valid until 31 July 2027.
- UHS currently has six (6) SUSE Linux Enterprise Server for SAP Applications subscriptions with Live Patching, valid until 31 July 2027. The new solution shall continue to use these six subscriptions with production support from SUSE until they expire. After that, the proposal shall include a renewal for three (3) more years with production support from SuSe for the same six (6) subscriptions.

Note: **Organization ID: UHS A191555**

Red Hat Enterprise Linux Server:

- UHS has an existing Qty: 13 Red Hat Enterprise Linux Server, Premium (Physical or Virtual Nodes, L3 Only) Subscription valid until 31 July 2027.
- UHS currently has thirteen (13) Red Hat Enterprise Linux Server subscriptions, valid until 31 July 2027. The new solution shall continue to use these thirteen (13) subscriptions with production support from Redhat until they expire. After that, the proposal shall include a renewal for three (3) more years with production support from Redhat for the same thirteen (13) subscriptions.

Note: Account number: 1334733, Org ID: 6100343

Veeam Backup:

- UHS currently has seventy (70) instances of Veeam Data Platform Advanced Universal Subscription License, including Enterprise Plus Edition features, valid until 10 May 2027.
- The new solution shall continue to use these seventy (70) subscriptions with production support from Veeam until they expire. After that, the proposal shall include a renewal for seventy (70) subscriptions, plus an additional eighty (80) subscriptions, for three (3) years with production support from Veeam.

Note: ID: 03352717

3.5 SAN Switches

- The solution shall include four (4) x 24 port 32 Gbps Fibre Channel SAN switches (two at Main Site, two at DR Site) compatible with existing and new storage and servers for mission-critical environments.
- Each SAN switch shall have a minimum of twenty (20) Fibre Channel (FC) ports populated and fully licensed.
- The SAN switches shall support NVMe over Fibre Channel (NVMe/FC).
- The solution shall feature redundant hot-swappable power supplies and cooling fans.
- The SAN switches shall provide a centralized management interface (GUI and CLI), support SNMP, syslog, and alerting, implement role-based access control (RBAC), and allow firmware upgrades without service disruption, where supported.
- The SAN switches shall have certified compatibility with leading enterprise storage and server vendors.

3.6 TOR Switches

- The solution shall include four (4) enterprise-grade 48-port Top-of-Rack (ToR) switches—two (2) at the Main Site and two (2) at the DR Site. The switches shall support high-performance 10/25 Gbps connectivity with stacking capabilities and be suitable for mission-critical environments.

- Each ToR switch shall have a minimum of 48 ports supporting 10/25 Gbps SFP28, with at least 24 ports populated with 25 Gbps SFP28 optics and a minimum of 10 ports populated with 1 Gbps SFP optics. The switches shall support auto-negotiation for 10 Gbps and 25 Gbps speeds.
- Each ToR switch shall support dual-port stacking per switch, with stacking bandwidth sufficient to handle full line-rate traffic. The stack shall support active-active operation, provide a single logical management interface for all stacked switches, and ensure no single point of failure within the stack.
- Each ToR switch shall have redundant hot-swappable power supplies and cooling fans, and a rack-mountable form factor suitable for Top-of-Rack deployment.
- Each ToR switch shall provide centralized management via GUI and CLI, support SNMP, Syslog, and NetFlow/sFlow, implement role-based access control (RBAC), and enable secure management using SSH, HTTPS, and TACACS+/RADIUS.
- Each switch shall feature non-blocking, wire-speed switching architecture, low latency suitable for data center workloads, and Layer 2/Layer 3 features including VLANs, trunking, Link Aggregation (LACP), Spanning Tree Protocol (RSTP/MSTP).

3.7 Rack, Power supplies and accessories

- The solution shall include two (2) server standard branded racks, four (4) 24-port managed 32 A PDUs (2 per rack) suitable for the proposed equipment, and all necessary accessories. The racks shall be 42U, provide proper cooling, cable management, and grounding. All required network and power cables shall be included, with additional spare cables for future use.

3.8 Installation & Implementation

Hardware Mounting:

- All proposed servers, storage systems, ToR switches, and SAN switches shall be rack-mounted and installed in standard 42U racks. All devices shall have dual power supplies connected to separate PDUs for redundancy. All required network, SAN, and power cables shall be supplied, properly labeled, and neatly terminated. Servers shall be redundantly connected to ToR switches for LAN connectivity and to SAN switches for storage connectivity. The overall cabling design shall ensure organized routing, high availability, and no single point of failure.
- The vendor shall ensure that all hardware components, including servers, storage systems, SAN switches, and networking devices, are updated and upgraded to the latest manufacturer-recommended firmware and software versions prior to deployment.

SAN Switches:

The vendor shall provide a complete scope of work for the installation and commissioning of SAN switches to support the storage and compute environment. The scope shall include, but not be limited to:

- The vendor shall install and configure SAN switches, including **rack-mounting, power connections, fiber cabling and SFPs, initial IP and VLAN/Fabric setup, zoning and access control, firmware/software upgrades to the latest versions, and end-to-end testing** for performance, redundancy, and failover.

ToR Switches:

The vendor shall provide full installation and configuration of Top-of-Rack (TOR) switches, including:

- The vendor shall install and configure TOR switches, including **rack-mounting, power connections, cabling, initial IP/VLAN setup, firmware/software upgrades, security configuration, and end-to-end testing**.
- The vendor shall configure TOR switches with **stacking, uplinks to aggregation/core switches, VLANs, and link aggregation (LACP) as per design**, ensuring redundancy, high availability, and proper network segmentation. (Note: Core switch-side configuration will be handled by UHS.)

