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

Posting Date: 1st September 2025
Tender Reference: UHS/IT/TENDER/024/2025
Tender Expiry Date: 10th September 2025

Title: EDR (Endpoint Detection and Response)

Dear Valued Vendors

University Hospital Sharjah (UHS) has decided to invite vendors for a Tender. You, as a vendor are requested to participate in the tender process by submitting your offer for one or more of the items described in attached technical indicative document.

The Tenderer should comply with the following terms & conditions:

1. All the prices should be presented in UAE Dirham.

2. The Specification of the proposed scope of services & materials used, should be clear, informative & include Brand, Origin, Unit of measurement, Qty, Duration, and Delivery Period.

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

4. The financial offer should be on your company letterhead containing the authorized signatory and may please be sent to the attention of the Director of Finance, **University Hospital Sharjah, PO Box 72772, Sharjah in a sealed document**.

5. 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.

6. As a part of the Tender document, the Vendors are requested to provide their valid Trade License, Name, and Designation of the Managing Director/General Manager/Sr. Manager have the authority to bind their company for the business relationship. Also, is required the authorization letter/Agency certificate confirming that the vendor is legalized to supply the items on behalf of the manufacturer/principal company. 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.

7. Standard payment terms are 90 days from the date of completion of delivery of all the items ordered or as specifically agreed in writing by the Materials Management Department of UHS
8. Any delays or short supply or non-conformance may result in the termination of Purchase contract and/or imposition of penalty for delayed supplies as per the Purchase Agreement terms and conditions. **A performance bond may be required to ensure commitment to the agreed timelines and quality standards**.

9. The proposed items should be evaluated & approved by UHS's technical team before confirmation. Once the agreement is signed off, the supplies will have to correspond to the same quality, specification, and source as originally agreed and any deviations shall be considered a contractual breach.
10. The specified brand and manufacturer must remain unchanged throughout the contract period unless otherwise approved by UHS in writing.
11. Any defective products should immediately be replaced with new ones or rectified, as and when notified within a maximum period of one month from the date of notification, at no additional cost to UHS.

[

12. UHS will be constantly evaluating the compliance of Contracted Terms and consistency in supplies and progress of work throughout the duration of the project. 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, therefore UHS reserves the right to terminate the contract if the vendor is not able to rectify during the time allotted by UHS's representative.
    Purchase 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 technical offer should conform to the Indicative specification as per the attachment.
        ii. Technical offer (hard copy and soft copy).
        iii. Reference project where similar work was performed.
        iv. Preferred Partner of the proposed solution.

    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 reserves the right to accept/reject the tenders without assigning any reason thereof.
    a. The tender will be awarded project-wise as per the Purchase contract.

15. 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 contract terms thoroughly. This will ensure that all deliverables, KPIs, and expectations are clearly outlined before the final agreement is signed.
16. . Vendors must submit a risk management plan, identifying potential risks to the project, such as security 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.
17. 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.

18. The Vendor, its employees, its subsidiaries, and everyone who has a direct or indirect relationship with implementing and securing the works and purchases 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.

19. 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.

20. The copyright of any documents and materials 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.

University Hospital Sharjah

ENDPOINT DETECTION AND RESPONSE PROJECT

Requirements:

1. EDR (Endpoint Detection and Response)

- The solution, including both agent and management components, must demonstrate robust security against insider and external threats, ensuring secure design, deployment, and operation.
- Must use behaviour analysis, leveraging real-time cross-machine correlations and enriched endpoint data to accurately identify threats.
- The solution should integrate advanced techniques such as machine learning (pre-execution and runtime), vulnerability protection, and behaviour analysis to enhance automated detection, response, and application control.
- The solution must provide robust ransomware protection, including the ability to detect, prevent, and respond to ransomware attacks, and offer file recovery options to restore data after an attack.
- Must support continuous data collection, analytics, and centralized reporting, managed from a single console with support for threat hunting and predefined automated incident responses.
- Agent must not degrade endpoint performance, including in virtualized environments (VDI).
- The solution must support USB device management (block or restrict read/write/execute) and provide host-based firewall capabilities for Windows and macOS.
- The solution must integrate with external threat intelligence feeds to enhance detection capabilities
- Must integrate with any SIEM/SOC/SOAR solutions for streamlined security information management.
- Must ensure full threat detection and prevention even in offline mode, without requiring network connectivity.
- Must use real-time techniques, including signature-based and behavioural analysis, to detect malware within files and provide reputation-based file protection to block suspicious applications.
- Must support application whitelisting, management of exceptions, and allow or block unsigned applications based on hash for minimizing false positives.
- Must support granular control over security policies by excluding specific files, folders, behaviours, and telemetry from designated applications to reduce false positives.
- Dashboards should provide actionable elements for incident investigation and resolution, including continuous hunting for threats and adversarial activity.
- Must continuously record telemetry for investigation, detect server exploitation, track social engineering attacks, privilege escalation, registry changes, and inbound network processes.
- Must provide incident response capabilities, isolating infected endpoints while maintaining communication for investigation, and automating actions based on specific conditions (e.g., endpoint isolation, notifications via email, SMS).

- Deployment must be smooth, without requiring multiple reboots or interruptions, and must include a lightweight agent with minimal performance impact.
- Must offer scheduled, customizable dashboards and reports for continuous monitoring and auditing.
- Should provide tool for uninstalling the existing antivirus agent and installing the new agent
- License required for 200 servers (which include 150 windows and 50 Linux) and 900 desktops which include 5 MAC

2. Training, Support and Subscription

2.1. Training

a) Vendor must provide free-of-cost certified (authorized) training from an authorized training partner for two UHS IT staff. Training should be a comprehensive administrative training and should not be basic.

2.2. Support and Subscription

a) Proposal must include subscription for 3 years with 24/7 support
b) Vendor should provide mandatory 3 Months support after go-live (remote or on-site support).
c) Need to specify what will be on-going maintenance cost for 4th and 5th year.

3. Security and Audit

The solution should not cause any security vulnerability