

South African National Accreditation System  
 Libertas Office Park  
 Cnr Libertas and Highway Streets  
 Equestria  
 Pretoria  
 0184

## REQUEST FOR QUOTATION



### PLEASE COMPLETE AND SUBMIT TOGETHER WITH REQUIRED DOCUMENTS AND QUOTATION

DATE OF ISSUE:	20 October 2022-Reissue	REQUISITION NUMBER	REQ0004539
CLOSING DATE:	28 October 2022	CLOSING TIME:	11:00
QUOTE VALIDITY:	60 days from the date the RFQ closed	Submissions and enquires to be made to:	Ms Nkhesani Mathebula <a href="mailto:procurement@sanas.co.za">procurement@sanas.co.za</a> 012 740 8536

#### 1. PRODUCT /SERVICE DETAILS

Description of goods / services: Threat detection and response system (TDRS) for a period of 36 months		Quantity required
<p><b>TERMS OF REFERENCE</b></p> <p><b>1. PURPOSE</b></p> <p>The purpose of this RFQ is to invite suitably interested qualified service providers to submit their quotations for the <b>Threat Detection and Response System (TDRS)</b>, as part of enhancing the security of the Users, Data, Information, and Information Systems for the South African National Accreditation System (SANAS).</p> <p><b>2. BACKGROUND</b></p> <p>The South African National Accreditation System (SANAS) is the sole national body responsible for carrying out accreditations in respect of conformity assessment, which includes the accreditation of calibration, testing and verification laboratories, certification bodies, inspection bodies, verification agencies and any other type of body that may be added to its scope of activity. SANAS is also the national body to monitor Good Laboratory Practice (GLP) compliance with principles adopted by the Organisation for Economic Cooperation and Development (OECD) for GLP facilities.</p> <p>1 The Accreditation for Conformity Assessment, Calibration and Good Laboratory Practice, Act No. 19 of 2006, recognises SANAS as the only National Accreditation Body for the Republic of South Africa for conformity assessment, calibration, monitoring of Good Laboratory Practice, and to provide for matters connected therewith.</p> <p>SANAS is a Section 3A Public Entity for purposes of the Public Finance Management Act (PFMA), 1999 (Act No. 1 of 1999) (as amended by Act No. 29 of 1999).</p> <p>SANAS business involves SANAS staff working remotely from home to perform their work. This remote work needs SANAS staff using Laptops to connect through a Virtual Private Network (VPN) to the Office. Our VPNs are terminated on Sophos Firewalls. The office IT Systems runs on Microsoft Windows Server version 2016 with Sophos Anti-Virus. Staff mobile Laptops run Microsoft Windows 10, with Sophos Anti-Virus without any other Mobile Extended/Advanced Detection features, except the malware detection and protection features. Our server farm is hosted on-premises, on 2 physical servers and virtualised into over 20 Virtual Servers. SANAS has fully managed Warm-site IT Disaster Recovery Solution hosted off-premises cloud solution so consider SANAS working during a</p>		1 Service provider

disaster and how this protection is transferred rapidly. Our MS Office365 Mail System is hosted in the cloud protected by Mimecast Mail Protection Service.

### 3. OBJECTIVES

The goal of this exercise is to solicit a proposal for a solution that will offer User, Endpoint, Host, Server, Application, and Network protection. A solution may comprise various systems to form a comprehensive proposal for the protection of our servers, network, desktops, laptops, and email system, and not limited to:

- a) To protect SANAS Data, Information, and Information Systems On-Premises and Cloud based MS Office365 Email System.
- b) To ensure SANAS Servers, Mobile Devices, Desktops, Network, and applications such Office 365 are monitored for threats.
- c) To create an IT security alert system that will detect any unauthorized actions on Data and Information Systems in SANAS.
- d) To identify and recommend safeguards, suited to SANAS' environment, with the aim to strengthen the level of protection of SANAS' Data and Information Systems.
- e) To prevent threats to users such as ransomware, phishing, and account takeovers on our email systems.
- f) To provide threat monitoring of our IT Systems, Emails, User activity, File and Records in our environment.
- g) To ensure all types of threats are detected, monitored, and responded to 24/7 with minimal staff intervention.

