UHS | UNIVERSITY HOSPITAL SHARJAH مستشفى الجامعة بالشارقة	**Tender Guidelines**

RFP Reference: UHS/IT/TENDER/039/2026 **17th September 2026**
RFP Closing Date: 1st October 2026

No.	Description
1	**Network Access Control System**

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

Network Access Control System

Including IoT, Medical IoT and OT Devices

1. Introduction

UHS invites qualified and experienced vendors to submit technical and commercial proposals for the supply, implementation, integration, configuration, testing, training, and three-year support of an enterprise-grade Network Access Control (NAC) system.

The solution shall provide centralized visibility, identification, profiling, authentication, authorization, access enforcement, segmentation, monitoring, and lifecycle management for devices connected through wired, wireless, VPN, remote-access, IoT, medical IoT, and Operational Technology (OT) networks.

The solution must protect UHS networks without adversely affecting patient safety, medical-device availability, operational reliability, or critical clinical and facilities-management services.

2. Project Objectives

- Discover and maintain visibility of all connected devices.
- Identify authorized, unauthorized, unknown, unmanaged, and non-compliant devices.
- Profile corporate, biomedical, IoT, medical IoT, and OT devices.
- Prevent unauthorized network access and enforce least-privilege access.
- Support secure wired, wireless, and remote-access authentication.
- Apply user-, role-, device-, location-, posture-, ownership-, and risk-based policies.
- Provide safe, passive, and agentless visibility for sensitive medical and OT devices.
- Enable dynamic segmentation, quarantine, remediation, and threat-based containment.
- Integrate with UHS identity, network, endpoint, security, SIEM, and service-management platforms.
- Support zero-trust security, regulatory compliance, audit readiness, and future growth.

3. Environment and Sizing

Requirement	Minimum Requirement
Active device capacity	3,500 active devices
Growth capacity	At least 30% without architectural replacement
Connectivity	Wired, wireless, VPN, and remote access
Device coverage	Corporate, guest, BYOD, IoT, medical IoT, OT, biomedical, clinical, security, and facilities devices
Network environment	Multi-vendor, physical and virtual infrastructure
Availability	High-availability production architecture
Support term	Three years warranty, maintenance, and support from principal vendor

4. Scope of Work

4.1 Assessment and Design

- Conduct requirement workshops and assess the existing wired, wireless, VPN, identity, endpoint, certificate, network, and security environment.

- Discover devices, network infrastructure, VLANs, subnets, access controls, integrations, and unsupported or incompatible components.
- Identify devices that cannot support 802.1X or endpoint agents and document medical and OT operational constraints.
- Prepare high-level and low-level designs, architecture and communication-flow diagrams, authentication and authorization design, segmentation design, policy matrix, rollout plan, rollback plan, and acceptance plan.

4.2 Supply, Installation and Configuration

- Provide all required licenses, subscriptions, appliances or virtual machines, connectors, certificates, professional services, and third-party components.
- Install and configure production and high-availability NAC components, policy services, monitoring, reporting, profiling, RADIUS, APIs, backup, restoration, role-based administration, logging, alerts, and health monitoring.
- Apply vendor-recommended security hardening and provide complete configuration documentation.

4.3 Policy Development and Phased Rollout

- Develop policies for corporate endpoints, thin clients, printers, IP phones, biomedical and medical devices, IoT, OT, CCTV, access control, building systems, guests, contractors, vendors, BYOD, unknown devices, non-compliant devices, and temporary exceptions.
- Implement in controlled phases: discovery, visibility-only mode, profiling, policy simulation, pilot, low-risk enforcement, corporate enforcement, guest and contractor enforcement, IoT/medical IoT/OT enforcement, optimization, and handover.
- Do not enable enforcement affecting critical clinical, biomedical, safety, or OT devices without documented testing, risk assessment, UHS approval, and an agreed rollback procedure.

