

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

Description of Request	Domain Name System (DNS) Security Managed Services for a period of (5) five years. (1 year implementation and 4 years Maintenance and Support)
-------------------------------	--

1. High level background

Domain Name System (DNS) and is the standard communication protocol on the internet. It is an Internet protocol that converts human-readable names to IP addresses, changes IP addresses back to names, and provides easy-to-remember names for many Internet-based services, such as e-mail.

The DNS system consists of multiple interconnected and hierarchical DNS servers that work together to ensure reliable and efficient name resolution. DNS queries and responses exchanged between devices across a network are known as DNS logs and contain valuable information such as the requested domain name, source IP address, the type of query, and the timestamp from DNS servers.

DNS Security is a set of security extensions that use cryptographic digital signatures to validate DNS queries before returning them to the client device, ensuring their authenticity and integrity.

The wealth of data embedded in DNS logs is the primary reason that lures cybercriminals to DNS, who use it to exfiltrate sensitive data. Another factor is the wide attack surface that DNS provides. DNS is a distributed system containing numerous components, each presenting malicious actors with potential and unique attack vectors to exploit.

DNS interacts with internet traffic before other security measures, forming a comprehensive dome for the entire network. Comparing findings from DNS layer implementations with latter security controls can reveal potential gaps. Which can then be addressed before they are exploited. This method reveals hidden gaps due to overlapping controls. It elevates the overall security status by complementing the existing policies.

1.1. Why is DNS security important?

Like many Internet protocols, the DNS system was not designed with security in mind and contains several design limitations. These limitations, combined with advances in technology, make DNS servers vulnerable to a broad spectrum of attacks, including spoofing, amplification, DoS (Denial of Service), or the interception of private personal information. And since DNS is an integral part of most Internet requests, it can be a prime target for attacks.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

In addition, DNS attacks are frequently deployed in conjunction with other cyberattacks to distract security teams from the true target. An organization needs to be able to quickly mitigate DNS attacks so that they are not too busy to handle simultaneous attacks through other vectors.

1.2. Commonly known attacks on the DNS protocol

- **DNS Spoofing:** Also known as DNS Cache Poisoning, this is a type of cyberattack where a piece of DNS server data is altered to redirect users to fake websites. This is done by attackers sending forged DNS responses to a DNS resolver or server. These fraudulent responses contain information that maps the requested domain to a false IP address, thus directing users to malicious websites or servers.
- **DNS Hijacking:** Also known as DNS Redirection, it refers to a form of attack where the DNS settings of a domain name are manipulated in such a way that redirects legitimate DNS queries to a destination of the attacker's choice.
- **DNS Tunnelling:** In this type of attack, malicious codes or programmes are encapsulated into DNS queries and responses to bypass firewalls and other security measures. The
- **Phishing:** DNS security solutions can help to block phishing websites and prevent users from falling victim to these scams.
- **Phantom Domain Attack:** Forcing the DNS resolver to wait for a response from non-existent domains, which in turn leads to poor performance.
- **Random Subdomain Attack:** Compromised hosts and botnets that essentially are DOSing a legit domain, but focusing its fire on false subdomains to force the DNS record lookups and override the service
- **Botnet-based CPE (Customer Premise Equipment) Attack:** These attacks are carried out using CPE devices; this is hardware given out by service providers for use by their customers, such as modems, routers, cable boxes, etc.). The attackers compromise the CPEs and the devices become part of a botnet, used to perform random subdomain attacks against one site or domain.
- **Malware Domain Generation Algorithm (DGA) protection**

1.3. Mitigating DNS-based threats

DNS attacks can be restrained with the right security measures in place. Some common approaches to mitigating DNS-backed threats include:

- **DNSSEC (DNS Security Extensions):** DNSSEC is a set of security extensions that use cryptographic digital signatures to validate DNS queries before returning them to the client device, ensuring their authenticity and integrity.
- **DNS Filtering:** It refers to the practice of blocking access to selected websites and services deemed malicious or unwanted at the DNS level. This is typically done by comparing a DNS query with an in-built or customised set of blacklisted domains or IP addresses. If there is a match, the domain will not be resolved, and access prevented.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

