

Maharashtra State Electricity Transmission Co. Ltd
(CIN No.U40109MH2005SGC153646)

<p>From Office of the Chief Engineer EHV Project Cum O&M Zone, Pune Administrative Building, 3rd floor, Block No.402, Rasta Peth, Pune-411 011 ☎ 020 26066106 (O) 020 26061132 E-Mail : cepune@mahatransco.in</p>	
--	---

No. CE/EHV PC O&M Zone/P/IT/

No. 1741 -

Date: -

10 4 SEP 2025

TO WHOM SO EVER IT MAY CONCERN

Subject: Budgetary offer for 'Supply, Installation, Maintenance & Support for Cloud based Enterprise/Professional 'Centralized Client Server Architecture Endpoint Security protection application for 610 numbers of Clients for one (1) year under EHV PC O&M Zone, MSETCL's jurisdiction'.

Budgetary offers are hereby invited on e-mail (itadmin6000@mahatransco.in) as per above mentioned work and as per 'Schedule-A' & 'Annexure-A' ('Scope of Work') enclosed herewith. Concerns are requested to quote your best reasonable rates for above work as per 'Annexure-A' ('Scope of Work') & as per 'Schedule-A'.

The Terms and conditions are as below:


1. The rates quoted should be valid for minimum 120 days.
2. The rates should be quoted on firm 'quotation'.
3. The exclusive rates and taxes should be quoted separately in given format.
4. You are requested to submit your best reasonable budgetary offer as per 'Schedule-A' & with respect to 'Annexure-A' ('Scope of Work'), for above works on E-mail ID: itadmin6000@mahatransco.in up to 11:00 Hrs on dtd. **11.09.2025**
5. This budgetary offer is invited for 'estimation purpose only' and same will not be considered for any bidding OR other activity & No 'work order' will be issued against this 'Budgetary Offer'. Contact no: 9322948870



(Anil Kolap)
Chief Engineer
EHV PC O&M Zone, Pune



Schedule-A - Supply , Installation, Maintenance & Support for Cloud based Enterprise/Professional EndPoint Security application						
Sr.No.	Description of Item	Quantity	Unit	Per 1 (One) Unit Exclusive Rate (INR)	Total Exclusive Rate (INR)	GST Amount (INR) on 'E'
	A (As per 'Scope of the Work')	B	C	D	E = (B*D)	G
1	Supply of 'End Point Security Application' as per scope of the work with 1 (One) year subscription as per 'Scope of the work' under Jurisdiction of EHV PC O&M Zone,Pune,MSETCL.	610	Number			
2	Installation & Configuration of 'End Point Security Application' as per scope of work	1	Each			
	Total					
						H = (E+G)


 (Anil Kolap)
 Chief Engineer
 EHV PC O&M Zone Pune

Maharashtra State Electricity Transmission Co. Ltd
(CIN No.U40109MH2005SGC153646)

Annexure-A: (Scope of the Work)

Sub: 'Supply, Installation, Maintenance & Support for Cloud based Enterprise/Professional 'Centralized Client Server Architecture Endpoint Security protection application for 610 numbers of Clients for one (1) year under EHV PC O&M Zone, MSETCL's jurisdiction'.

..... 'Scope of the Work' thereof

Supply, Installation, Maintenance, and Support of a Cloud-based Enterprise/Professional 'Centralized Client-Server Architecture' Endpoint Security Protection Application for 610 clients, to be provided for a period of one (1) year under the jurisdiction of EHV PC O&M Zone, MSETCL, with all features and conditions as outlined in this document ('Scope of Work'). Commencement Date of application should be 25 November 2025 & one (1) years validity onwards. Agency has to plan installation accordingly.

Endpoint security application should be of **'Cloud based Enterprise/Professional 'Centralized Client-Server architecture' (Hereafter also referred as 'End Point Security Solution' Or 'Application')**.

The application must be based on a cloud-based Enterprise/Professional 'Centralized Client-Server Architecture' (hereinafter referred to as the 'Endpoint Security Solution' or 'Application') and application **should** include the following features and functionalities:

1. Antivirus:

Antivirus solution should be designed to detect, prevent, and remove malicious software (malware) from computers and networks with following features & functionalities:

- a. Malware Detection and Removal:** Identification and elimination of various types of malwares, including viruses, worms, Trojans, ransomware, spyware, and adware etc.
- b. Real-Time Protection:** Monitoring system activities and network traffic continuously to block threats before they execute or spread.
- c. Behaviour Analysis:** Detection of malicious programs based on their actions rather than relying on signatures, protection against zero-day threats.
- d. Web Protection:** Blocking access to malicious websites and prevention during web browsing. Internet Security to the End Points.
- e. Ransomware Protection:** Protection against encryption-based attacks by monitoring file activities and blocking suspicious processes.
- f. File Activity Monitoring:** Tracking and analysing of file operations such as creation, modification, deletion, and access to detect unusual or harmful activity.
- g. Data Loss Prevention (DLP):** Prevention from unauthorized access, modification, or exfiltration of sensitive data.
- h. System Performance Optimization:** Functionality to clear junk files, optimize system resources, and improve device performance.

