

## **ANNEXURE B**

### **TERM OF REFERENCE**

#### **1. Background and Objectives**

The objective is to strengthen the security posture of the organization by deploying a high-assurance endpoint security solution for both workstations and servers. The solution must include centralized threat detection, protection against modern cyber threats, and 24/7 threat monitoring and incident response capabilities over a three-year period. Installation and setup must be completed in the first year.

#### **2. Scope of Work**

2.1 The service provider shall provide a comprehensive, enterprise-grade endpoint security solution that includes the following capabilities

##### **2.1.1 Endpoint Security Deployment**

- Deploy security software on all 140 workstations and 20 servers.
- Configure automated updates and patch management.
- Implement endpoint detection and response capabilities.

##### **2.1.2 Threat Monitoring and Response**

- Provide 24/7 monitoring of all endpoints.
- Detect and respond to malware, ransomware, and suspicious activities.
- Generate timely alerts and incident reports.

##### **2.1.3 Centralized Management Console**

- Provide a single pane of glass for managing endpoints.
- Enable reporting on security status, incidents, and compliance metrics.



- Support role-based access control for IT administrators.
- Centralized console for policy management, reporting, and monitoring
- Role-based access control and audit logs
- Integration with existing IT infrastructure and Active Directory

#### **2.1.4 Deployment & Support:**

- Assistance with installation and configuration
- Ongoing technical support and software updates
- Licensing model that accommodates enterprise-scale deployment

#### **2.1.5 Reporting and Documentation**

- Assistance with installation and configuration
- Ongoing technical support and software updates
- Licensing model that accommodates enterprise-scale deployment

#### **2.1.6 Compliance & Reporting:**

- Compliance with industry security standards and best practices
- Generation of security reports and alerts for auditing purposes

#### **2.1.7 Core Security Features:**

- Anti-virus, anti-malware, and anti-ransomware protection
- Real-time threat detection and automated response
- File, email, and web threat protection

#### **2.1.8 Reporting and Documentation**

- Provide quarterly reports summarizing threat trends, incidents, and system health.



- Maintain documentation of deployment, policies, and incident responses

## **2.2 Endpoint Security Licensing and Provisioning**

### **2.2.1 Supply of enterprise-grade endpoint security software for:**

**2.2.1.1** 140 workstation endpoints

**2.2.1.2** 20 server endpoints

**2.2.1.3** Licensing must be valid for a continuous period of 36 months

**2.2.1.4** The licensing model must support annual once-off payment per year

## **2.3 Year 1 – Installation and Initial Setup**

2.2.1 Deployment of endpoint security agents on all designated devices

2.2.2 Configuration of security policies

2.2.3 Setup of centralized management console (cloud or on-prem)

2.2.4 One-time system hardening and optimization

2.2.5 Integration with directory services (if required)

2.2.6 Provide installation documentation and post-deployment verification

## **2.3 Years 1–3 – 24/7 Threat Monitoring**

2.3.1 Provision of continuous threat detection and monitoring services

2.3.2 Automated threat response and expert-led investigation

2.3.3 Escalation of critical incidents as per defined SLAs

2.3.4 Monthly or quarterly summary reports on detected threats, trends, and resolutions

2.3.5 Access to threat intelligence data

## **2.4 Support and Maintenance**

2.4.1 No monthly operational support tasks required

2.4.2 Vendor must provide access to updates, patches, and security definitions throughout the license period

2.4.3 Product support and issue resolution must be available upon request via service desk or escalation channels



### 3. Technical Requirements

- 3.1 Protection against malware, ransomware, phishing, zero-day threats
- 3.3 Lightweight, tamper-proof agent
- 3.4 Cloud-based or centralized management console
- 3.5 Real-time alerting and automatic remediation capabilities
- 3.6 Reporting and visibility features (dashboard, activity logs)
- 3.7 Must operate 24/7 with incident response capabilities

