

SERVICE LEVEL AGREEMENT

BETWEEN

ESKOM HOLDINGS SOC LIMITED

(Hereinafter referred to as Eskom)

AND

VENDOR

(Name of contractor/Vendor, hereinafter referred to as Vendor)

Initials:

	Services and Service Levels	APPENDIX A
---	------------------------------------	-------------------

1. Introduction

- 1.1. This document is a service-level agreement (SLA) between Eskom Holdings SOC Limited (Eskom) and Vendor
- 1.2. The SLA constitutes a formal agreement, which defines and formalises key components of the working relationship between Eskom and Vendor.
- 1.3. The SLA document must be read together with the main NEC3 Professional Services Contract, (PSC3).
- 1.4. This SLA document will be reviewed twice a year to take cognisance of any constant changes or as when Eskom strives to improve the print environment on a continuous basis.

2. Scope

- 2.1. This SLA documents:

- key roles and responsibilities.
- the service levels, support availability and service requirements provided for the offerings.
- service-level monitoring and
- service performance management.

3. Purpose

- 3.1. The aim of this agreement is to provide a formal and reporting basis for cooperation between Eskom and Vendor and to clarify each party's responsibilities, as well as to provide a framework for common understanding between the two parties, ultimately ensuring that a timely and efficient service and support are available to meet the objectives of the service.
- 3.2. The agreement defines, in detail, the services to be delivered by Vendor and the level of service that can be expected by Eskom, thereby reducing the risk of misunderstandings, and providing a common understanding of service requirements/capabilities and of the principle involved in the measurement of service levels.

4. Effective date

- 4.1. This agreement will be effective on the date of the signature of the main NEC3 Professional Services Contract (PSC3) by both parties to this agreement.
- 4.2. The act of signing the SLA will be binding on both parties with respect to the terms of the agreement.

5. Normative/informative references

- 5.1. Parties shall apply the most recent edition of the documents listed in the following paragraphs.

5.1.1. Normative

- Eskom Information Security Policy (32-85)

6. Definitions

Definition	Explanation
Acknowledgement	Means that Eskom will receive a reference either by email or verbally to indicate that the call has been logged.
Billing Schedule	Supporting document provided by Vendor to validate volumes and services provided.
Incident	Incident tickets will indicate that something is broken or faulty. Incidents can be generated manually via the Vendor service desk (telephone or email) or via system generated tickets
Problem	Problem calls indicate that there are various incidents calls related to the same root cause.
Project Implementation Services	Implementation of request or change request that will take more than 200 hrs but less than 6 months , will be classified and managed as a BAU project.
Response	The response time is the time, measured in hours or part thereof, for the technician to arrive on site in person once an incident has been logged at the call management centre.
Resolution	The resolution time is the time taken to resolve the call.
Working Day	Normal business hours between 08:00 and 17:00 from Monday to Friday.

7. Abbreviations

Abbreviation	Explanation
BAU	Business as Usual
Eskom	Eskom Holdings SOC Limited
KPI	Key Performance Indicator
Vendor	Vendor (Pty) Ltd
NEC	National Engineering Contract
OEM	Original Equipment Manufacturer
PPE	Personal Protective Equipment
PSC	Professional Services Contract
SLA	Service Level Agreement

8. Roles and responsibilities

8.1. Eskom is responsible for:

- Collaborating with Vendor so that they may fulfil their obligations to Eskom.
- Setting and monitoring Vendor's performance.

8.2. Vendor is responsible for:

- Delivering the solution and service to Eskom.
- Configuring and deploying the solution in the Eskom environment.
- Continuous improvement of the capabilities of the solution within Eskom.
- Configuring B2B collaboration between Eskom and external identity providers together with Eskom team.
- Integrate solution to Eskom's other solutions as directed by Eskom.

9. Services and service levels

9.1. Description of service

9.1.1. Deployment environments

Initials:

- a) Vendor shall provide a DLP solution that supports different forms such as on-premises, cloud-based services, appliance and/or virtual appliance, hybrid and as add-ons in popular office applications.
- b) Vendor shall provide a DLP solution that supports 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.

9.1.2. Supported platforms

- a) Vendor shall provide a DLP solution that supports the following: Windows, MacOS, Linux, iOS, Android, and other emerging platforms such as Windows for ARM.
- b) Vendor shall provide a DLP solution that integrates into Eskom's Cloud Access Security Broker as well as other popular broker platforms.