- i. **Cloud Integration:** Cloud based facilities for threat intelligence and processing, updates etc. GUI Web based access to administrator to control root level & client level functionalities.
 - j. **Vulnerability Scanning:** Identification of outdated software, misconfigurations, or unpatched systems that could be exploited by attackers.
 - k. **Automatic Updates:** Up-to-date with the latest malware definitions and features as per industry standard.
 - l. **Device and Network Scanning:** Feature to verify all connected devices and network endpoints for threats or vulnerabilities & On demand scan option.
 - m. **Sandboxing:** Isolation of suspicious files in a secure environment to analyse their behaviour before allowing them to interact with the system.
2. **Core Features:**
- a. **Centralized Management Console:** Single web-based GUI dashboard to manage all endpoint security tasks policies, and configurations. Role-based access control for administrators. Over LAN, local server copy for a particular location.
 - b. **Endpoint Protection:** Real-time malware detection and removal. Protection against ransomware, spyware, Trojans, and phishing attacks. Behaviour-based threat detection for zero-day vulnerabilities.
 - c. **Cloud Updates:** Automatic updates for malware definitions and security policies. Cloud-based threat intelligence for real-time protection.
 - d. **Network Traffic Monitoring:** Inspection of inbound and outbound traffic to detect and block malicious activities. Integration with firewalls and intrusion detection/prevention systems.
 - e. **File Integrity Monitoring (FIM):** Tracks and logs changes to critical files to identify unauthorized modifications.
 - f. **Data Loss Prevention (DLP):** Monitors sensitive data movement to prevent unauthorized access or exfiltration. Encryption enforcement for data at rest and in transit.
 - g. **Device Control:** Policy enforcement for peripheral devices like USBs, external drives, and printers. Blocks unauthorized devices from accessing endpoints.
 - h. **Endpoint Detection and Response (EDR):** Continuous monitoring and detailed analysis of endpoint activities. Incident response tools, including threat hunting and remediation.
 - i. **Security Information and Event Management (SIEM):** Seamless integration with Security Information and Event Management (SIEM) systems. Centralized logging and alerting for compliance and audit purposes.
 - j. **Cloud Access Security:** Ensures secure access to cloud applications and data of the solution. Enforcing security policies to the clients via central console.
 - k. **User Behaviour Analytics (UBA):** Monitors user activity for anomalies indicative of insider threats or account compromise.
 - l. **Application Control:** Restricts execution of unauthorized or malicious applications. Enforce application whitelisting and blacklisting.
 - m. **Cloud:** Application will be installed & maintained at OEM's Cloud infrastructure.
3. **Enterprise-Grade Features:**
- a. **Multi-Tenancy Support:** Enabled management of multiple organizational units or clients under a single solution. Scattered locations should be controlled & observed under single GUI.

- b. Policy Customization and Enforcement:** Configurable security policies tailored to specific groups or users. The server application should display the complete list of installed client systems, along with their active or inactive status. Additionally, the server application must have the capability to categorize clients into groups. For example, all clients within a specific office should be grouped together, enabling group-specific policy applications, such as managing applications, web filters, or access controls.
 - c. Scalability and High Availability:** Support all endpoints with minimal latency. Redundant infrastructure to ensure continuous availability.
 - d. Incident Reporting and Analytics:** Real-time alerts with detailed reports on threats and actions taken. Customizable dashboards for security insights.
 - e. Remote Management:** Management of endpoints across locations remotely. Automates patching and updates. Centralized control of antivirus solutions across multiple devices.
 - f. Reporting and Alerts:** Detail logs, alerts, and reports for system administrators or users to review detected threats and actions taken. Report format: PDF, Excel etc.
 - g. Asset Management:** Identifying, tracking, and managing all the devices and software endpoints within an MSETCL that are protected by this solution. It should ensure that all assets are properly secured, monitored, and compliant with security policies. Inventory Management, Reporting and Auditing with device technical details should be available.
 - h. Client Deletion:** The server application should include a feature to delete client entries as required
- 4. Compliance and Security Standards:**
- a. Regulatory Compliance:** CERT-IN guidelines provided by C.O. MSETCL such as IP Blocking, Url Blocking, Hash value blocking etc. Agency will carry out this activity on server side immediately.
 - b. Audit Trails:** Comprehensive logs for analysis and compliance reporting.
 - c. Incident Response Tools:** Pre-configured workflows for fast response to breaches or outbreaks.
- 5. General terms & conditions for Installation, Maintenance & Support Services:**
- a.** The agency shall be solely responsible for the complete installation, configuration, support, maintenance, and re-installation of the application as required by MSETCL, at any time during the contract period.
 - b. Installation:** The agency shall be responsible for the complete installation, which must be physically carried out at each designated location. Additionally, the application is to be installed across remote sites of MSETCL like but not limited to all offices, sub-stations, sub-divisions, units etc. located in the Pune and Solapur districts. All locations are scattered within Pune & Solapur districts. A detailed list of these locations will be provided by MSETCL during the execution phase. While online remote support may be facilitated, its provision will be at the sole discretion of MSETCL. The installation process should be completed within 60 days from the issuance of the Work Order. Upon completing the installation at each circle or division office jurisdiction, the agency will obtain a 'Work Completion Certificate'