5. Mandatory Technical Requirements

No.	Area	Requirement
1	Discovery and Visibility	Real-time and historical visibility of wired, wireless, VPN, known, unknown, unmanaged, unauthorized, static-IP, and roaming devices. Correlate data from switches, wireless controllers, DHCP, DNS, ARP, SNMP, RADIUS, flow data, SPAN/mirror ports, firewalls, endpoint tools, and APIs.
2	Device Profiling	Profile device type, manufacturer, model, operating system, firmware, hostname, MAC/IP, services, DHCP fingerprint, certificates, traffic behaviour, location, ownership, management status, and authentication method. Support built-in and custom profiles, confidence scoring, reclassification, tagging, and audit history.
3	IoT, Medical IoT and OT	Provide agentless and passive discovery. Avoid active scans unless approved. Identify device attributes and normal communications, detect unusual behaviour or unauthorized destinations, assign risk, and restrict access to approved resources. Critical medical devices must not be automatically quarantined without UHS approval.
4	Authentication	Support IEEE 802.1X, MAC Authentication Bypass, web authentication, certificate authentication, machine and user authentication, EAP-TLS, PEAP, RADIUS, Active Directory, LDAP, internal identity stores, Microsoft Entra ID where applicable, and MFA integration where applicable.
5	Authorization and Enforcement	Support contextual authorization using user, group, device, profile, ownership, management status, posture, connection type, location, time, clinical role, criticality, risk, threat, and compliance information.
6	Segmentation	Support dynamic VLANs, downloadable or dynamic ACLs, security-group tags or equivalent, firewall tags, role-based access, CoA, restricted networks, quarantine, remediation, captive portals, and identity-based segmentation across wired and wireless networks.
7	Endpoint Posture	Assess supported corporate endpoints for operating system, patching, EDR/antivirus, firewall, MDM/UEM, applications, certificates, domain status, and UHS-defined controls. Support remediation and reauthorization. Do not apply incompatible posture agents to medical, IoT, or OT devices.
8	Guest, Contractor and BYOD	Provide guest registration and sponsorship, time-limited access, branded portals, contractor approval and expiry, accountable sponsors, BYOD registration, certificate provisioning and revocation, acceptable-use controls, and restricted access.

No.	Area	Requirement
9	Threat Response	Integrate with EDR, XDR, SIEM, SOAR, vulnerability-management, firewalls, and threat platforms to trigger reauthentication, access restriction, quarantine, ticket creation, alerts, and approval-based containment.
10	Administration and Audit	Provide role-based administration, least privilege, AD and MFA integration for administrators, complete administrator and policy-change audit logs, read-only auditor access, and maker-checker approval where available.
11	Availability, Security and Scalability	Provide high availability, secure communications, encryption in transit and at rest, current TLS support, hardened systems, secure backups, vulnerability and patch management, IPv4/IPv6 support, scale-out capability, capacity monitoring, and support for 30% growth.
12	Monitoring and Reporting	Provide dashboards and reports for inventory, profiles, medical IoT/OT, authentication, policy decisions, posture, guests, contractors, BYOD, quarantine, risk, movement, system health, availability, integration status, and license use. Reports must be searchable, filterable, schedulable, and exportable to PDF, CSV, and Excel.

6. Integration and Compatibility Requirements

- Identity: Microsoft Active Directory, LDAP, certificate authorities, MFA, and Privileged Access Management where applicable.
- Network: multi-vendor switches, wireless controllers and access points, routers, firewalls, VPN gateways, data-centre networking, SDN, cloud networking, DHCP, DNS, and network-management systems.
- Security: SIEM, SOAR, EDR/XDR, antivirus, vulnerability management, IDS/IPS, NDR, threat intelligence, MDM/UEM, and firewalls.
- Technical compatibility: RADIUS Change of Authorization, SNMPv3, secure APIs, secure syslog where available, IPv4, IPv6, physical and virtual infrastructure, branch sites, and network high-availability configurations.
- The bidder shall provide a current product-support and network-device compatibility matrix, including minimum firmware requirements and all limitations.

7. Implementation, Pilot and Acceptance

The bidder shall submit a project methodology, schedule, resource plan, responsibilities, dependencies, risk register, escalation process, change-management approach, rollback approach, and acceptance criteria.

7.1 Minimum Project Stages

1. Project initiation and stakeholder workshops.
2. Assessment, discovery, high-level design, and low-level design.
3. Platform installation, integration, visibility-only deployment, and device classification.
4. Policy design, simulation, pilot, user acceptance testing, and phased enforcement.
5. Medical IoT and OT validation, high-availability and disaster-recovery testing.
6. Training, production go-live, hypercare, documentation, handover, and closure.

