POLMED
OUR INVESTMENT OUR HEALTH OUR FUTURE

Address: Crestway Office Park, Block A, 20 Hotel Street, Persequor Park, Lynnwood, Pretoria, 0081
Postal Address: PO Box 14812, Hatfield, Pretoria, 0028
Tel: 0861 511 049 • **Website:** www.polmed.co.za

REQUEST FOR INFORMATION

RFI 01/2023 – INFORMATION REQUEST FOR CYBERSECURITY MANAGED SERVICES, CONTINUOUS VULNERABILITY ASSESSMENTS, PENETRATION TESTING AND AWARENESS TRAINING PROGRAMME.

RFI Number	**RFI01/2023**
Compulsory Briefing Session	**Yes - 20 January 2023**
Closing Date to Confirm Attendance of Briefing Session	18 January 2023
Venue of Briefing Session	**POLMED Virtual Platform**
Time of Briefing Session	10h00 a.m
Closing Date of the RFI	26 January 2023
Closing Time	12h00 pm
Response Address	procurement@polmed.co.za

TABLE OF CONTENTS

1. INTRODUCTION

The South African Police Service Medical Scheme (POLMED) is a closed medical scheme registered under the Medical Schemes Act (Act 131 of 1998) ("the MS Act").

The Scheme Rules and the MS Act regulate the duties and responsibilities of the Board of Trustees. The Board of Trustees must ensure the optimal operation of the Scheme to the members' benefit.

The annual report of POLMED is available on the website www.polmed.co.za. Refer to the POLMED website for further detail on the size and composition of the Scheme.

2. OVERVIEW OF THE RFI

2.1. Invitation to Service Providers

POLMED invites all interested parties to submit a written response to this Request for Information (RFI). This RFI strictly seeks to gain knowledge of services and supplies available with an estimate of their related costs. The RFI is not an intent, commitment, or promise to acquire services or solutions offered. Information submitted in response to this RFI will become the property of POLMED. POLMED is not obliged to contract or pay for any requested information, nor is it liable for any costs incurred by interested parties.

Interested parties should submit information on all components in Section 3 of this document.

2.2. Project Overview

The project seeks to provide the organisation with full-time proactive cybersecurity and vulnerability management services.

3. SCOPE OF WORK

The scope of this project is to provide proactive cyber security and vulnerability management services to the Scheme. The service provisioning should address and include the following:

a) Definition and implementation of Cybersecurity Framework

b) Definition and implementation of a Cybersecurity Strategy

c) Definition and implementation of Cyber Security Operating procedures and related policies

d) Implementation of a vulnerability management program and related solution

e) Conducting cyber security technical activities and user awareness training (i.e., penetration testing and vulnerability assessments).

4. PROCESS OF MARKET ENGAGEMENT

The engagement process is two-fold.

Stage 1: Industry Engagement to obtain Information (RFI)

This document represents the first stage which involves getting information from the market. Interested parties are requested to submit information in line with the scope of work contained in this document and the estimated prices.

Stage 2: Request for Proposals (RFP)

The second stage involves developing terms of reference/specifications with input from stage 1. The RFP would cover more detailed requirements involving solution options, pricing, BBBEE and negotiations. POLMED will only invite interested parties -who will respond to this Request for Information and are found to understand the scope of work- to submit proposals through a closed tender process.

The RFP process will ultimately lead to the appointment of a suitable service provider.

5. NO BINDING AGREEMENT

5.1. POLMED will not award any business to any interested parties out of this request for information.

5.2. Prices submitted with the request for information are for information only, and POLMED will not hold any interested parties to any submitted price.

5.3. POLMED reserves the right to contact individual interested parties to obtain further information, should this be deemed necessary. POLMED may use responses from this RFI to pre-screen interested parties for the RFP process.

6. RESERVATION OF RIGHTS

Please note that POLMED reserves the right, at its sole discretion, to:

6.1. Reject all submissions that do not respond to critical aspects of the requirements set out in this RFI.

6.2. Not to proceed with the RFP process, post the RFI process.

7. CONTACT DETAILS

7.1. POLMED requires interested persons to send all RFI-related inquiries in writing to the POLMED central email, i.e. procurement@polmed.co.za, using the RFI reference number in the email subject.

