

REQUEST FOR PROPOSAL (RFP)

Provision of Identity, Access & Device Management Solution (JumpCloud Implementation)

Opening date of RFP: 25/03/2026

Closing Date of RFP: 04/04/2026 – 23:59 hours

I. INTRODUCTION

LEHS is a charitable organization in India with the objective of advancing inclusive development across healthcare, education, agriculture, and governance. Through its flagship program Wadhvani AI, LEHS designs, builds, and deploys artificial intelligence solutions for large-scale social impact in partnership with State and National Governments and ecosystem stakeholders.

To support its growing workforce and distributed infrastructure, Wadhvani AI intends to implement a centralized identity, access, and device management platform.

LEHS hereby invites proposals from eligible and experienced vendors for the procurement, implementation, configuration, testing, and support of JumpCloud as the organization's Identity and Device Management solution.

II. BACKGROUND

Wadhvani AI operates in a cloud-first environment with users accessing multiple SaaS applications and cloud platforms such as Amazon Web Services and Google Cloud Platform, along with internal tools.

Currently:

- Identity is managed via Google Workspace
- No centralized device management (MDM) exists
- SSO and MFA are not uniformly enforced

The organization aims to implement a Zero Trust-aligned architecture with centralized control over identity, access, and devices.



III. CURRENT ENVIRONMENT OVERVIEW

Field	Details
Organisation	Lords Education and Health Society
Programs	LEHS - Wadhvani AI
Domains	wadhwaniai.org, lehsindia.org
Corporate Users	~250
BYOD Users	~70–80 consultants
Identity Provider	Google Workspace
MDM	None
OS Mix	70–80% macOS, rest Windows
Device Ownership	Mostly corporate-owned
User Privileges	Local Admin (all users)
Apple Business Manager	Partially configured
HRIS	Zoho People Plus and SGCM
Compliance	ISO 27001

IV. PROJECT OBJECTIVES

The selected bidder must enable the organization to achieve the following:

- Establish a centralized identity platform across Google Workspace, Amazon Web Services, Google Cloud Platform, and SaaS tools
- Implement secure access via SSO and mandatory MFA
- Deploy unified device management with security enforcement
- Enable Zero Trust architecture based on identity, device posture, and role
- Automate user lifecycle management (onboarding/offboarding)
- Implement SaaS governance and application allowlisting
- Eliminate all personal/unmanaged logins on organizational devices
- Ensure minimal disruption to business operations

V. SCOPE OF WORK

The bidder shall provide end-to-end implementation including licensing, deployment, testing, and support.

5.1 Licensing Requirements

- JumpCloud Platform Prime licenses for ~250 users
- SSO licenses for ~75 consultants/interns
- All features, updates, and security modules must be included
- Scalability for future growth

5.2 Identity & Access Management

- Configure Google Workspace with JumpCloud as Central IdP
- Implement SSO across all applications
- Enforce MFA for all users
- Configure RBAC based on:
 - Departments
 - User types (FTE / Consultant / Intern)

5.3 Device Management (MDM)

- Enroll and manage all corporate devices
- Integrate with Apple Business Manager
- Enforce:
 - Disk encryption (FileVault / BitLocker)
 - Patch management
 - Password policies
 - Remove local admin rights post-enrollment
 - Implement software distribution
- Implement security policies across devices

5.4 BYOD Management

- Implement restricted access model:
 - Conditional access enforcement
- Ensure secure access to SaaS and cloud resources

5.5 SSO Implementation

- Google Workspace, Slack, GCP, AWS
- Asana, Confluence, Cursor
- Zoho, Canva
- Others TBD

5.6 Security & Conditional Access

- Implement Zero Trust policies

- Enforce device-based conditional access
- Restrict access to approved applications only
- Eliminate direct login (non-SSO) access

5.7 Password Manager

- Deploy and configure password manager for all users
- Enable secure credential storage and audit logs

5.7 Audit & Compliance

- Enable logging (Directory Insights)
- Ensure audit readiness for ISO 27001
- Define log retention policies

VI. IMPLEMENTATION APPROACH (MANDATORY)

The implementation must be executed in the following phases:

- Phase 0 – Discovery & Planning
- Phase 1 – Identity Setup
- Phase 2 – Device Management
- Phase 3 – SSO & Security Hardening
- Phase 4 – UAT & Go-Live

Bidders must:

- Provide effort estimation (days)
- Assign resource roles

VII. TIMELINES

- Total implementation: 30 days from kickoff (tentative)
- Vendors must submit:
 - Detailed execution plan
 - Milestones and dependencies

VIII. TRAINING & HANDOVER

Vendor must provide:

- End-user training sessions
- Admin training sessions
- Documentation and runbooks
- Knowledge transfer to IT team

IX. Service Level Agreements (SLAs)

The bidder must clearly specify SLAs for:

- Implementation timelines
- Issue response/resolution times
- Post-go-live support
- Escalation matrix

X. Evaluation Criteria

Proposals will be evaluated based on following criteria -

Criteria	Weightage
Technical approach & architecture	25%
Experience with JumpCloud	20%
Implementation & Support Capability	20%
Commercials	25%
Delivery Timelines	10%

Only bids meeting all mandatory technical and commercial conditions will be considered.

XI. Submission Instructions

- Submission Email: rfp.lehs@wadhwaniai.org
- All documents should be in PDF format.
- Subject line of the email: **"Provision of Identity, Access & Device Management Solution (JumpCloud Implementation) – [Bidder Name]"**
- Submission Deadline: [04/04/2026 & 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.

XII. 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 or 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

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.