



NATIONAL LIBRARY OF SOUTH AFRICA

228 Johannes Ramakhoase Street
Private Bag X397
Pretoria
0001

5 Queen Victoria Street
Cape Town
8001

TERMS OF REFERENCE/SPECIFICATIONS FOR THE PROCUREMENT OF MANAGED ANTIVIRUS/ENDPOINT PROTECTION SOLUTION FOR THE NATIONAL LIBRARY OF SOUTH AFRICA, PRETORIA AND CAPE TOWN CAMPUS.

CLOSING DATE: 28 NOVEMBER 2025

TIME:11H00

NB: All proposal/quotation must be submitted to Quotations@nlsa.ac.za, kindly note that failure to submit via this email address will result in your proposal /quotation being rejected and disqualified.

1. BACKGROUND

The National Library of South Africa (NLSA) is a premier African institution tasked with the collection, preservation, and dissemination of South Africa's national documentary heritage. As a custodian of this heritage, NLSA promotes awareness, appreciation, and access to published works both nationally and internationally, contributing significantly to the country's cultural development and prosperity. The NLSA operates from its campuses located in Pretoria and Cape Town.

2. SCOPE OF WORK

- 2.1 The scope of work for implementing and to strengthen the security posture of the National Library of South Africa by deploying a high-assurance endpoint managed security solution for both workstations and servers. The solution must include centralised threat detection, protection against modern cyber threats, and 24/7 threat monitoring and incident response capabilities over a one-year period. Installation and setup must be completed in the first month. The solution should be licensed for a period of 12 months.

2.2 The system should provide alerts, reports, and visualizations to facilitate effective decision making and prompt issue resolution. It should provide continuous monitoring, alerting, and reporting on servers and application health and performance.

2.3 We require an anti-virus solution that offers **seamless integration with our existing firewall environment**

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

2.4.1. Endpoint Security Deployment

- 2.4.1.1. Deploy security software on all X workstations and X servers
- 2.4.1.2. Configure automated updates and patch management
- 2.4.1.3. Implement Endpoint Detection and Response capabilities
- 2.4.1.4. Integrate Extended Detection and Response functionality for correlation across endpoints, email, and network layers

2.4.2. Threat Monitoring and Response

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

2.4.3. Centralized Management Console

- 2.4.3.1. Provide a single pane of glass for managing endpoints
- 2.4.3.2. Enable reporting on security status, incidents, and compliance metrics
- 2.4.3.3. Support role-based access control (RBAC) for IT administrators
- 2.4.3.4. Include centralized console for policy management, reporting, and monitoring
- 2.4.3.5. Maintain audit logs
- 2.4.3.6. Integrate with existing IT infrastructure and Active Directory

2.4.4. Deployment & Support

- 2.4.4.1. Assistance with installation and configuration

2.4.4.2. Ongoing technical support and software updates

2.4.4.3. Licensing model that accommodates enterprise-scale deployment

2.4.5. Reporting and Documentation

2.4.5.1. Provide documentation for installation and configuration

2.4.5.2. Ensure ongoing access to updates and support information

2.4.5.3. Maintain development and operational records

2.4.5.4. Provide quarterly reports summarising threat trends, incidents, and system health.

2.4.5.5. Maintain documentation of deployment, policies, and incident responses.

2.4.6. Compliance & Reporting

2.4.6.1. Compliance with industry security standards and best practices

2.4.6.2. Generation of security reports and alerts for auditing purposes

2.4.7. Core Security Features

2.4.7.1. Anti-virus, anti-malware, and anti-ransomware protection

2.4.7.2. Real-time threat detection and automated response

2.4.7.3. EDR and XDR-based threat correlation and analysis

2.4.7.4. File, email, and web threat protection

2.4.8. Endpoint Security Licensing and Provisioning

2.4.8.1. Supply enterprise-grade endpoint security software for:

2.4.8.1.1. 320 workstation endpoints

2.4.8.1.2. 25 server endpoints

2.4.8.1.3. Licensing must be valid for a continuous period of 12 months

2.4.8.1.4. The licensing model must support annual once-off payment per year

2.4.9. Installation and Initial Setup

2.4.9.1.1. Deploy endpoint security agents on all designated devices

2.4.9.1.2. Configure security policies

- 2.4.9.1.3. Setup of centralized management console
- 2.4.9.1.4. One-time system hardening and optimization
- 2.4.9.1.5. Provide installation documentation and post-deployment verification
- 2.4.9.1.6. Access to threat intelligence data

2.4.9.2. Support and Maintenance

- 2.4.9.2.1. Vendor must provide access to updates, patches, and security definitions throughout the license period
- 2.4.9.2.2. Product support and issue resolution must be available upon request via service desk or escalation channels

2.4.9.3. Technical Requirements

- 2.4.9.3.1. Protection against malware, ransomware, phishing, and zero-day threats
- 2.4.9.3.2. Lightweight, tamper-proof agent
- 2.4.9.3.3. Cloud-based or centralized management console
- 2.4.9.3.4. Real-time alerting and automatic remediation capabilities
- 2.4.9.3.5. Reporting and visibility features (dashboard, activity logs)
- 2.4.9.3.6. Must operate 24/7 with incident response capabilities

3. NLSA'S RIGHTS

- 3.1 The NLSA is entitled to amend any RFQ conditions, RFQ validity period, RFQ terms of reference, or extend the RFQ's closing date, all before the RFQ closing date.