9.1.3. Data protection

- a) Vendor shall provide a DLP solution for "Data in use" requirements – 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.
- b) Vendor shall provide a DLP solution for "Data in motion" requirements – 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.
- c) Vendor shall provide a DLP solution for "Data at rest" requirements – The DLP solution must be able to perform data store scanning, fingerprint scanning and monitor all data regularly in accordance with Eskom's policies.
- d) Vendor shall provide a DLP solution for Encryption requirements – The DLP solution must be able to perform encryption on documents through add-ons.
- e) Vendor shall provide a DLP solution that has features to control slow leaking of information by monitoring multiple transfer instances of sensitive data using artificial intelligence capabilities.
- f) Vendor shall provide a DLP solution that has Automated Discovery and Classification of 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.
- g) Vendor shall provide a DLP solution that shall 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 of it, and receive real-time alerts when user activity deviates from a pre-established baseline.
- h) Vendor shall provide a DLP solution that uses automation using Artificial Intelligence capabilities such as machine learning – 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) Vendor shall provide a DLP solution that supports Data Privacy Regulations Compliance – 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.

9.1.4. Centralised management

- a) Vendor shall provide a DLP solution that shall provide an easy-to-use single pane management console used across all deployment form factors.
- b) Vendor shall provide a DLP solution that shall provide integration with Active Directory, LDAP, and other supported Identity Providers to help manage and enforce user policies. External identity providers must be supported for B2B document sharing.

Initials:

- c) Vendor shall provide a DLP solution that provides policy templates that are built-in and easily customisable to implement industry regulation such as POPIA, PCI, GDPR, etc.
- d) Vendor shall provide a DLP solution that shall generate employee alerts and self-remediation capabilities such as confirmations and justification of data policy breaches shall be configurable.

9.1.5. External business collaboration

- a) Vendor shall provide a DLP solution that enables Eskom to share in a controlled manner documents with external business partners.
- b) Vendor shall provide a DLP solution that 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.

9.1.6. Integrations

- a) Vendor shall provide a DLP solution that is able to integrate to the following solutions:
 - a. Anomaly Detection
 - b. End-Point Protection
 - c. Email Security Solution
 - d. Security Incident and Event Management
 - e. Secure Web gateway

9.1.7. Training and support

- a) Vendor shall provide an online training platform and training documentation shall be made accessible for the use by Eskom for the following:
 - a. User Manuals
 - b. Administrator Manuals
- b) Vendor shall provide an online training platform that supports a combination of video and static content to all Eskom users.
- c) Vendor shall provide an online platform that does not require a license or subscription fee for each individual user at Eskom.
- d) Vendor shall provide support services that are available across the solution's value chain. These shall be made available 24 hours/ 7 days a week.

9.2. Support Services

- I. Hours of Service
 - Services (including technical support) shall be provided for 24 hours and 7 days per week.
- II. Eskom Information Security Policies
 - All existing and new implementations undertaken or supported, all existing and new Products and Services Supplied/Supported/Maintained by the Vendor shall adhere to all the Eskom policies and relevant standards and procedures. This includes but is not limited to Security policies, network design and deployment strategies, IT policies and Procedures, local agent site infrastructure policies and all Eskom Data Centre Policies and procedures.

9.3. Product Licencing

Automated Managed DLP Service

Enterprise license

9.4. Incident management

- Incident tickets will indicate that something is broken or faulty with the Automated DLP Managed System. Incidents can be generated manually via the Vendor service desk (telephone and/or email).

Initials:

- Actual time to resolve an incident will be measured during the Working Day.
- 95% of all incident tickets must be acknowledged within 5 minutes of logging the incident by either email or telephone.
- All incidents must be resolved within 24 hours. Where incidents cannot be resolved within 24 hours, due to reasonable inhibitors, it must be resolved within 36 hours.

9.5. Access to Eskom premises

- All Eskom offices require site-specific safety induction to be completed and the correct personal protection equipment (PPE) to be put on before entering the premises. Induction training will be arranged by the onsite contact person appointed by Eskom.

9.6. Reporting

- Vendor will provide various management reports to Eskom on a monthly basis by not later than the 5th working day of the month for the previous month's operations. The reports will be customisable to meet Eskom operational requirements and will include, but not be limited to, the following:
 - Outcome of an assessment for third parties.
 - Measures that may place Eskom at risks by third parties.
 - Updated dashboard indicators
 - Latest audits and assessments of a third party.
 - Defines standards for third parties.
 - Amount of data collected via the Automated DLP Managed System.
 - Number of Eskom personnel trained on the Automated DLP Managed System.
 - Performance on the KPIs defined in this SLA.
- All the reports mentioned above must be available electronically.
- Data collected and proposals made as a result of data collected shall NOT be shared with other parties without Eskom's written consent.

9.7. Key Performance Indicators (KPIs)

- Unless otherwise defined in the exception list, all service offerings in this agreement are operated and managed according to the KPIs summarised below.

