TERMS OF REFERENCE (TOR)
CYBER THREAT DETECTION, THREAT HUNT SOLUTION AND PATCH MANAGEMENT-INSTALLATION, CONFIGURATION AND MAINTENANCE

1. PURPOSE

1.1. The Pan South African Language Board (PanSALB) seeks to appoint a suitably qualified service provider for the provision of **Cyber Threat Detection**, **Threat Hunt Monitoring** and **Patch Management Solution**.

1.2. The project has a requirement and responsibility to review and enhance its cybersecurity capability, response and readiness through detection and threat hunting tactical capabilities.

1.3. It is to deliver comprehensive cyber threat detection and cyber threat hunt solutions to assist in the capacitation of the environment, to provide continuous and on demand ICT Security Information and Event Management (SIEM) services.

2. BUSINESS OBJECTIVES

2.1. PanSALB is on a significant growth path, as the organization grows; it is looking at streamlining its processes and enabling itself for a high-rate growth.

2.2. Information Security has been identified as one of the critical functions that will assist the business to meet its objectives.

2.3. The information security services will ensure tat controls are embedded in the systems when executing daily operational functions and during project planning, designing, testing and execution.

2.4. This is critical especially taking into consideration business projects such as cloud services, unified communications, stabilizing of the SAGE environment, website etc. PanSALB has ten (10) offices nationally.

2.5. One of the main objectives of PanSALB is to ensure that the information security approach is structured, well designed, planned, aligned with business objectives, and executed properly.

3. SCOPE OF WORK

3.1. The successful service provider will be responsible for assisting PanSALB to implement Information Security Operations, Installation, Configuration, and training after implementation.

3.2. The successful service provider will be required to provide security as a service by implementing Security Information and Event Management (SIEM) that would be beneficial for the organization which covers the following areas:

- **Anti-Virus** – monitoring PanSALB's current Anti-Virus

- **Patch Management** – Monitoring PanSALB's current patch management software
- **Vulnerability Management –** Assist with network penetration test and vulnerability assessment and implement relevant remedial actions.
- **Email Security** – Monitoring of the accesses and contents of all mailboxes or accounts, this includes ant-phishing, data loss prevention, malicious email, anti-spam, threat visibility and response.
- **Firewall Management –** Interrogate reports and provide recommendations for access to web content.
- **Intrusion Detection and Prevention System (IDS/IPS)** – monitor and make recommendations on reports received for Intrusion detection and prevention.
- **Real Time Threat Analysis –** Analyse reports received from real-time visibility into the organization's posture.
- **Web security –** Analyse and provide recommendations ensuring confidential information that is stored online is protected from unauthorized access and modification.
- **Application Security –** Improve the security applications by finding and preventing security vulnerabilities.
- **Identity and Access Management –** Ensure that users have access to authorized resources, access is appropriate, and access is used appropriately.
- **Security Incident Management and Response –** Security Incident response plan includes support after implementation.

3.3. **Skills transfer – the successful service provider will be expected to transfer skills to PanSALB's ICT team.**

3.4. PanSALB uses Microsoft Platforms (Windows 10 & Microsoft 365) and has Fortinet Firewall.

4. DELIVERABLES

4.1. Service provider or cyber security vendor is required to deliver a successful implementation within a stipulated project plan due to the need for immediate interoperability between the key deliverables that will provide the maximum impact at the earliest opportunity.

4.2. Service provider or cyber security vendor must demonstrate the ability to implement, maintain and support the solution and must provide a reference/s of where the solution is deployed.

4.3. Where the service provider is not the OEM, a requirement to provide OEM details and assurance (verifiable proof) from the OEM as the capable and reputable reseller to provide maintenance, support, and OEM training.

4.4. The service provider must provide **A VALID OEM AUTHORIZATION CERTIFICATE** that includes licensing, installation, configuration, building of rules and optimization with preferably the highest level of product support given by OEM to the service provider.

4.5. Thread detection and threat hunting: provide solutions that are aligned with market related business requirements and best practices in cyber threat detection and threat hunting, response capabilities and processes, preferably Fortinet SIEM.

4.6. The cyber threat detection and threat hunting service provider should be able to work alongside the tactical cyber threat intelligence to deliver enhanced, proactive threat detection and threat hunting options.

4.7. Training: Provide an appropriate package of dedicated training to enable the project team to optimally derive value out of the required tools. The successful vendor should also clearly demonstrate a plan to mature and transfer Mission-critical skills and capabilities to the project team.

4.8. A proven market leader in local and global cyber threat detection and threat hunting tools and technologies implementation, support, and maintenance. The service provider must possess technical expertise, skills, and experience of minimum of 3 years on the solution.

Service Response Priority Levels:

Priority 1	**Priority 2**	**Priority 3**	**Priority 4**
Response Time – 2 Hours	Response Time – 4 Hours	Response Time – 1 Business Day	Response Time – 2 Business Days
Any failure of the system resulting in a critical impact on business operations.	Total failure of a system resulting in serious but non-critical impact on business operations, Or, Partial failure of a system causing large numbers of users to be unable to function thereby causing serious but non-critical impact on business operations.	Failure of a system resulting in slight impact on business operations, Or, Partial failure of system either causing large numbers of users to be slightly hindered or a small number of users to be seriously impacted with slight impact on business operations.	Low level fault to one or more users not affecting business operations.

REQUIRED INFORMATION

The service provider is required to demonstrate that they have resources and adequate experience in similar projects.

This experience must include but not limited to:

- Experience in Information Security and Data Protection.
- Experience in an ICT Environment.
- Analytical skills (experience in security monitoring and reporting)
- Knowledge and understanding of NIST, OWASP, ISO 27000, POPIA, COBIT, ITIL
- Skills in Network Security, Web Security, Application Security, Database Security and Security Operations