- **DNS over HTTPS (DoH):** It is a protocol that allows secure communication between DNS clients and servers by encrypting DNS queries and responses. DoH uses port 443, the standard HTTPS port, to embed DNS traffic within other HTTPS traffic, thus ensuring that DNS traffic is not tampered with.
- **Multi-Factor Authentication (MFA):** It is a security measure that allows users to verify their identity using more than the traditional username-password combination. MFA is especially critical to implement as it prevents networks and equipment from being compromised even if malicious actors manage to hack the associated usernames and passwords.
- **Threat Intelligence Feed (TIF):** A TIF is a continuous stream of up-to-date data on emerging threats that can adversely affect network security. By deploying a TIF in their armoury, organisations can promptly detect vulnerabilities and enhance their cybersecurity defences.
- **Malware Domain Generation Algorithm (DGA) protection**
- **Leverages machine learning or other heuristics to augment threat feeds**
- **Deploys across hybrid architectures**
- **Ability to prevent Typo squatting**

1.4. Benefits of using a DNS Security Suite

- **Improved security:** DNS Security Suites can assist to defend organizations against a number of DNS threats, such as DNS poisoning, DNS tunnelling, phishing, and malware.
- **Reduced risk:** DNS Security Suites can help minimize your organization's risk of data breaches, financial losses, and reputational harm by mitigating DNS risks.
- **Improved compliance:** DNS Security Suites can assist your firm in complying with industry requirements and standards.
- **Increased visibility and control:** DNS Security Suites may give enterprises insight into their DNS traffic as well as control over which websites and domains individuals can access.

The Domain Name System Security Extensions (DNSSEC) is a suite of extension specifications by the Internet Engineering Task Force (IETF) for securing data exchanged in the Domain Name System (DNS) in Internet Protocol (IP) networks. The protocol provides cryptographic authentication of data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

2. Scope of work

These business scope requirements aim to ensure that the DNS security suite provides comprehensive advanced protection against DNS attacks, enables efficient DNS traffic management, and integrates seamlessly with existing information security ecosystem.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

The required managed services solution should be based on purpose-built hardware to provide the most robust, scalable, and integrated controls for network DNS security services available in the market today. These services, including DNS, DNSSEC, DHCP, FTP, TFTP, HTTP, HTTPS and NTP, are critical to supporting various network devices leveraging real-time database that is managed centrally using the IP Address Management service. The managed service will require also a dedicated project manager for implementation phase.

NB: The scoping of the device/ system will have to take into consideration that Eskom require two devices or system which one will be placed at megawatt park data centre and another at teraco data centre.

The envisaged managed services should be designed, sized and implemented to fulfil the below requirements:

1. The envisaged solution service should offer DNS Firewall capabilities to protect against DNS Malware.
2. The envisaged solution service should provide Hardware High Availability (HA) for all enabled services.
3. The envisaged solution service should provide Protocol HA including DHCP fail over protection, DNS, TFTP/HTTP, NTP, Syslog and other enabled services.
4. The envisaged solution service should offer Geographical Redundancy across both Data centre (DC) and Disaster Recovery (DR).
5. The envisaged solution service should be in compliance with DNSSEC and IPv6.
6. The envisaged solution service must offer Network Discovery for L2/L3 devices and connected endpoints.
7. The envisaged solution service should support Network Configuration Changes and Management Automation.
8. The envisaged solution service should be able to provide Network Policies and Compliance Enforcement.
9. The envisage solution should have a fail-safe architecture. This includes providing a robust and secure by design architecture.
10. The envisaged solution service must be able to provide integrated DNS Traffic Control capabilities to load balance traffic across multiple datacentres.
11. Real-time threat detection through DNS query analysis.
12. DNS Traffic Behaviour and anomaly detection.
13. Access Guard reporting to evaluate firewall, proxy and DNS Security performance including but not limited to showing malicious traffic blocked or missed by security control services.
14. One-click infected device identification passing through the DNS.
15. Real time visibility on DNS Security layer with the following details MAC address, username, Source IP, Device name and Host Name.
16. Agentless DNS log Collection with a minimum 1- year log retention for auditing and investigations including a 1-year real time search capabilities.
17. One-premise deployment with full administrative control.
18. DNS-level infected device detection (root cause). The solution should must apply automation to find and contain infected files and devices as quickly as possible.
19. The on-premise DNS security solution must be capable of integrating seamlessly with existing firewall, proxy, and NDR. It should offer out-of-the box integration capabilities to ensure efficient deployment and interoperability.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

