

Specification for Next generation Anti-Virus Solution (Business and Enterprise) for Disaster Management Centre

Features	Requirements	Yes/No	Remark
	Product name		
	Version		
	Country of Origin		
	Antivirus		
	Duration (as option 1 & 2)		
Options- 01	For the period of one year (01)		** Forward your quotations separately, as on option 01 and 02
Options- 02	For the period of three years (03)		

Scope of the project

The selected solution shall provide centralized, enterprise-grade malware protection for:

Endpoint Type	Quantity	Operating System
Laptops	104	Windows 10 / 11/ 12
Desktops	220	Windows 10 / 11/ 12
Servers	11	Windows Server (2016 or later)

Total Endpoints 335

The solution must support **geographically distributed endpoints** connected via the public internet and private networks.

Technical Specification

1. Solution Architecture Requirements	Yes/ No	Remarks
<p>1.1 Deployment Model The solution shall support any of the following architectures, without functional limitation:</p> <ul style="list-style-type: none"> • Cloud-managed console (SaaS) • On-premises management server • Hybrid (cloud + on-premises) <p>The bidder shall clearly state the proposed architecture.</p>		
<p>1.2 Centralized Management</p> <ul style="list-style-type: none"> • Single centralized management console • Web-based access using HTTPS. • Role-based access control (RBAC) 		

<ul style="list-style-type: none"> • Supports multi-site / group-based policy management (Head Office, District Offices, Servers) 		
2. Core Security Capabilities (Mandatory)		
<p>2.1 Malware Protection</p> <p>The solution shall provide protection against:</p> <ul style="list-style-type: none"> • Viruses • Worms • Trojans • Ransomware • Spyware / Adware • Rootkits • Fileless malware <p>Detection methods must include multiple layers, such as:</p> <ul style="list-style-type: none"> • Signature-based detection • Heuristic analysis • Behavioral monitoring • Machine-learning or AI-based detection • Memory-based attack detection 		
<p>2.2 Real-Time Protection</p> <ul style="list-style-type: none"> • Real-time (on-access) scanning of files • Monitoring of running processes • Protection against malicious scripts and macros • Email attachment scanning (endpoint-based) 		
<p>2.3 Ransomware Protection</p> <ul style="list-style-type: none"> • Behavioral ransomware detection • Unauthorized encryption activity blocking • Ability to rollback or remediate malicious changes (where supported by OS) 		
3. Endpoint Coverage & Control		
<p>3.1 Endpoint Compatibility</p> <p>The solution must support:</p> <ul style="list-style-type: none"> • Windows 10 (64-bit) • Windows 11 (64-bit) upward • Windows Server 2016 / 2019 / 2022 upward 		
<p>3.2 Policy Management</p> <ul style="list-style-type: none"> • Separate security policies for: <ul style="list-style-type: none"> ○ Laptops ○ Desktops ○ Servers • Policy inheritance and override capability • Scheduled and on-demand scans • USB and removable media scanning 		
<p>3.3 Offline & Remote Endpoint Support</p> <ul style="list-style-type: none"> • Endpoints must remain protected when offline. • Automatic synchronization of logs and updates when reconnected. • Optimized update mechanisms for low-bandwidth district offices 		

<p>4. Update & Threat Intelligence</p> <ul style="list-style-type: none"> • Automatic malware definition updates • Frequent updates (multiple times per day) • Secure update channels (encrypted) • Local coaching or bandwidth optimization options (preferred) 		
<p>5. Centralized Monitoring & Reporting</p>		
<p>5.1 Dashboard</p> <ul style="list-style-type: none"> • Real-time threat status • Endpoint health status • Update compliance view. • Infection and remediation summary 		
<p>5.2 Alerts & Notifications</p> <p>Configurable alerts for:</p> <ul style="list-style-type: none"> ○ Malware detection ○ Failed updates ○ Disabled protection ○ Policy violations • Alerts via: <ul style="list-style-type: none"> ○ Email ○ Console notifications + 		
<p>5.3 Reporting</p> <ul style="list-style-type: none"> • Predefined and custom reports • Export formats: PDF, CSV • Historical data retention (minimum 12 months) • Endpoint-wise and site-wise reporting 		
<p>6. Security & Compliance Requirements</p> <p>The solution shall align with recognized standards and best practices, including:</p> <ul style="list-style-type: none"> • ISO/IEC 27001 (Information Security Management) • NIST Cybersecurity Framework • CIS Critical Security Controls • GDPR-style data protection principles (where applicable) • The manufacture as a leader on end point protection in the position of the Gartner magic quadrant for the last two years. <p>Additional requirements:</p> <ul style="list-style-type: none"> • Secure communication between agents and the management console • No hard-coded credentials 		

<ul style="list-style-type: none"> • Tamper protection to prevent unauthorized disabling of the agent. 		
<p>7. Performance & Resource Utilization</p> <ul style="list-style-type: none"> • Lightweight endpoint agent • Minimal impact on: <ul style="list-style-type: none"> ○ CPU usage ○ Memory consumption ○ Disk I/O ○ OS compatibility for Windows 10/11 MAC OS and LINUX • Configurable scan scheduling to avoid business disruption. 		
<p>8. Licensing Requirements</p> <ul style="list-style-type: none"> • License coverage for 335 endpoints • License type: <ul style="list-style-type: none"> ○ Per endpoint (user/device) ○ Includes laptops, desktops, and servers. • License validity: Minimum 1 year (preferably extendable to 3 years) / 03 years (as the optional) • All features must be included without additional hiding costs. 		
<p>9. Installation, Support & Maintenance</p>		
<p>9.1 Deployment Support</p> <ul style="list-style-type: none"> • Centralized deployment options: <ul style="list-style-type: none"> ○ Manual installer ○ Silent installation ○ Remote deployment tools • Clear documentation for distributed deployment 		
<p>9.2 Technical Support</p> <ul style="list-style-type: none"> • Vendor or authorized partner support • Support channels: <ul style="list-style-type: none"> ○ Email ○ Phone ○ Online ticketing ○ On site if required • Defined SLA: <ul style="list-style-type: none"> ○ Critical issues ○ High / Medium / Low severity 		
<p>10. Documentation & Deliverables</p> <p>The guide must provide:</p> <ul style="list-style-type: none"> • Product datasheets • Architecture overview • Installation & administration guides • Licensing details • Support and SLA documentation. • Manufacturer Authorization Dealers for the last 05 years 		
<p>11. Optional Enhancements (Non-Mandatory, Scored Separately)</p> <ul style="list-style-type: none"> • Endpoint Detection & Response (EDR) • Centralized log export to SIEM • Device control (USB, external drives) 		

<ul style="list-style-type: none"> • Application control / whitelisting • Web threat protection 		
12. Operational requirements		
<ul style="list-style-type: none"> • Device Control – Centrally manage and scheduling of device permissions of users. • Web Control –Should have web filter with URL, category base & centrally manage and scheduling of web access permissions of users. • App control- Should have App control functionality to control Start applications, terminate and suspend other processes, and other application modification. • Endpoint firewall control includes rule creating and customization. Endpoint firewall control should support Network connection and connection profiles. 		
13. Support		
<ul style="list-style-type: none"> • Describe if and how you will provide support and the time frame of guaranteed initial response time during the acceptance period. • Specify whether you will provide on-site support in case of emergency. • Supply, Installation and maintenance of all virus guard for DMC requirements 		