| | | |
|---|---|---|
| Eskom | **Services and Service Levels** | **APPENDIX C** |

# Service Level Agreement

**Between**

**Eskom Holdings SOC**

(hereinafter referred to as Eskom)

**and**

**Service Provider**

(hereinafter referred to as Service Provider)

# 1. 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 Service Provider to validate volumes and services provided. |
| **Incident** | Incident tickets will indicate that something is broken or faulty. Incidents can be generated manually via the Service Provider 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. |
| **Response** | The response time is the time, measured in hours or part thereof, for the technician to make first contact once an incident has been logged in the ITSM system. |
| **Resolution** | The resolution time is the time taken to resolve an incident. |

# 2. Abbreviations

| Abbreviation | Explanation |
|---|---|
| **AI** | Artificial Intelligence |
| **Eskom** | Eskom Holdings SOC Limited |
| **ITSM** | Information Technology Service Management |
| **KPI** | Key Performance Indicator |
| **MTTr** | Mean Time to Respond |
| **MTTR** | Mean Time to Resolve |
| **NEC** | National Engineering Contract |
| **PPE** | Personal Protective Equipment |
| **SLA** | Service Level Agreement |
| **SMS** | Short Message Service |
| **TSC** | Term Service Contract |
| **PSC** | Professional Service Contract |
| **RCA** | Root Cause Analysis |
| **CAB** | Change Advisory Board |
| **UAT** | User Acceptance Testing |
| **POPIA** | Protection of Private Information Act |
| **GDPR** | General Data Protection Regulation |
| **Service Provider** | Service Provider (Pty) Ltd |

# 3. Normative/Informative References

**3.1.** Parties shall apply the most recent edition of the documents listed in the following paragraphs.

3.1.1. Normative

- Eskom Information Security Policy (32-85)

## 4. Introduction

**4.1.** This document is a service-level agreement (SLA) between Eskom Holdings SOC Limited (Eskom) and Service Provider (Service Provider)

**4.2.** The SLA constitutes a formal agreement, which defines and formalises key components of the working relationship between Eskom and Service Provider.

**4.3.** The SLA document must be read together with the main NEC3 TSC (Contract Name).

**4.4.** This SLA document will be reviewed as when necessary to take cognisance of any constant changes or as when Eskom strives to improve the print environment on a continuous basis.

## 5. Scope

**5.1.** This SLA document contains:

- Services descriptions and categories;
- Key roles and responsibilities;
- The service levels, support availability and service requirements provided for the offerings under Asset Tracking Solution;
- Service-level monitoring and
- Service performance management.

## 6. Purpose

**6.1.** This agreement establishes a formal framework for cooperation between Eskom and the Service Provider, clarifies each party's responsibilities, and ensures efficient service and support for end-users.

**6.2.** The agreement specifies the services required from the Service Provider and outlines the expected service levels for Eskom. This establishes clear requirements and methods for measuring service levels, helping to prevent misunderstandings between parties.

## 7. Effective Date

**7.1.** This agreement will be effective on the date of the signature of the main NEC3 TSC (Contract) by both parties.

**7.2.** The act of signing the SLA will be binding on both parties with respect to the terms of the agreement.

# 8. Roles and Responsibilities

## 8.1. Eskom is responsible for:

- Reporting any fault on services/devices to the Service Provider's Service Desk as and when an incident arises, excluding when the problem can be automatically detected by the solution;
- Timely payment for services after all approved supporting documents have been submitted;
- Informing the Service Provider of any change within the Eskom environment;
- Providing access to Eskom's monitoring applications which need to be integrated with the Service Provider monitoring tools for end-to-end proactive solution monitoring.
- Logging requests with the Service Provider for ongoing maintenance services e.g. request to update licences for removal and reallocation; and
- Facilitating activation of the any services that may be required to enable effective maintenance and support of the solution e.g. chip by the Eskom Third Party Service Provider(s) (Known as the Supply, Delivery and Support of Endpoints).
- Providing timely notification of data deletion requirements and review audit evidence provided.
- Identifying training participants, provide training facilities (if onsite), and ensure attendance.
- Log tickets promptly, classify business impact, escalate unresolved issues to governance forums where required.

## 8.2. The Service Provider is responsible for:

- Providing, procuring and where applicable licenses under its own name;
- Support and maintenance of the solution as described in this SLA and NEC TSC Contract;
- Reporting on key performance indicators (KPIs) as described in this SLA to foster consistent measurement of performance;
- The timeous provision of the billing schedule in order to avoid delayed payment;
- Providing training to the end-users;
- The monitoring of the entire solution and ensuring integration with Eskom's monitoring solutions.
- Installation and activation (Current and future purchases) of the tool on every device in accordance with Eskom requirements and might be required to work with Eskom appointed 3rd party service providers.
- Providing continuous protection of Eskom's sensitive procurement data, including vendor, contract, financial, and transaction information.
- Ensuring the solution can be persistently accessed remotely by authorised administrators to safeguard or protect data in the event of a risk, incident, or breach.
- Implementing secure deletion and/or purging processes for data that reaches end-of-life, ensuring it is not recoverable or accessible by unauthorised persons.
- Providing immutable audit logs and certificates of data deletion/purging as proof of compliance.
- Ensuring that no support and maintenance of the solution either directly by the Service Provider or its third-party contractors is conducted outside of POPIA and or GDPR jurisdictions.