### 4. Mandatory Compliance and Regulatory Alignment

- 4.1 The solution and provider must comply with:
  - 4.1.1 ISO/IEC 27001 – Information Security Management
  - 4.1.2 ISO 9001 – Quality Management Systems
  - 4.1.3 Protection of Personal Information Act (POPIA)

### 5. Evaluation Criteria

This BID will be evaluated in three phases namely Software Specification, functionality and price & BEE (80/20)

**Table 5.1: Technical Evaluation Criteria Based on Software Specifications**

Item	Specification Area	Evaluation Focus	Weight (%)
1	<b>Core Protection Features</b>	Malware, ransomware, phishing, zero-day threat protection	20%
2	<b>Detection &amp; Response Capabilities</b>	real-time alerting, automated remediation	20%
3	<b>Management Console</b>	Centralized dashboard, role-based access, integration with AD	15%
4	<b>Monitoring &amp; Reporting</b>	24/7 threat monitoring, incident response, quarterly reports	15%



5	<b>System Architecture</b>	Lightweight agent, tamper-proof design, cloud/on-prem console	10%
6	<b>Compliance Alignment</b>	POPIA, ISO/IEC 27001, ISO 9001 adherence	10%
7	<b>Licensing Model</b>	3-year validity, annual once-off payment, scalability for 140 workstations & 20 servers	10%

**Minimum threshold to qualify: 70% total score**

**Table 5.2 - FUNCTIONALITY**

Item	Description	Total Score 100%	Bidder Score %
1	<p><b>Bidder must have Firewall delivery, installation, and configuration in the past three (3) years</b></p> <ul style="list-style-type: none"> <li>❖ No work experience letter attached = 0 points</li> <li>❖ One (1) work experience letter attached = 5 points</li> <li>❖ Two (2) work experience letters attached = 10 points</li> <li>❖ Three (3) work experience letters attached = 15 points</li> <li>❖ Four (4) or more work experience letters attached = 20 points</li> </ul>	20	
2	<b>The Bidder must have three (2) resources certified in the Endpoint Security and 1 Project</b>	20	



	<b>Manager with TOGAF certification. CV with original certified certifications must be attached.</b> <ul style="list-style-type: none"> <li>❖ NO certified resource = 0</li> <li>❖ 1 x certified resource = 5</li> <li>❖ 2 x certified resources = 10</li> <li>❖ 3 or more certified resources = 20</li> </ul>		
3	<b>The Bidder must have the following original certification letter from the vendor (OEM) attached</b> <ul style="list-style-type: none"> <li>❖ 20</li> </ul>	20	
4	<b>Mandatory Compliance and Regulatory Alignment Certificates attached. ISO/IEC 27001 (Information Security Management), ISO 9001 (Quality Management Systems) and ISO/IEC 2000 – 1 (IT Service Management) =10</b> <ul style="list-style-type: none"> <li>❖ 3 Certificates = 20</li> <li>❖ 2 Certificates = 15</li> <li>❖ 1 Certificate = 5</li> </ul>	20	
5.	<b>Functionality &amp; Technical Compliance</b> <p>Meets all listed solution features (core endpoint security, centralized console) =10</p>	20	



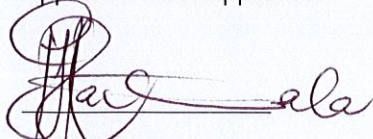
	Integration with firewall and existing IT systems (e.g., AD, DNS) = 10		
<b>Total score obtained</b>			

**NB: Bidders must score a minimum of 70 points to proceed to the next evaluation criteria**

#### 6. Payment Schedule

Year	Payment Structure	Due Date
Year 1	Once-off payment (setup and configuration)	Upon deployment completion
Year 2	Once-off payment (licenses)	12 months after initial payment (start of Year 2)
Year 3	Once-off payment (licenses)	24 months after initial payment (start of Year 3)

Approved / Not Approved.



**RAMOTHWALA R.J**

**Municipal Manager**

Date: 05/09/2025