7.2. Interested parties must refrain from contacting any of the POLMED personnel regarding this RFI unless they make use of the email provided in paragraph 7.1 or such other email as POLMED may designate.

7.3. POLMED will respond to interested persons' requests for clarification and or additional information by the close of business on the date specified on the cover page.

8. BRIEFING SESSION

8.1. Service Providers are required to attend the compulsory briefing session.

8.2. Interested parties who wish to attend the briefing session must submit their emails to the designated email address **two (2) working days** before the briefing session date so they can receive the link to join the briefing session through Microsoft Teams.

9. SUBMISSION OF REQUESTS FOR INFORMATION

All submissions in response to this request for information must reach POLMED on the date and time indicated in the document.

10. LATE RESPONSES

Response to the RFI is late if POLMED receives it after the closing date and time indicated on the cover page; and will not be accepted.

11. PRICING

Interested parties must note the following regarding pricing:

- The pricing must include all costs;
- Please provide pricing Inclusive and Exclusive of VAT;

- Any other conditions

12. REQUIRED DOCUMENTATION

Interested parties must submit the following information, together with the response to the RFI:

- Valid BBBEE Certificate
- Valid Tax Clearance Certificate
- Company Registration documents/Company profile

13. POLMED ENVIRONMENT

POLMED is modernising its Information Technology (IT) and Operational Technology (OT) infrastructures. To that end, POLMED seeks to deploy the latest technologies, capabilities, and personnel to ensure a reliable, secure, and sustainable environment.

Cybersecurity is a cornerstone of a fortified and agile IT/OT environment that ensures that POLMED is compliant with the requirements set by the following:

- Protection of Personal Information Act, 2013 (Act No 4 of 2013) (“PoPIA”).
- Information Security Management Systems - International Standardisation Organisation (ISO) 27001: 2015 to 2022 (“ISO27001:2015 to 2022”).

POLMED will deploy its cybersecurity structure within the internationally recognised foundation of:

- National Institute of Standards and Technology (“NIST”)
- Open Web Application Security Project (“OWASP”)
- SysAdmin, Audit, Network, and Security (“SANS”)

- MITRE Adversarial Tactics, Techniques and Common Knowledge ("MITRE ATT&CK")

14. SCOPE OF WORK

The Scope of Work is set into three (3) Categories

14.1 MANAGED SERVICES (CATEGORY 1)

14.1.1.	Understanding of the Actual IT/OT infrastructures of POLMED by performing a thorough audit and creating a detailed topology covering the entire IT/OT environment. The final Topology of the Actual IT/OT environment should mainly include the following: - Human Resources (and their skills) - Hardware - Clouds - Software - Running Services - Related Suppliers/Vendors - Governance Documentation and Implemented Policies Provide user training targeting technical and non-technical staff. Cybersecurity awareness plan.
14.1.2.	Assess the topology to identify technical, logical, and operational issues and highlight misconfigurations, vulnerabilities, and risks by priority. Additional Expectations from the Assessment: (a) What must be protected (b) Understand risk appetite and thresholds (c) Understand the threat landscape (d) Understand cybersecurity maturity levels

14.1.3.	Document the governance framework that includes policies and standards that comply with the following: (a) The *Constitution of the Republic of South Africa ("the Constitution")*; (b) The *Medical Schemes Act, 1998* (Act No 131 of 1998) ("*the MS Act*") (c) The *National Health Act, 2003* (Act No 61 of 2003) ("*the NH Act")* (d) *PoPIA* (e) King Report and King Code on Corporate Governance ("the King V Code") (f) Control Objectives for Information and Related Technology ("Cobit 5") (g) ISO 27001, 27002, 27017 and 27018; and (h) Other best practices, methodologies, and frameworks Develop and continuously improve the- (a) Cybersecurity Strategy Plan, (b) Policy and Standard Operating Procedures, and (c) Review change-management policy.
14.1.4.	Deploy and Manage a Zero-Trust Environment.
14.1.5.	Upgrade, Deploy and Monitor: (a) Security Operations Centre ("SOC") with capabilities of continuously assessing the security posture, detecting misconfigurations, and enforcing security best practices and compliance frameworks (b) Network Firewalls (c) Web Application Firewalls (d) Cloud Security Solutions (e) Active Directory Security (f) End-point detection response ("EDR")/ extended detection response ("XDR") (g) Digital Forensics and Incident Response (h) Disaster Recovery Infrastructure (i) Vulnerability Management Infrastructure (External/Internal) (j) And other required security solutions and strategies (if applicable after the Final Topology Assessment)

