

REQUEST FOR PROPOSAL (RFP)

Provision, Deployment & Support of Next-Generation Firewall and Enterprise Wireless Access Points - LEHS

Opening date of RFP: 10/08/2026

Closing Date of RFP: 22/08/2026 – 23:59 hours

I. INTRODUCTION

Lords Education and Health Society (LEHS) is a charitable organization in India working towards advancing inclusive development across healthcare, education, agriculture, and governance.

Through its flagship program, WadhvaniAI, LEHS designs, develops, and deploys artificial intelligence solutions for large-scale social impact in partnership with State and National Governments, development organizations, and ecosystem stakeholders.

As part of its continued growth and digital transformation, LEHS – WadhvaniAI intends to strengthen its office network and perimeter security infrastructure through the deployment of an enterprise-grade Next-Generation Firewall (NGFW) solution and centrally managed Enterprise Wireless Network.

The proposed solution is expected to provide a secure, resilient, high-density, and centrally managed network environment aligned with Zero Trust principles, enterprise security practices, and ISO 27001 requirements.

LEHS therefore invites proposals from qualified and authorized system integrators / technology partners for the supply, implementation, configuration, integration, testing, commissioning, licensing, and support of the proposed solution.

II. BACKGROUND

LEHS – Wadhvani AI operates in a cloud-first environment where users access multiple SaaS applications and cloud platforms, including Google Workspace, Amazon Web Services (AWS), Google Cloud Platform (GCP) and other business-critical applications.

The organization currently operates a combination of corporate-managed devices, consultant/BYOD devices, legacy network infrastructure, and standalone wireless access points.

The organization intends to modernize the network infrastructure to provide:

- Secure internet and perimeter connectivity
- High-density enterprise Wi-Fi
- Network segmentation and isolation
- Identity-aware access control
- Secure access for corporate and BYOD users

- Centralized monitoring and management
- Advanced threat prevention
- Secure remote administration
- Resilient connectivity through redundant ISPs
- Improved visibility into network traffic, users, applications, and security events

III. CURRENT ENVIRONMENT OVERVIEW

Field	Details
Organisation	Lords Education and Health Society
Programs	LEHS - Wadhwani AI
Domains	wadhwaniai.org, lehsindia.org
Corporate Users	~300
BYOD Users	~50 Consultants/Users
Identity Provider	Jumpcloud And Google Workspace
MDM	JumpCloud
OS Mix	70–80% macOS, rest Windows
Device Ownership	Mostly corporate-owned
ISP Bandwidth	Primary & Secondary redundant leased lines (100 Mbps)
Compliance	ISO 27001

IV. PROJECT OBJECTIVES

The selected bidder shall enable LEHS / Wadhwani AI to achieve the following objectives.

1 Secure Network Perimeter

Deploy an enterprise-grade Next-Generation Firewall capable of protecting the organization's Internet perimeter and supporting the organization's current and anticipated network traffic.

The firewall shall support appropriate security controls including IPS, application control, URL filtering, malware protection, VPN and SSL/TLS inspection capabilities.

2 Enterprise Wireless Connectivity

Deploy six (6) enterprise-grade Wi-Fi Access Points to provide secure and reliable wireless coverage across the designated office areas.

The final placement of the APs shall be determined based on the bidder's proposal/site assessment and the physical layout of the office.

3 Network Segmentation

Implement appropriate VLANs and security zones to logically segregate:

- Corporate users
- Consultants / BYOD
- Guest users
- IoT / unmanaged devices, where applicable
- Network management
- Servers / development environments, where applicable

4 Identity-Aware Access

Enable secure authentication and access control for corporate wireless users using appropriate enterprise authentication mechanisms such as:

- WPA2/WPA3-Enterprise
- Integration with the organization's identity platform, where technically supported

5 Advanced Threat Protection

The firewall solution shall provide security capabilities including:

- Intrusion Prevention
- Anti-Malware
- Application Control
- URL/Web Filtering
- SSL/TLS inspection
- Threat intelligence
- VPN
- Security logging and alerting

6 Centralized Management and Monitoring

The proposed solution shall provide centralized management and visibility for the firewall and wireless infrastructure, either through an integrated platform or appropriate management consoles.

V. SCOPE OF WORK

The selected bidder shall provide end-to-end supply, installation, configuration, commissioning and support for one (1) Next-Generation Firewall and six (6) Enterprise Wireless Access Points, including all required hardware, software, licenses, subscriptions and accessories.

The scope shall include the following:

1 Supply & Licensing

- Supply and delivery of 1 enterprise-grade Next-Generation Firewall.
- Supply and delivery of 6 enterprise-grade Wi-Fi Access Points.
- Provision of all required software, security and management licenses/subscriptions for the quoted solution.
- Provision of all necessary accessories, mounting kits, power/PoE requirements and other components required for a fully operational deployment.

2 Installation & Configuration

The selected bidder shall install and configure the firewall and wireless access points, including:

- Internet/WAN connectivity and primary-secondary ISP failover.
- Firewall security policies, NAT, application control, IPS, URL filtering, anti-malware and other quoted security features.
- Required VLANs and network segmentation for corporate, BYOD/consultant and guest networks.
- Secure wireless SSIDs with appropriate authentication, encryption and access controls.
- Integration with RADIUS / identity services where required.
- Centralized management, monitoring, logging and alerting.

3 Wireless Deployment

The bidder shall conduct a basic site/RF assessment to determine appropriate placement of the six APs and shall optimize the deployment for the office environment.