from the respective SE/EE. Format of 'Work Completion Certificate' will be outlined & given by MSETCL.

- c. **Offline Installation:** In certain locations, where internet access may be **unavailable**, offline installation must be carried out. The corresponding report should include detailed information regarding this process.
- d. **Maintenance & Support:** The agency shall provide a dedicated 'Email ID' and 'Contact Number' for support services throughout the entire contract period. MSETCL users will contact these communication channels for assistance. The agency must ensure that a direct service contact number is available to MSETCL, and an IVR-based waiting or response system will not be accepted. All support services must be provided from within India, except for online updates or any online services provided by the Original Equipment Manufacturer (OEM). The agency shall be responsible for the comprehensive maintenance of the application throughout the duration of the contract period. This includes ensuring its seamless operation, implementing necessary updates, addressing technical issues, and providing support as required to meet the agreed-upon service standards. The agency shall perform any number of re-installations as required by MSETCL, utilizing the specified communication channels for assistance and support.
- e. **Node Disconnection:** If a node remains disconnected for a continuous period of 60 days, the associated license should be released, and the available license count should be updated accordingly to reflect the increase.
- f. **Count:** The total count of live installations should be clearly displayed, along with the live/offline status and the corresponding status update date. Installation count will be considered as per 'Work Completion report'. The current live & inactive license count should be accessible via the admin portal for monitoring and management purposes.
- g. **Subscription:** Subscription shall be valid for one (1) year from the date of acceptance.
- h. **Clubbing:** The supply, installation, maintenance, and support are all integral components of this contract. MSETCL will process invoices for both 'supply and installation' together. Invoices that pertain solely to the supply portion will not be processed by MSETCL.
- i. **Compatibility:** The application must be compatible with Microsoft Windows operating systems, including Windows 7, 8, 8.1, 10, and 11. Additionally, if newer versions of Microsoft Windows are released during the contract period, the application should ensure compatibility with those versions as well. The application must be capable of supporting all clients simultaneously, ensuring smooth and efficient performance.
- j. **License:** The application should be licensed to the Chief Engineer, EHV PC O&M Zone, Pune, MSETCL, for a period of contract from the date of acceptance/finalisation.
- k. **Application Compliance:** The application must not be prohibited by any legal body in India.
- l. **Password protection:** The uninstallation of the application shall be secured through the use of an 'Uninstallation Password' to ensure controlled and authorized removal. The management and control of the uninstallation password shall remain exclusively with the agency.

- m. **Security Standards:** The application must be fully secure and adhere to recognized industry standards for cybersecurity, ensuring compliance with best practices for data protection, system integrity, and user privacy.
- n. **Malware Removal and Antivirus Uninstallation:** The agency shall ensure the removal of all existing malware from the systems prior to the installation of the application. Additionally, any previously installed antivirus software must be uninstalled before the new application is deployed.
- o. **Project Planning Responsibility:** It shall be the agency's sole responsibility to develop and execute both macro and micro-level project plans, ensuring that all project requirements are thoroughly addressed and implemented. The agency will be accountable for ensuring the timely and effective completion of all project deliverables.

6. Operational Acceptance of Application:

- a. Upon the successful installation of the solution, the agency shall notify MSETCL via email at itadmin6000@mahatransco.in. Following this notification, MSETCL will allow a 7-day period to address any potential issues. If no issues are reported within this period, the solution will be deemed accepted.
- b. During the Operational Acceptance period, if any queries arise, they shall be communicated to the agency through the provided email address. The agency is required to promptly resolve these queries and inform MSETCL via the same email address.
- c. The complete scope of work and the application should be fully functional by End of November 2025.

7. Billing:

- a) After successful Supply & Installation of the complete application, agency shall raise bills/e-invoices, in physical & through MSETCL Bill tracking System (BTS) system.
- b) Invoices will be processed in due time with respect to MSETCL standard terms & conditions.