Eskom	**Group IT Scope of Work** Request for Proposal (RFP) for a Cloud-Based Email Perimeter Threat Protection, Email Archiving and Email Journaling

1. Scope of work/Business requirements

The supplier is required to provide the following services:

a. Provision of a Cloud-Based Email Perimeter Threat Protection service that has the following capabilities but not limited to:

1. Email online defence
2. Advanced email threat defence
3. Built-in Intelligence for Targeted attacks
4. Predictive Analysis and Sandboxing
5. Internal Email defence (protecting against internal email threats)
6. Brand exploitation defence

b. Provision of an Internal Email Threat Protection service that has the following capabilities but not limited to:

1. Email online defence
2. Scanning of attachments and URLs for malware and malicious links
3. Detection of lateral movement of attacks via email from one internal user to another.
4. Automated remediation of infected or sensitive emails and attachments from employees' inboxes
5. Identification and blocking of threats or sensitive data attempting to leave an organization
6. Continuous monitoring and re-checking of the status of all previously delivered files with automated alerting and removal.

c. Provision of Cloud-Based Email Journaling service that has the following capabilities but not limited to:

1. Analytics based Email eDiscovery service
2. Email data governance and retention
3. Secure and easy access for investigations and data retrieval
4. Provide quick response time for data extraction and regulatory inquiries
5. Provide sound chain of custody with encrypted data end-to-end

d. Provision of a Cloud-Based Email archiving service that has the following capabilities but not limited to.

1. Email data governance and retention
2. Easy end-user access and data retrieval

e. Provide Integrated and analytics based real-time reporting for email internal and external email security, email e-discovery/ journaling and email archiving

f. Data Migration:

1. Upon resumption of the new contract with Eskom, the new Incumbent must liaise and contract with the current incumbent for the purpose of data migration process.
2. Data migration costs must form part of the response.

3. Data migration to the incumbents' platform and Data Centre of choice must be completed within 18 months of the contract resumption.
4. During data migration, Eskom must still be able to access and search data for operational purposes.
5. The incumbent must ensure and guarantee that the chain of the custody is maintained throughout the migration process.

DOCUMENT ACKNOWLEDGEMENT

By signing this document, the people listed record their agreement on the contents of this document.

	Name:	Sithembile Singo
Senior Manager: IT Security Services	**Signature:**	
	Date:	16-03-2022
	Name:	Beresford Jelliman
Chief Advisor – IM Security	**Signature:**	
	Date:	22 -03- 2022
	Name:	Mmutle Kgampe
Senior Advisor: IM Security	**Signature:**	
	Date:	09-03-2022