20. Security layer detection of domains accessed for the first time within the organization on DNS layer (firstly seen domain detection).
21. On-Premises Solution (Reporting, which is to happen daily, weekly, and monthly) Delivers full visibility and compliance-friendly DNS logging for organizations with regulatory requirements.
22. AV-Test (AV-TEST is an independent organization which evaluates and rates antivirus and security suite software for Microsoft Windows, macOS and Android operating systems, according to a variety of criteria.) Compliance to meet the requirement of achieving an 80% or higher success rate in the DNS Security category as evaluated by AV-Test within the last three years, the product must demonstrate consistent performance in several key areas:
 - a. Threat Detection: The product should successfully identify a wide range of DNS-based threats, including phishing domains, malware sites, and other malicious URLs. This detection capability should be evaluated over multiple test periods by AV-Test to ensure reliability. It should be able to detect and drop DNS based attack queries before they reach the core DNS server.
 - b. Blocking Efficiency: In addition to detection, the product must block access to harmful domains effectively, preventing user interaction or device compromise. This blocking should cover a range of threat vectors such as DNS tunnelling, Command and Control (C2) server communications, and domain-based malware. It should be able to predict and analyze the disruptive attacks that use DNS for command-and-control and for data theft and also able to neutralize threat hidden in the DNS Tunneling.
 - c. Industry Benchmarking: The product must maintain or exceed industry benchmarks in independent testing conducted by AV-Test over the last two years. These benchmarks would include detection rates, false positive rates, and overall blocking effectiveness.
 - d. Efficacy Reporting: The product's performance must be verifiable through published AV-Test results, showing at least 80% success rate in all DNS Security test reports conducted within the last three years.
23. Compliance with Industry Standards ((System and Organization Controls 2) SOC 2) Ensures that DNS security controls meet SOC 2 compliance requirements for data protection and privacy.
24. Ruleset-Based Policy Management
 - a. Protective DNS Security allows the creation of advanced, customizable rulesets based on multiple criteria, enabling fine-tuned control over DNS filtering and protection. The ruleset can be customized using the following parameters:
 - b. Category: Grouping domains or IP addresses based on content or threat categories.
 - c. Client IP: Filtering based on specific client IP addresses.
 - d. CNAME & CNAME Domain: Blocking based on Canonical Name records and their associated domains.
 - e. CNAME TLD: Filtering by Top-Level Domains associated with CNAMEs.
 - f. CVE: Integrating threat intelligence related to specific vulnerabilities (Common Vulnerabilities and Exposures).
 - g. Device Name: Creating rules based on specific device identities.
 - h. DoH & DOT: Support for DNS over HTTPS and DNS over TLS for encrypted DNS resolution.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

- i. Domain & Domain Age: Filtering domains based on name and age (e.g., newly registered domains).
- j. Domain Classification: The solution should be able to classify domains based on content, security level and report unclassified domains. The classification should be automated and occur within a very short space of time, i.e. less than 15 minutes.
- k. Domain TLD: Blocking by Top-Level Domains (e.g., .com, .net, .org).
- l. FQDN (Fully Qualified Domain Name): Rules based on exact domain names.
- m. IP & IP Country: Filtering based on specific IP addresses or countries.
- n. Nameserver, Nameserver Domain, Nameserver IP, Nameserver IP Country, Nameserver TLD: Creating policies that target specific nameserver attributes.
- o. Open Port: Blocking based on specific port usage in DNS queries.
- p. Proxy IP: Blocking domains or queries originating from proxy IPs.
- q. Query Type: Filtering based on DNS query types (A, AAAA, MX, etc.).
- r. Domain Registrar: Filtering based on the registrar information of the domain.
- s. Status: Applying rules based on DNS response status.
- t. Username: User-based filtering, allowing rules to be applied based on authenticated users.