4. DURATION OF THE PROJECT

- 4.1 The appointed service provider shall make an undertaking that the delivery shall be concluded within 30 days after issuing the Purchase Order.

5. CONDITIONS OF RFQ

- 5.1 The NLSA reserves the right not to accept the lowest proposal.
- 5.2 The NLSA reserves the right to appoint one or more Bidders.
- 5.3 The NLSA reserves the right not to award the contract.

5.4 The NLSA reserves the right to have any documentation submitted by the successful Bidder checked or inspected by any other person or organisation.

5.5 The NLSA will not be held responsible for any costs incurred by the Bidder in the preparation and submission of the RFQ.

5.6 No upfront Payment will be done by NLSA.

5.7 The quotation is valid for a period of 30 days and may be extended at the discretion of the NLSA.

6. EVALUATION CRITERIA

6.1 Pre evaluation (standard bid documents)

6.1.1. Fully completed SBD 4 and SBD 6.1 forms.

6.1.2. All bidders must be registered on the National Treasury Central Supplier Database (CSD) and must attach a copy of the most recent report.

6.2 Mandatory:

6.2.1. Bidder to produce letter/certificate stating that the bidder is authorized to provide the proposed solution.

6.2.2. Datasheet for the solution proposed to ensure that all requirements are met.

6.2.3. Bidder must attach an original certification letter from the vendor (OEM)

6.3 Evaluation stage one (1): Technical Evaluation

Bidders are expected to obtain a minimum of sixty (60) points out of one hundred (100) points available to proceed to the next evaluation stage. Failure to obtain the prescribed points will automatically disqualify the bidder from proceeding to the next evaluation stage.

Item	Description	Weight	Point	Score
1	Bidder must have Endpoint Security delivery, installation, and configuration experience in the past three (3) years - No work experience letter attached = 0 points - One (1) reference letter attached = 5 points - Two (2) reference letters attached = 10 points - Three (3) reference letters attached = 15 points - Four (4) or more reference letters attached = 20 points - Four (5) or more reference letters attached = 25 points	25		

2	Bidder must have at least two (2) resources certified in Endpoint Security. CVs with certified copies certifications must be attached. - No CV and/or certified certificates not attached = 0 1 CV with certified certificates attached = 5 2 CVs with certified certificates attached = 15 3 or more CVs with certified certificates attached = 25	25		
3	Mandatory Compliance and Regulatory Certificates attached - No Certificate = 0 - Partnership Certificate = 25	25		
4	Methodology – Proposal confirming that solution meets all technical requirements and can integrate with existing firewall and IT systems - Meets technical requirements and integration requirements = 25 - Meets one or no requirements = 0	25		
Total score obtained				

6.4 Preference Point System

In terms of Regulation 5 of the Preferential Procurement Regulations of 2022/23, Gazette Number 47452 dated 4 November 2022 pertaining to the Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000), responsive bids will be adjudicated by the State on the 80/20-preference point in terms of which points are awarded to bidders based on: -

- The bid price (maximum 80 points)
- Specific Goals (maximum of 20 points):

The following formula will be used to calculate the points out of 80 for price in respect of an invitation for a tender, inclusive of all applicable taxes.

$$P_s = 80 \left(1 - \frac{P_t - P_{min}}{P_{min}} \right)$$

Where-

- P_s = Points scored for price of tender under consideration;
 P_t = Price of tender under consideration; and
 P_{min} = Price of lowest acceptable tender.

- **Specific Goals (maximum of 20 points):**

100% Black owned (20 points), 10 points for other than 100% black owned.

6.5 Evaluation Criteria Stage 2: Pricing

6.5.1. Quotation must provide a pricing schedule which clearly sets out the cost of providing the services including any applicable charges.

6.5.2. The pricing schedule must clearly indicate the unit or item price as well as the total price for the requested.

6.5.3. **All cost items must be inclusive of VAT.**

6.6 Pricing schedule for Antivirus/Endpoint Protection Solution

Item	Description	Unit Cost (ZAR)	Quantity	Total Cost (ZAR)
1. Solution Procurement	Antivirus / Endpoint Protection Solution			
2. Configuration and Setup	Initial configuration and reconfiguration as needed.			
2.1. Initial Configuration	Setup and integration into existing systems			
2.2. Customization	Tailoring the solutions to fit NLSA's specific needs			
3. Training				
3.1. Administrator Training x 5	Training for administrators on solution navigation and management (Virtual)			
3.2. Training Manuals	Comprehensive training manuals for administrators			
4. Maintenance and Support				
4.1. Annual Maintenance	Yearly maintenance and support services			
4.2. Technical Support for 4 hrs. per month for 24 months	Ongoing technical support and troubleshooting			
6. Total Project Cost Including VAT				

7. ENQUIRIES

All enquiries regarding this RFQ must be directed to the SCM Office:

For any RFQ related enquiries please send to the following email address quoting the RFQ Reference Number, Bid Description as a Reference; Judy.Moshige@nlsa.ac.za and quotations@nlsa.ac.za OR (012) 402 3017