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

Description of Request	The implementation of a Data Leakage Prevention solution as part of a cyber risk strategy to enable the protection of data at-rest and data in-transit across all Information Technology platforms.
-------------------------------	---

1. High level background

Eskom must implement a Data Leakage Prevention solution as part of its cyber risk strategy to enable the business to protect data at-rest and data in-transit across all Information Technology platforms. At present the business is at risk of suffering data leakage that could lead to reputational damage or a leakage in Intellectual Property data. The current tools employed in the organisation do not provide full capabilities to prevent data leakage from insider threat actors.

2. Scope of work/Business requirements


The implementation of a Data Leakage Prevention Solution

Deployment environments	<ul style="list-style-type: none"> The DLP solution must support different forms such as on-premises, cloud-based services, appliance and/or virtual appliance, hybrid and as add-ons in popular office applications. The DLP solution shall support mobile DLP functionality to monitor data on mobile devices and provide organisation wide DLP controls. The feature shall integrate with Eskom's Mobile Device Management and/or Mobile Application Management capabilities.
Supported platforms	<ul style="list-style-type: none"> Support for the following is required: Windows, MacOS, Linux, iOS, Android, and other emerging platforms such as Windows for ARM. The DLP solution shall integrate into Eskom's Cloud Access Security Broker as well as other popular broker platforms.

Data protection

- *“Data in use”* – Ability to assign management rights (manually or automatically) to files and data to specify what actions can and cannot be taken with them such as read-only, print controls, copy/paste actions as a minimum. The tool must be able to specify which device and protocols can be used to access sensitive data. The type and brand locking for authorised devices to access sensitive information must be possible.
- *“Data in motion”* – The DLP solution must implement web controls and be able to perform content inspection to prevent sensitive information from being sent through the web, email, blogs, social networks, and other communications channels including command line tools. The solution must be able to integrate with Eskom’s secure web gateway and email gateway to apply its protection policies. Further integration will be required into Eskom’s Zero trust Network Architecture and other security controls.
- *“Data at rest”* – The DLP solution must be able to perform data store scanning, fingerprint scanning and monitor all data regularly in accordance with Eskom’s policies.
- *Encryption* – The DLP solution must be able to perform encryption on documents through add-ons.
- The DLP solution shall have features to control slow leaking of information by monitoring multiple transfer instances of sensitive data using artificial intelligence capabilities.
- *Automated Discover and Classify Sensitive Data using Artificial Intelligence capabilities such as machine learning* – The DLP solution must be able to automatically discover and classify, using machine learning techniques, specific types of both structured and unstructured data as they are found, created, or modified using Eskom’s classification policy.
- *Monitor all Valuable Data* – The DLP solution must be able to track anytime sensitive data is accessed, moved, modified, or destroyed, administrators must have a record

	<p>of it, and receive real-time alerts when user activity deviates from a pre-established baseline.</p> <ul style="list-style-type: none"> • <i>Use of Automation through the use of Artificial Intelligence capabilities such as machine learning</i> – The DLP solution must use automation, using machine learning techniques, to detect and respond to anomalous activity, perform repetitive, time-consuming tasks, install updates, enforce policies. • <i>Data Privacy Regulations Compliance</i> – The DLP solution must help to comply with various data privacy regulations, such as, POPIA, GDPR, CCPA, HIPAA, or PCI DSS, by providing visibility into where sensitive data resides and how it's being used, and by enforcing policies and controls to prevent data loss
Centralised management	<ul style="list-style-type: none"> • The DLP solution shall provide an easy-to-use single pane management console used across all deployment form factors. • The DLP shall provide integration with Active Directory, LDAP, and other supported Identity Providers to help manage and enforce user policies. • Policy templates shall be built-in and easily customisable to implement industry regulation such as POPIA, PCI, GDPR, etc. • Employee alerts and self-remediation capabilities such as confirmations and justification of data policy breaches shall be configurable.
External business collaboration	<ul style="list-style-type: none"> • The DLP solution shall enable Eskom to share in a controlled manner documents with external business partners. • The DLP solution shall be able to revoke access to documents, even those that have an expiry date. The supported documents shall be native office files and PDFs as a minimum.
Training and support	<ul style="list-style-type: none"> • An online training platform and training documentation shall be made accessible for the use by Eskom for the following:

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

	<ul style="list-style-type: none"> ○ User Manuals ○ Administrator Manuals • The online training platform shall support a combination of video and static content to all Eskom users. • The online platform shall not require a license or subscription fee for each individual user at Eskom. • Support services shall be available across the solution's value chain. These shall be made available 24 hours/ 7 days a week.
--	--

2.1. Training/Transfer of skills:

Online training to be provided for the use of the tools that come with the solution.

3. Service Level Agreement requirements

The services Level Agreement shall be in accordance with Appendix 1 – Managed DLP Solution Service Level Agreement Final for the five-years duration of the contract.

4. Approvals:

End user / requestor:	Name:	Sibusiso Dlamini
	Designation:	Chief Engineer: Cyber Security
	Date:	11 September 2024
	Signature:	
Senior Manager:	Name:	Sithembile Songo
	Designation:	Senior Manager: Information Security
	Date:	11-09-2024
	Signature:	