The following capabilities are required by DNS Security Solution but not limited to:

- a. **Compatibility** – The DNS security suite should be compatible with a wide range of operating systems, including Windows, macOS, Linux, and mobile platforms such as iOS and Android.
- b. **Protection against DNS attacks** – End-user detection capabilities should be included in the suite to avoid various sorts of DNS attacks, such as DNS hijacking, DNS spoofing, and DNS cache poisoning. These capabilities should be equipped with detecting and blocking malicious DNS requests, as well as providing real-time monitoring and notifications for odd DNS behavior including malicious domains without IP address. This means that it should be able identify and protect against newly emerging malware (i.e., zero-day attacks) and security vulnerabilities that have not yet been detected by traditional security solutions.
- c. **DNS filtering and content blocking** – To restrict access to harmful or unsuitable websites, the suite should be able to monitor and filter DNS queries. Businesses should be able to construct and maintain bespoke blacklists and whitelists, as well as restrict certain categories of websites based on content or reputation, with this capability. The suite should enable customizable web filtering features, allowing block access to specific categories of websites or content. This helps enforce acceptable use policies, prevent access to inappropriate or non-work-related websites, and protect against phishing and other web-based attacks.
- d. **DNS traffic analysis** – The suite should include in-depth analysis of DNS traffic data, such as logs, requests, and responses. This capability should enable enterprises to detect trends and abnormalities in DNS traffic, which will aid in troubleshooting and recognizing possible security concerns.
- e. **DNS encryption** – To encrypt DNS communication and defend against eavesdropping and man-in-the-middle attacks, the suite should implement the DNS over HTTPS (DoH) or DNS over TLS (DoT) protocols. Solution should be able to detect invisible traffic with ability to identify the source of malicious DNS traffic.
- f. **Reports and analytics** – The suite should include comprehensive data and visualizations on DNS security events such as DNS assaults, banned requests,

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

and DNS traffic patterns. These reports should be able to be tweaked and exported for more investigation and auditing. This helps gain insights into their network's security posture, identify potential vulnerabilities, and make informed decisions to improve their overall security strategy. Reporting should leverage the DNS platforms to provide long-term network reporting, trending, and tracking. Instead of manually cobbling together reports one-by-one, Reporting should provide pre-built reports for easier administration and robust monitoring. It should offer centralized reporting capability in order to provide visibility and to enable different teams to easily diagnose a problem/s happening across they system.

- g. **Integration with existing security services** – The suite should be able to integrate with existing security tools and infrastructure, such as firewalls, intrusion prevention systems (IPS), AI Threat detection systems/ solutions, next generation firewalls, and Security Information and Event Management (SIEM) systems. This integration should allow for seamless sharing of DNS security information and enable better overall security management. This allows for a more robust and coordinated security approach, leveraging the strengths of multiple security tools. Bidirectional XDR Integration Enhances endpoint detection and response (XDR) solutions by correlating DNS data with endpoint activity. The proposed service should have the capability to integrate with AI threat detection services through bidirectional data sharing supporting open architecture methodology like API. For encrypted traffic the service should be able to share keys to other deployed solution in the estate for visibility, collaboration and complementing each other. The service should have integration or data sharing capability to other or leading Enterprise DNS service solutions in the market.
- h. **Scalability, flexible, and performance** – The suite should be able to handle high volumes of DNS traffic and provide fast and efficient DNS resolution without impacting network performance. It should also be scalable to accommodate growing network environments and support large enterprises with multiple DNS servers. It should offer flexible deployment options, including on-premises, cloud-based, or hybrid solutions, allowing choice on the deployment model that best suits their requirements.
- i. **Ease of deployment and management** – The suite should be easy to deploy and manage, with a user-friendly interface and centralized management console. It should support remote management and allow administrators to easily configure and monitor DNS security policies and settings. The service should be easy to customizable.
- j. **Automatic threat remediation** – The suite should not only identify and blocks malicious domains and IP addresses but also automatically takes remediation actions to protect the network. This can include blocking suspicious DNS requests, quarantining infected devices, or notifying security teams for further investigation and response. Active Directory User Name, Hostname and mac address should be added to the report instead of using a variable IP Address.
- k. **Data exfiltration prevention** – The suite should monitor DNS traffic for signs of data exfiltration attempts. It can detect and block unauthorized attempts to transfer sensitive data out of the organization, helping to prevent data breaches and protect against insider threats. Automatic detection and blocking of data exfiltration should be in real time.
- l. **Minimizes Business and Legal Exposure** – DNS security suite combats malware and APTs and prevents data theft, providing maximum protection for users from becoming infected when they go to a malware website or click on a malicious link.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

Furthermore, hijacked DNS command and control requests are not executed, preventing botnets from operating. Lastly, all malware activities are logged and reported to pinpoint infected clients and attacks.