Storage (Active-Active Stretch Cluster):

- The vendor shall install and configure the storage system in an Active-Active stretch cluster across two datacenters, including hardware deployment, cabling, power, network connectivity, synchronous replication setup, cluster failover/failback configuration, integration with VMware hosts, validation of performance and redundancy, and documentation.
- The vendor shall configure the storage system including controllers, disk groups, pools, volumes, datastores, RAID, tiering, deduplication/compression, network connectivity, storage-to-host mapping, zoning, multipathing, HA, and failover.
- The vendor shall deploy and configure **datacenter storage optimized according to UHS requirements and industry best practices**, ensuring performance, availability, scalability, and reliability.
- The vendor shall create storage volumes as per UHS capacity requirements and configure NFS shares for Linux/Unix and SMB shares for Windows. Access permissions shall be applied via Active Directory (AD) / LDAP.
- The vendor should install and configure the **centralized storage monitoring and analytics server** to monitor **health, performance, capacity utilization, and faults in real-time**, generate **alerts for threshold breaches or failures**, and provide **performance analytics, trending reports, and capacity forecasting**.
- The vendor shall configure policy-based automated and immutable snapshot scheduling for Virtual Machines (VMs), Windows and Linux file servers, Microsoft Exchange, Microsoft SQL Server, SAP HANA, and Oracle databases. Snapshots shall support application-consistent and crash-consistent options with configurable frequency (hourly, daily, weekly) and retention policies as per business requirements. The system shall enable granular restore capabilities including full VM recovery, individual files and folders, mailboxes and emails (Exchange), databases and point-in-time recovery (SQL, SAP HANA, Oracle), and transaction/log management where applicable. The solution shall support centralized management, snapshot replication (if required), encryption at rest and in transit, and successful testing of full and granular restore procedures.

VMware components Deployment:

- Install and configure latest ESXi hypervisors on the physical servers. Deploy vCenter Server for centralized management of ESXi hosts, clusters, and virtual machines. Configure roles, permissions, and SSO as required. Cluster Configuration: Set up clusters, enable DRS, HA, and vMotion for workload mobility and high availability.
- Deploy NSX components including NSX Manager, NSX Controllers, and Edge nodes. Create logical switches, routers, and distributed firewalls to segment and secure the network. Implement micro-segmentation policies to protect workloads at the VM level. Scope is limited to around 10 virtual machines.
- Deploy SDDC Manager to orchestrate and automate the lifecycle of the VCF environment.
- Deploy VMware Aria Operations for performance monitoring, capacity management, and predictive analytics. Enable centralized log management and analytics for troubleshooting and compliance.

- The vendor shall configure network connectivity from VMware servers to TOR switches, including NIC mapping, cabling, link aggregation (LACP) where applicable, VLAN assignments, and validation of connectivity and redundancy to ensure high availability and proper integration with the network design.

Backup:

- The vendor shall deploy Veeam Data Platform Advanced on the new backup server and migrate the existing Veeam configuration database to the new server to retain all existing backup jobs, configurations, and restore points. The migration shall be completed without data loss.
- The vendor shall integrate the backup appliance with Veeam Backup & Replication, configure it as a backup repository, and ensure successful backup and restore operations.
- The backup and restore configuration shall cover up to 10 VMs, physical hosts, or applications.
- The vendor shall configure Veeam SureBackup to automatically test VM restores in an isolated environment, verifying backup integrity and ensuring application availability.
- Configure Veeam tape library repository, set up media pools and jobs, test backups, and provide documentation.

The vendor shall supply, deploy, and configure the Backup Appliance, ensuring it is fully integrated with the existing IT backup infrastructure. The configuration shall include, but is not limited to, the following:

- **Integration with existing backup software** Veeam to ensure seamless backup operations.
- The backup appliance shall be rack-mounted in accordance with standard data center practices, ensuring proper airflow, grounding, and cable management. All network interfaces shall be connected and configured to optimize bandwidth utilization, including any necessary link aggregation or bonding. Once installed, connectivity to backup servers and the existing storage infrastructure shall be verified to ensure seamless integration and reliable data flow across the environment.
- **Storage configuration**, including retention tiers, landing zone, and long-term storage.
- Implementation includes configuring ransomware protection and recovery, with a non-network-facing tier, delayed deletes, and immutable objects to ensure backups cannot be immediately deleted or encrypted.
- **Enable and configure deduplication** to optimize storage utilization and minimize backup footprint.

3.9 Support & Maintenance

- 3 years OEM support and warranty and indicating price for 4th and 5th year.
- 24×7 production support for the entire solution. Storage components shall be covered with 4-hour hardware replacement, while all other components included in the proposal shall be covered with Next Business Day (NBD) hardware replacement and shipping.

4.0 Testing, Training and Documentation

- The proposed solution shall be fully tested in a non-production environment to verify that all components function as intended and meet the defined scope before being moved to the production environment.
- The vendor shall provide comprehensive training and complete documentation for the proposed solution.
- The vendor shall deliver authorized, hands-on training for two (2) engineers on all proposed products.

4. Vendor Qualifications

Vendors must provide: - Company profile and relevant certifications - Proven experience in similar projects - client references – qualified engineer details - Authorized partner status with the proposed OEM.

---

5. Proposal Submission Requirements

Proposals should include: - Executive summary - Detailed technical solution - Bill of Materials (BoM) - Implementation plan and timeline - Support and warranty details - Commercial proposal (separate, clearly itemized)

---

6. Evaluation Criteria

Proposals will be evaluated based on: - Technical compliance and solution quality - Scalability and future readiness - Vendor experience and support capability - Total cost of ownership (TCO) - Implementation timeline

---

7. Timeline

- Proposal submission deadline: 26/02/2026

---

8. Terms & Conditions

- University Hospital Sharjah reserves the right to accept or reject any or all proposals
- This RFP does not constitute a contract or commitment