Service Category	Service description (Monday to Sunday (00:00 to 23:59))	Service Target		Measurement Period	Weightings
Deployment environments	Service Delivery	As per agreed timelines	98%	1	10%
Supported Platforms	Service Delivery	As per agreed timelines	98%	1	10%
Data Protection	Service Delivery	As per agreed timelines	98%	1	10%
Centralised Management	Service Delivery	As per agreed timelines	98%	1	5%
External Business Collaboration	Service Delivery	As per agreed timelines	98%	1	10%
Integration	Service Delivery	As per agreed timelines	98%	1	5%
Training and Support	Service Delivery	As per agreed timelines	98%	1	1%

Initials:

9.8. Service performance management

- Service-level reports will be compiled, and reports will be produced by Vendor and forwarded in electronic format to Eskom's representative monthly by the 5th working day of the month for the previous month's operations.
- Vendor will provide an SLA dashboard showing the service offering for each service against the reporting as defined in this SLA. The measurement report will show performance trending for the service offerings monthly. A six-month view should be made available to do the trend analysis.
- Service-level breaches should be identified by Vendor in the service offering reports and shared electronically and will be monitored by Eskom. If no SLA reports are provided before the due date, the performance for that reporting month will be presumed as failed, until such report is provided.
- Actual levels of service will be compared with agreed-on target levels monthly by both parties, and in the event of a discrepancy between actual and targeted service levels, both parties are expected to identify and resolve the reason(s) for any discrepancies in close cooperation.
- All KPIs to be achieved for the overall SLA to be considered as achieved. If one or more KPI is violated in a particular reporting period, then the overall SLA for that particular reporting period will be considered as not achieved.
- In instances where there are no assigned/reported activities or work performed, the affected KPI will not be measured and will be reported as a no event and/or no action and/or ongoing.
- The results of KPIs reported quarterly and/or annually will not be considered for measuring and reporting of the overall SLA in the months where they were not reported.

9.9. Service Level review

- Eskom and Vendor will hold monthly service-level review meetings to discuss the level of service offering. Meetings will be scheduled by Eskom.
- This SLA is a dynamic document and will be periodically reviewed biannually and/or changed when the following events occur:
 - Eskom's expectations and/or needs have changed.
 - Better metrics, measurement tools, and processes have evolved in the industry as per the benchmark that will be conducted in close cooperation between both parties.
- Customer satisfaction survey will be conducted by Vendor twice a year in close cooperation with Eskom to determine a level of customer satisfaction.

Initials:

9.10. Penalties and recoveries

- In the case of an element of the service levels not being achieved, a resolution or remedy process is to be engaged. A resolution or remedy will be documented by a corrective action plan tied to an agreed-on timeline to bring the services within targeted standards within a 30-day time frame. The remedy may require service delivery correction actions, the addition of incremental capacity, and modification to the service process. Should the service level remain unchanged at below service level target after implementation of the remedy, escalation letters will be issued, which may lead to invoking of penalties.
- If Vendor fails to meet performance target in any full calendar month, penalties will be applicable. Penalties or any recoveries will be enforced should Vendor breach any of the KPIs set out in this agreement. The penalty will amount to 5% of that reporting month's service bill.
- Breaches in service are defined as not meeting agreed KPIs over a month's time. Breaches will be recorded, classified, and reviewed monthly utilising the service-level management process.
- The penalties will be recoverable in the form of a credit note against the reporting month's service bill.
- Breaches reports and opportunities for improvement will be made available in the monthly service performance report by Vendor.
- Penalties will not be applied during the transition period (the first three months after contract is signed).

This agreement constitutes the sole Service Level Agreement between Vendor and Eskom, and no variation, modification, or waiver of any of the provisions of this agreement or consent to any departure from these shall, in any manner, be of any force or effect, unless confirmed in writing and signed by both parties, and such variation, modification, waiver, or consent shall be effective only in the specific instance and for the specific purpose and to the extent for which it was made or given.

Initials:

This agreement is signed on behalf of the Vendor and Eskom, each signatory to this warranting that he/she has the requisite authority to do so.

Vendor Responsible Manager *(responsible for signing the contract on behalf of the vendor)*

Signed this day of 20 at

..... *(Place)*

(Full name)..... *(Signature)*on

behalf of **(Vendor/contractor)**

Witnesses

1.

2.

Eskom Holdings SOC Limited (Eskom's representative) *(responsible for signing the contract on behalf of the Eskom)*

Signed this day of20.....

at *(Place)*

(Full name)..... *(Signature)*.....on behalf of

Witnesses

1.

2.

Initials: