Tender Guidelines

RFP Reference: UHS/IT/TENDER/002/2026 **4th February 2026**
RFP Closing Date: 19th February 2026 before 12:30 PM.

No.	Description
1	**Email Security Gateway Solution**

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)

Email Security Gateway Solution

1. Introduction

University Hospital Sharjah invites qualified and experienced vendors to submit a proposal for the supply, implementation, and support of an **Email Security Gateway (ESG)** solution. The objective of this RFP is to procure a comprehensive solution that provides advanced protection against email-based threats while ensuring compliance, reliability, and ease of management.

2. Organization Overview

University Hospital Sharjah is currently using Microsoft Exchange On-Premises with approximately **1650 mailboxes**. An estimated **8000 inbound and 2000 outbound emails** are processed daily through the Exchange servers.

The email environment is protected by a two-layer security architecture: the first layer consists of a secure email gateway, and the second layer provides advanced protection against spam, malware, phishing, and other advanced threats.

3. Scope of Work

Providing an Email Security Gateway solution covering **1,800 mailboxes**, with scalability to support at least **3,000 mailboxes** in the future without requiring a change in the core architecture. in full compliance with the requirements defined in this RFP.

The selected vendor shall be responsible for: - Providing an Email Security Gateway solution as per the requirements defined in this RFP - Design, deployment, configuration, and testing of the solution - Integration with existing email and security infrastructure - Knowledge transfer, documentation, and training - Ongoing support, maintenance, and updates directly from principal vendor.

4. Vendor Information

Vendors must provide the following details: - Company profile and legal entity details - Years of experience in email security solutions - Regional presence and local support capability - Details of similar implementations (preferably in enterprise or healthcare environments) - customer references - Product roadmap for the next 3–5 years

5. Technical Requirements

5.1 Deployment & Architecture

- Supported deployment models (Cloud / On-premises / Hybrid) Preferred deployment option: On-Premises.
- High availability and redundancy architecture
- Scalability to support future mailbox growth
- Supported email platforms (Exchange)

5.2 Core Email Security Features

- Anti-spam and bulk mail filtering
- Anti-malware and ransomware protection
- Advanced phishing detection
- Business Email Compromise (BEC) protection
- URL reputation analysis and time-of-click protection
- Attachment sandboxing / detonation
- Impersonation and spoofing protection
- User Security Awareness Training

5.3 Threat Detection & Intelligence

- AI / Machine Learning–based threat detection
- Real-time threat intelligence feeds
- Zero-day threat protection
- Look-alike and spoofed domain detection

5.4 Email Authentication & Compliance

- Support for SPF, DKIM, and DMARC (monitoring and enforcement)
- DMARC reporting and analytics
- Email encryption capabilities (TLS, policy-based, end-to-end)
- Regulatory compliance support (HIPAA, GDPR, ISO 27001, etc.)
- Detailed reporting.

---

6. Administration & Management

- Centralized management console
- Role-Based Access Control (RBAC)
- Policy customization and granular rule creation
- End-user quarantine and self-service portal
- Reporting and dashboards (security posture, trends, incidents)

---

7. Incident Response & Automation

- Automated threat response and remediation
- Ability to retract malicious emails from user mailboxes

- Integration with SIEM / SOAR platforms
- Alerting and notification mechanisms
- Email trace and forensic investigation capabilities

8. Performance & Reliability

- Guaranteed uptime SLA (minimum 99.9%) for cloud option.
- Email delivery latency
- False positive and false negative rates
- Mail continuity and failover during outages

9. Reporting & Visibility

- The secure email gateway must provide detailed and customizable reporting on email traffic, security threats, spam filtering effectiveness, malware detection, phishing attempts, and policy enforcement, with options for scheduled and on-demand reports.

10. Integration & Compatibility

- Integration with leading security tools (SIEM, SOC, EDR, XDR)
- API availability for automation and reporting
- Directory services integration (Active Directory)

11. Security & Data Privacy

- Data residency within the UAE is preferred in the case of a cloud-based deployment
- Encryption of data at rest and in transit
- Compliance certifications (HIPAA, GDPR, ISO 27001, etc.)
- Data retention and deletion policies
- Whitelist (safelist) or blacklist (block) an email source.

12. Support & Maintenance

- Support model and hours (24×7 preferred)

13. Commercial & Licensing

- Licensing model (per user / mailbox / domain)
- Minimum licensing requirements
- Subscription options (3 years, indicative price for 4th and 5th year renewal)
- Principal vendor support services for 3 years 24/7 same day support.

14. Proof of Concept (PoC)

- Availability of Proof of Concept
- PoC duration and scope
- Success criteria and evaluation methodology

15. Proposal Submission Guidelines

Vendors must submit their proposal including: - Technical proposal - Commercial proposal - Compliance matrix against RFP requirements - Product datasheets and certifications

Submission Deadline: 19/02/2026

Submission Method: Physical Submission

16. Evaluation Criteria

Proposals will be evaluated based on: - Compliance with technical requirements - Solution capabilities and scalability - Vendor experience and references - Support and SLA commitments - Commercial competitiveness