Web presence and web applications infrastructure need a robust network fabric to deliver the high performance that drives both internal and external customer satisfaction, especially where revenue-generating services are concerned, such as web presence, e-commerce sites, customer-facing portals, or internal business-critical applications.

Solution Service IPAM Capability

The proposed solution service must cover an enterprise-grade IP Address Management (IPAM) solution. The service must support comprehensive IP address management and meet the current and future needs of a hybrid IT infrastructure that spans on-premises and multiple cloud environments.

The proposed IPAM solution should include, but not be limited to, the following features:

- a. **Comprehensive IPAM Functionality:** Centralized management of IP address space including automated IP address allocation, tracking, and auditing across all enterprise networks.
- b. **Cloud and Hybrid Environment Support:** Native or API-driven integrations with leading cloud providers (e.g., Microsoft Azure, Amazon Web Services, Google Cloud Platform) to enable IPAM visibility, management, and automation across hybrid cloud environments.
- c. **API and Automation Support:** Robust RESTful APIs and scripting capabilities for integration with existing network automation tools, orchestration platforms, and custom workflows.
- d. **Scalability and Performance:** Ability to scale efficiently for large IP address pools, supporting IPv4 and IPv6 address spaces, with high availability and performance.
- e. **Security and Compliance:** Role-based access controls, audit logging, and compliance reporting features to ensure secure and accountable IP address management.
- f. **Migration:** The vendor shall be responsible for the migration of the existing IPAM database from Cisco Prime Network Registrar to the new system, limited to IP address records and associated metadata, excluding DHCP and DNS data.
- g. **User Interface and Reporting:** Modern, user-friendly interface with customizable dashboards, reporting, and alerting to support proactive network management.
- h. **Vendor Support and Roadmap:** Commitment to ongoing product support, maintenance, and product roadmap aligned with emerging technologies and hybrid cloud trends.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

- i. **Integrated DNS and DHCP Management:** Seamless integration and automated management of DNS and DHCP services, either built-in or tightly integrated with major DNS/DHCP platforms.
- j. The solution service must have the following capabilities:
 - i. Must be able to import current Active Directory DNS or Integrate with Active Directory DNS
 - ii. DDNS – Dynamic DNS
 - iii. RPZ Zones - Response Policy Zones allows administrators to block or redirect malicious domain requests at the DNS level
 - iv. DNSSec - Domain Name System Security Extensions
 - v. DDOS Protection - helps prevent major disruptions like Distributed Denial of Service attack
 - vi. DNS Blacklist Feeds – Automatically load curated list of malicious Domain names
 - vii. Extensive Logging – Must support logging information to SIEM
 - viii. EDNS - Extension Mechanisms for DNS, is a specification that extends the capabilities of the traditional DNS protocol, most notably by allowing for larger DNS messages than the original 512-byte limit over UDP. This is crucial for modern internet applications, enabling larger responses needed for features like DNSSEC and allowing DNS servers to exchange more metadata

The following features must be available on the proposed solution:

- a. **Real-Time Threat Detection** – Detects malicious domains, phishing attempts, and other threats in real-time using AI-driven analytics and global intelligence feeds. Block potential exfiltration and identified malicious domains that are used to attack Eskom and blacklisted domains.
- b. **DNS Traffic Behaviour and Anomaly Detection** – Monitors DNS request patterns and identifies unusual behaviours that could indicate compromised devices or advanced persistent threats.
- c. **Continuous Security Gap Report** – Service should provide an in-depth analysis of existing security gaps in the DNS security service, enabling proactive risk mitigation.
- d. **One-Click Infected Device Detection** – Instantly identifies and isolates compromised devices within the network to prevent further damage.
- e. **Image-Based Anti-Phishing** – Uses advanced AI models to detect phishing attempts through image recognition and domain reputation analysis.
- f. **Crypto Mining Domain Classification** – Identifies and blocks DNS requests associated with crypto-jacking and unauthorized mining operations.
- g. **Global Threat Intelligence Feed** – Continuously updated database of known malicious domains and IPs sourced from a global network of threat analysts and partners.
- h. **Built-In Threat Intelligence** – Enhances threat detection by leveraging proprietary and open-source threat intelligence feeds.
- i. **Proactive Threat Hunting** – Provides security teams with advanced search capabilities to proactively hunt for emerging threats within the DNS layer.
- j. **Ease of Deployment** – Deployable as an on-premises, cloud, or hybrid solution with minimal configuration and fast integration. The service should support Multi-factor authentication.
- k. **Agent-less Deployment** – Offers flexible deployment options to support diverse IT environments without requiring endpoint installations.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

- l. **Roaming Clients for Off-Network Users** – Ensures DNS security and visibility for remote and roaming users outside corporate networks.
- m. **iOS & Android Support** – Extends DNS security protection to mobile devices, preventing phishing and malware infections on smartphones and tablets.
- n. **Cloud-Based Solution (Protection)** – Provides real-time cloud security for DNS traffic without requiring on-premises infrastructure.
- o. **On-Premises Solution (Reporting)** – Delivers full visibility and compliance-friendly DNS logging for organizations with regulatory requirements.
- p. **Bidirectional EDR Integration** – Enhances endpoint detection and response (EDR) solutions by correlating DNS data with endpoint activity.
- q. **SOAR & API Integration** – Automates threat response workflows by integrating with security orchestration, automation, and response (SOAR) platforms.
- r. **Content Filtering and Policy Management** – Enables organizations to enforce custom DNS policies for acceptable internet usage and security compliance.
- s. **Granular Rule Creation** – Allows detailed rule definitions to control access to specific domains, applications, and services.
- t. **Advanced Allow/Block List Management** – Provides dynamic and static allow/block lists to tailor security settings to organizational needs.
- u. **Dynamic Allow/Block Lists with URL Feeds** – Integrates with external URL threat feeds to automatically update filtering policies.
- v. **MSP-Friendly Architecture** – Designed for multi-tenant environments, allowing managed service providers (MSPs) to offer secure DNS services.
- w. **AV-Test Success Score** – Demonstrates strong performance in independent security assessments and AV tests.
- x. **Compliance with Industry Standards** – Ensures that DNS security controls meet best practice framework compliance requirements (IETF (RFCs 4033-4025, 6840, 6781) for data protection and privacy).

Therefore, Global server load balancing (GSLB) and DNS Traffic Control technology is required to protect services, share load between different sites, and to implement disaster recovery (DR) or remote failover arrangements.

3. Safety:

The resource will be required to work at Eskom Megawatt Park on ad-hoc basis and no requirement exist for any Eskom sites visits.

4. Training/Transfer of skills

- a. Provide onsite, classroom-based, and web-based training for end-users and system support staff on a pre-booked basis. The recommended method of training delivery would be required on implementation and, as per request in future. 10 x resources on the first year of implementation with hands on practical implementation.
- b. Mentor 10 x Eskom resources through the installation, configuration and deployment stages using a defined skills transfer program.
- c. The service provider will be required to train 10 x Eskom IT staff to provide first line support. This will be onsite training.
- d. Service provider to provide appropriate recognised certifications for the product (e.g. ISO/IEC 27001, SSAE16) and attestation reports if it's a cloud-based solution.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

- e. Expert level training with relevant certification 10 resources.

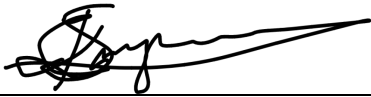
5. Service Level Agreement requirements

The Service Provider must provide **24/7/365** second- and third-line support with OEM. Comprehensive SLA shall be drafted or compiled with the successful supplier upon agreeing on the required SLA KPA and KPI including liabilities.

Service Level	Description	Escalation to SP	Escalation to OEM
Critical	Business has stopped	Response within 1 (one) hour – Level 1 Response within 3 (three) hours – Level 2	Response within 4 (four) hours
Major	Business severely impacted	Response within 1 (one) hour – Level 1 Response within 3 (three) hours – Level 2	Response within 4 (four) hours
Normal	Minor business impact / product failure	Response within 1 (one) business day – Level 1 Response within 2 (two) business days – Level 2	Response within 1 (one) business day
Low	No business impact but requires one or more updates	Response within 2 (two) business days – Level 1 Response within 2 (two) business days – Level 2	Response within 2 (two) business days
Informational	Request for information	Response within 3 (three) business days – Level 1 Response within 3 (three) business days – Level 2	Response within 3 (three) business days

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

6. Approvals:

End user / requestor:	Name:	CS Kungwane
	Designation:	Middle Manager information Security
	Date:	09 December 2025
	Signature:	
Senior Manager:	Name:	Sithembile Songo
	Designation:	Senior Manager Information Security
	Date:	09-12-2025
	Signature:	