### 4. SCOPE, APPROACH AND METHODOLOGY

#### Scope of Services

SANAS desires to engage the services of a service provider who can combine systems to provide the following services sought, acknowledging that no one system can provide a combined service:

- a) **Secure Mail gateway Service:**
  - i. API Integration
  - ii. Identify threat bypassed and Interoperability with existing email security solution
  - iii. Security awareness and training with simulated phishing tests built-in
  - iv. Machine Learning/Artificial Intelligent Self-learning for Cloud Based MS O365
  - v. User Behavior analysis to identify malicious content and traffic
  - vi. Early warning threat intelligent
  - vii. Mobile Apps visibility to manage and monitor threats identified and responded
  - viii. Zero impact Integration on our existing email security system
  - ix. Compatible with an existing Mimecast Mail Protection System
- b) **Threat Detection and Response Service:**
  - i. 24/7 Threat Detection and Response Service
  - ii. Network Threats Detection and Response Service
  - iii. User Behavior and Threat Intelligence Analysis/Reporting
  - iv. Endpoint Protection and Visibility
  - v. Server Protection and Log Analysis
  - vi. Endpoint Device Control & remote management capabilities
  - vii. Vulnerability Management and Asset Inventory
  - viii. Cloud Security for MS Office365 Mail System

**5. REQUIREMENTS**

These are minimum requirements in our environment for the proposed system(s) to meet:

No	Description	Specification
1.	Number of Users	80
2.	No. of Virtual Servers	30
3.	Number of Email Accounts	120
4.	Server & Laptop Platforms	MS Windows Server 2016 and MS Windows 10
5.	Server(S) Infrastructure	MS Server 2016, Virtual Machines, 2 Physical Machines
6.	Number of Years on Contract Term	Three (3) Years
7.	Type of Deployment	Remote (SANAS Staff currently working remotely)
8.	Type of Email Systems	MS Office O365 (Cloud-based) No Exchange on-site

**6. ADDITIONAL NOTES**

- i. SANAS has just below 80 staff,
- ii. SANAS does not support tablets, hence, this RFQ excludes tablets at this stage.
- iii. SANAS can do with an onsite resource maybe during the installation and stabilization period, after that an on-call support system would suffice.
- iv. SANAS usually works on a minimum three (3) year contracts.
- v. SANAS has its offices in Equestria, Pretoria, South Africa.
- vi. Currently, SANAS is using Enterprise version of Sophos Intercept-X for its endpoint anti-virus protect for the next three (3) years.
- vii. All proposal submitted MUST have pricing in South African Rands (ZAR).
- viii. The bidder MUST name the systems that form part of the proposed solution.

<b>Expected date of delivery:</b>	November 2022
<b>Contract or once-off:</b>	36 months contract
<b>Technical / Mandatory requirements:</b>	As per the specification
<b>Other information:</b>	

**SECTION TO BE COMPLETED BY SUPPLIER****2. SUPPLIER DETAILS**

<b>Supplier name:</b>	
<b>CSD number:</b>	
<b>Contact person:</b>	
<b>Contact number:</b>	
<b>Email:</b>	
<b>VAT number (if applicable):</b>	
<b>Physical address:</b>	


### 3. SCM COMPLIANCE REQUIREMENTS (please tick)

Central Supplier Database Report or Summary	
Completed and signed SBD 4	
Completed and signed SBD 6.1	
Completed and signed SBD 8	N/A
Completed and signed SBD 9	N/A
Certified valid B-BBEE Certificate	

**Certified valid B-BBEE Certificate**

(Please note bidders will not be disqualified for not submitting a valid certified BBBEE certificate or a sworn affidavit but will lead to the service provider not being awarded preference (BEE) points where the preferential point system is applicable)

### EVALUATION PROCESS

All bids will be evaluated as follows:

• **The First stage**, bids will be evaluated first for Administrative requirements, Only bids that meet Administrative and Compliance requirements will be considered for further evaluation.

• **The second stage**, bids will be evaluated in terms of price and 80/20 preference point system for quotations above R30 000 and below R50 000 000.

### 4. QUOTATION TERMS & CONDITIONS:

1. Quote validity refers to calendar days
2. SANAS reserves the right to award to multiple suppliers.
3. SANAS reserves the right to increase or decrease quantities at the prices quoted.
4. SANAS reserves the right to cancel this request.
5. All goods/services must be quoted in Rand value.
6. SANAS reserves the right to negotiate with bidders.
7. All fields must be filled in / completed for this document to be accepted.
8. Failure to submit the quotation by the date and time stipulated will result in disqualification.
9. Payment will be made 30 days after delivery of goods of services.
10. THIS QUOTE DOES NOT CONSTITUTE AN ORDER

### 5. ACKNOWLEDGEMENT AND SUBMISSION:

I hereby acknowledge and accept the terms and conditions of this request for quotation:

Name: .....

Signature: .....

Date: .....

**Annexure A**-Pricing to be completed and submitted with your proposal.

No.	Description	Quantity Number of licences	Unit cost	VAT	Total	Year 1 monthly cost	Year 2 monthly cost	Year 3 monthly cost
1.	Threat Monitoring and Response Service (License Per User/device)	80						
2.	Secure Mail Gateway Service (License per email account)	120						
3.	Deployment of the two (02) systems/service	2(Once-off)				N/A	N/A	N/A
Total year 1+ Year 2 + Year 3 including VAT								