The wireless solution shall support:

- Wi-Fi 6 / Wi-Fi 6E
- WPA2/WPA3-Enterprise
- Multiple SSIDs
- VLAN assignment
- Network isolation
- Rogue AP detection

4 Network Security & Segmentation

The bidder shall implement appropriate network segmentation and security controls to isolate, at minimum:

- Corporate users

- Consultants/BYOD
- Guest users
- Management/network infrastructure
- Other networks identified during implementation

Inter-network access shall be governed through appropriate firewall policies based on least-privilege principles.

5 Testing & Go-Live

The bidder shall perform configuration validation and User Acceptance Testing covering, at minimum:

- Internet connectivity
- Primary/secondary ISP failover
- Firewall security policies
- VLAN segmentation
- Corporate Wi-Fi authentication
- BYOD/consultant isolation
- Guest network isolation
- Wireless coverage and connectivity
- Firewall security features
- Monitoring and logging

The solution shall be considered successfully commissioned following completion of agreed UAT and handover.

6 Documentation & Handover

The bidder shall provide:

- Network architecture/topology
- Firewall and VLAN configuration summary
- Wireless/AP placement details
- SSID and authentication configuration
- Device and license inventory
- Configuration backup
- Warranty and OEM support details
- As-built documentation

The bidder shall provide basic knowledge transfer to the designated LEHS IT team.

7 Warranty & Support

The bidder shall provide OEM-backed warranty and support for the proposed hardware, software and subscriptions and shall specify applicable response and resolution SLAs, escalation procedures and advance replacement arrangements.

8 Implementation Timeline

The complete deployment shall be completed within 7 calendar days from PO issuance and site readiness,

subject to hardware availability.

The bidder shall provide a concise implementation plan identifying key activities, dependencies and expected go-live date.

VI. TIMELINES

The selected bidder shall complete the supply, installation, configuration, testing and commissioning of the proposed solution within 7 calendar days from the date of Purchase Order (PO) issuance and site readiness, subject to availability of the required hardware, licenses and site access.

The implementation shall broadly include:

1. Site assessment and RF assessment
2. Delivery and installation of the firewall and six (6) wireless access points
3. Firewall, WAN and security configuration
4. Wireless, SSID and network segmentation configuration
5. Integration with required authentication/identity services
6. Testing and User Acceptance Testing (UAT)
7. Go-live and handover
8. Submission of final documentation and configuration details

The bidder shall confirm its ability to meet the above timeline in the technical proposal and identify any dependencies or prerequisites that may affect the implementation schedule.

Any delay attributable to the bidder, including delays in deployment, configuration or commissioning, shall be communicated to LEHS promptly along with a revised recovery plan.

VII. Service Level Agreements (SLAs)

The selected bidder shall provide post-implementation support for the supplied firewall, wireless access points, associated software, licenses and subscriptions throughout the applicable warranty/support period.

The bidder shall clearly specify the following in its proposal:

- Support coverage and support hours
- Remote and onsite support availability
- OEM support and escalation mechanism
- Response and resolution/workaround timelines
- Hardware replacement/RMA process
- Escalation matrix and contact details

The bidder shall provide the following SLA matrix as part of its proposal:

Priority	Description	Maximum Response Time	Resolution / Workaround
P1 – Critical	Complete firewall/network outage or critical security issue		
P2 – High	Significant degradation affecting multiple users/services		
P3 – Medium	Partial service degradation or non-critical issue		
P4 – Low	General service request, configuration or information request		

VIII. Evaluation Criteria

Proposals shall be evaluated based on technical compliance, solution quality, bidder capability, implementation approach and commercial competitiveness.

Criteria	Evaluation Parameters
Technical Compliance & Solution Quality	Compliance with mandatory firewall and Wi-Fi requirements, security features, performance, scalability and proposed architecture
Firewall & Wireless Capability	NGFW capabilities, threat protection, SSL inspection, VPN, network segmentation, Wi-Fi, WPA3, 802.1X, centralized management
OEM & Partner Credentials	Authorized OEM partner status, relevant certifications and OEM support entitlement
Implementation & Support Capability	Relevant deployment experience, implementation plan, technical resources, SLA and post-implementation support
Relevant Experience & References	Experience in similar firewall and enterprise wireless deployments and client references
Commercials / TCO	Total cost including hardware, licenses/subscriptions, implementation, warranty/support and applicable taxes
Delivery Timeline	Ability to meet the required 7-calendar-day implementation timeline

IX. Submission Instructions

- Submission Email: rfp.lehs@wadhwaniai.org
- All documents should be in PDF format.
- Subject line of the email: **"Provision of Next-Gen Firewall & Enterprise Wireless Access Points – LEHS / Wadhvani AI – [Bidder Name]"**
- Submission Deadline: [25/08/2026 & 23:59 Hours]

Bidders who submit complete technical with password protected financial proposals and all mandatory enclosures will be considered only.

Any proposals received by LEHS after the deadline for submission of proposals prescribed in the RFP are liable to be rejected.

X. Mandatory Enclosures

Please submit the following as enclosures or attachments with your quotation:

- Company profile
- Relevant client references
- Work completion reports, purchase orders
- GST registration certificate.
- PAN & TAN registration.
- MSME Certificate, if any
- Audited Financials for the last three years
- Income Tax Return with computation of Income for the last three years
- Cancelled cheque.
- Copy of registration documents/certificate and most recent renewal as a legal entity
- Preferably Private Ltd company and has sound business records.

This section is mandatory for consideration of the proposal.

Disclaimer: LEHS reserves the right to:

- Accept or reject any or all proposals
- Modify or cancel the RFP at any stage
- Seek clarifications without obligation to select any bidder

If bidders do not hear from LEHS within two weeks of RFP closure, the proposal may be considered unsuccessful.