14.1.6.	Implement, Improve and Monitor an Awareness Training Programme for the Entire Personnel of POLMED. The Awareness Training Programme should include Phishing campaigns and Real-Life Attacks that could potentially impact POLMED IT/OT Infrastructures through Human Vulnerabilities. POLMED Personnel should be scored according to their commitment to the Awareness Programme and given access to an easy-to-use yet user-friendly User Interface for Training sessions.

14.2 PENETRATION TESTS AND VULNERABILITY ASSESSMENTS (CATEGORY 2)

14.2.1.	Continuous Internal and External Vulnerability Assessments. **Targets:** (a) Web Applications (Internet Protocol (IP) Address and fully qualified domain name ("FQDN")) (b) Application Programming Interface ("API") (IP Address and FQDN) (c) Networks (IP Address and FQDN) (d) Servers/Endpoints (IP Address and FQDN) (e) Internet of Things ("IoT") (IP Address) (f) Mobile Devices
14.2.2.	Continuous Internal and External Penetration Tests. **Targets:** (a) Web Applications (IP Address and ADNFQDN) (b) API (IP Address and FQDN) (c) Voice over Internet Protocol ("VoIP") (IP Address and AND/FQDN) (d) Wireless (e) Networks (IP Address and ADN/FQDN) (f) Servers/Endpoints (IP Address and AND/FQDN) (g) IoT (IP Address)

14.3 SCOPE OF WORK KEY EXPECTATIONS (CATEGORY 3)

(a) Define Clear Boundaries

(b) Deter Insider Threats

(c) Security Awareness Training

(d) Network Segmentation

(e) Vulnerability Management and Remediation

(f) Security and Privacy by Design

(g) Review the Latest Cybersecurity Cases

(h) Data Mapping

15. MANAGED SERVICES AND TECHNICAL REQUIREMENTS

15.1.	Interested persons must have accreditation for product supply and service delivery (as applicable), where the solution must be delivered/installed.
15.2.	Interested persons must be accredited by OEM to supply the specific products proposed in the RFI.
15.3.	The proposed solution must be capable of monitoring the health of the solution/device and providing detailed reporting on performance and utilisation.
15.4.	The solution response must include technical details on the offered solution and a complete configuration report from the OEM (i.e. the output from the OEM's system configuration tool) to ensure that the response includes all required components.
15.5.	Products and Certifications: (a) Check Point Software (b) Tenable One Software (c) Veeam Software (d) Cloud Service Certifications (e) CybeReady

16. PENETRATION TESTING TECHNICAL REQUIREMENTS

16.1.	Certifications: (a) Offensive Security Certified Professional (“OSCP”) (b) Certified Ethical Hacker (“CEH”) (c) Global Information Assurance Certificate (“GIAC”) (d) Certified Information Security Systems Professional (“CISSP”)
16.2.	Interested persons should provide at least eight (8) letters of recommendation from clients satisfied with a Penetration Testing Service.
16.3.	Interested persons should provide at least five (5) CVs of cybersecurity experts with the listed certifications as in **Section 16.1.**

17. VULNERABILITY ASSESSMENT AND MANAGEMENT TECHNICAL REQUIREMENTS

17.1.	Interested parties must be accredited for product supply and service delivery (as applicable) in the area where the solution must be delivered/installed.
17.2.	Interested parties must have partner accreditation by OEM to supply the specific products proposed in the RFI.
17.3.	The proposed solution must be capable of monitoring the health of the solution/device and providing detailed reporting on performance and utilisation.
17.4.	The solution response must include technical details on the offered solution and a complete configuration report from the OEM (i.e. the output from the OEM’s system configuration tool) to ensure that the response includes all required components.
17.5.	Products and Certifications: (a) Tenable IO (b) Tenable AD (c) Tenable CS (d) Tenable SC (e) Tenable OT (f) Tenable Lumin