7.2 Proof of Concept

UHS may require shortlisted bidders to conduct a non-disruptive proof of concept covering selected discovery, profiling, 802.1X, MAB, certificate authentication, dynamic access assignment, guest access, posture, quarantine, integrations, reporting, and high-availability use cases. The bidder shall provide prerequisites, test cases, success criteria, rollback procedures, and a results report.

7.3 Final Acceptance

- Completion of the agreed scope and successful integration with agreed systems.
- Successful functional, authentication, authorization, segmentation, profiling, security, backup, restoration, failover, failback, performance, and user acceptance testing.
- Resolution of all critical and high-priority issues.
- Completion of agreed device onboarding and profiling.

- Completion of training and submission of all required documentation.
- Formal written approval by UHS.

8. Required Deliverables

- Project plan, requirements document, assessment report, discovery report, and risk register.
- Supported-device and network-compatibility matrices.
- High-level and low-level designs, architecture diagrams, communication matrix, and integration design.
- Authentication, authorization, profiling, segmentation, IoT, medical IoT, and OT policy matrices.
- Installation, configuration, security-hardening, backup, restoration, high-availability, and operational guides.
- Test plans and results, user acceptance report, license inventory, final configuration backup, and project-completion report.
- All documentation in editable electronic format.

9. Training and Knowledge Transfer

- Knowledge-transfer sessions, training materials, and recordings.
- Authorized virtual classroom NAC administrator training interactive, live, instructor-led sessions (or) pre-recorded material.

10. Warranty, Support and Maintenance

The bidder shall provide three years principal-vendor warranty and support, including:

- 24 x 7 support for critical incidents.
- Remote technical support and principal-vendor escalation.
- Software updates, security patches, product upgrades, and device-profiler library updates.
- Integration updates, problem diagnosis, support-portal and knowledge-base access.
- Product security notifications and critical vulnerability advisories.

11. Vendor Qualification Requirements

- Company profile, local UAE office, and local support capability.
- Principal-vendor authorization and proposed project-team details.
- Number of years implementing NAC solutions and number of certified engineers.
- Relevant network, security, project-management, information-security, and quality certifications.
- NAC references, including healthcare, banking, government sector reference.
- Demonstrated experience with medical IoT, OT or building-management environments, multi-vendor networks, and high-availability NAC deployments.
- Product lifecycle and roadmap confirmation, including confirmation that the proposed product is not approaching end of sale or end of support.

12. Licensing and Commercial Proposal

The commercial proposal must include all licenses, subscriptions, appliances, virtual machines, integrations, professional services, training, warranty, maintenance, and support required for the complete scope.

- Clearly explain whether licensing is based on concurrent endpoints, unique endpoints, active sessions, users, devices, IoT/OT devices, guests, BYOD, profiling, posture, integrations, HA, DR, reporting, APIs, log storage, or subscriptions.
- Clearly identify all optional, separately licensed, third-party, capacity-dependent, or future-cost components.
- Provide license growth options, true-up conditions, support renewal terms, and product upgrade entitlements.
- Provide separate one-time and recurring costs and a complete three-year total cost.

13. Bidder Response Instructions

The bidder shall respond to each requirement using one of the following classifications:

- Fully Comply
- Partially Comply
- Does Not Comply
- Available through Customization
- Available through Third-Party Integration
- Planned in Product Roadmap

Any partial compliance, limitation, customization, dependency, third-party requirement, roadmap item, or additional licensing requirement must be clearly explained.

RFP Section	Compliance	Bidder Response / Remarks	Additional License / Dependency
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

14. Proposal Submission Checklist

- Technical proposal and completed compliance response.
- Solution architecture, sizing, HA design, and implementation methodology.
- Product and network compatibility matrices.
- Project schedule, team profiles, certifications, and references.
- Licensing model and complete three-year commercial proposal.
- Warranty, support, escalation, and service details.
- Product lifecycle, roadmap, security advisory, and vulnerability-management information.
- List of assumptions, exclusions, dependencies, optional items, and deviations.

Important: The successful bidder is responsible for providing a complete and operational solution. Any component required to meet the stated scope but omitted from the proposal shall be identified before contract award.