- Ensuring that technical controls, deletion processes, and audit records are consistently maintained and available for Eskom review.
- All Service Provider-provided SaaS software (tools) must expose and support industry-standard, secure APIs (e.g., REST/JSON, SOAP, OData) to enable seamless integration with Eskom's systems and with approved third-party supplier systems.
- Ensuring that Eskom has full access to API documentation, test environments, and support for integration.
- Where Eskom requires integration to existing or future systems (e.g., SAP, Vendor Master Data Management, regulatory reporting platforms), the Service Provider shall provide reasonable assistance to complete and support such integrations, with or without the involvement of Eskom's other third-party providers.
- Providing API documentation, and sandbox/test environments.
- Developing and delivering all training content, updating materials, maintaining knowledge base, and providing trainers/facilitators.
- Provide user and supplier training for the first three years after the solution go live.
- Provide training and knowledge transfer to Eskom's application support staff for the the first three years after the solution go live.
- Operate Service Desk, monitor and escalate tickets, meet SLA targets, provide reports and trend analysis.

### 8.3. Eskom 's IT Service Provider (IT Outsource partner) is responsible for:

- Installation and activation of the Asset Tracking Solution on the endpoints.

## 9. Services and Service Levels

### 9.1. Description of Service

This SLA applies to the provision, support and maintenance of the SaaS eProcurement solution for Eskom, covering:

- PR/PO management,
- Tendering,
- Auctioning,
- Contract lifecycle management,
- Supplier risk/performance management,
- Reporting, and system integrations.
- Support services - incident/problem/request/change management,
- Compliance, and
- Governance.

Any other modules which may be added as a proposal by the Service Provider and accepted as part of the contract by Eskom are also included.

9.1.1. **Service Desk & Ticketing**

- 24x7 Service Desk (email, phone, web portal).
- Logging, categorisation, prioritisation, and tracking of incidents and service requests.
- Automatic acknowledgment of logged tickets via email/SMS.
- Escalation to 2nd/3rd level support as per defined processes.
- Access to online knowledge base and FAQs for self-service.
- Acknowledgment Time: 95% of tickets acknowledged within 30 minutes.
- Response Time (First Contact):
  - Priority 1 (Critical): ≤ 15 minutes
  - Priority 2 (High): ≤ 15 minutes
  - Priority 3 (Medium): ≤ 30 minutes
  - Priority 4 (Low): ≤ 30 minutes
- Reporting & Monitoring
  - Monthly Service Desk Report including:
  - Ticket volumes by type and severity.
  - SLA compliance (response and resolution).
  - Root Cause Analysis (for repeated P1/P2 issues).
  - Customer Satisfaction (CSAT) survey scores.
  - Real-time SLA dashboard accessible to Eskom.

9.1.2. **Incident Management**

- Response and resolution times aligned to SLA priority levels (P1–P4).
- Escalation procedures (to Service Provider's L2/L3 engineers and Eskom's CAB if required).
- Root Cause Analysis (RCA) for critical/repeated incidents.

9.1.3. **Problem Management**

- Identification of recurring issues, RCA, and long-term fixes.
- Monthly "Problem Report" highlighting trends, risks, and fixes.
- Problem Identification and resolution is prioritised as follows:
  - P1 – Critical: major service outage or failure impacting end-to-end procurement operations or payments
  - P2 – High: significant functional degradation — e.g., delayed approvals, integration or API failures, contract document errors
  - P3 – Medium: recurring incidents or localised functional issues with moderate impact — e.g., incorrect vendor data, catalog mismatches, workflow slowness
  - P4 – Low cosmetic, non-critical or enhancement-related problems (UI layout, report formatting, etc.).

9.1.4. **Request Fulfilment**

- Standard requests (user setup, supplier onboarding, reporting templates) fulfilled within SLA timelines.
- A Service Desk portal integrated with the Eskom's Service Desk for request logging and tracking.
- Request fulfilment priorities are as follows:
  - P1 – Critical business-impact request (e.g., urgent supplier access to submit tender).
  - P2 – High: High-priority requests (e.g., urgent catalog update or role reassignment).
  - P3 – Normal/Standard requests (e.g., routine supplier profile updates, user report access).
  - P4 – Low-priority or informational requests (e.g., data extracts, configuration documentation).

9.1.5. **System Maintenance & Updates**

- Regular patches (security, bug fixes) applied with minimum disruption.
- Scheduled upgrades/releases communicated at least 30–60 days in advance.
- Emergency patches (e.g., security vulnerabilities) applied within 24 hours.

9.1.6. **Change Management Support**

- UAT/test environment provided for Eskom to validate changes.
- Formal change process (Standard, Normal, Emergency) with Eskom CAB approval.
- Documentation and release notes for all changes.
- Changes will be categorised as follows:
  - Standard: Pre-approved by the CAB, low-risk, recurring changes.
  - Normal: Planned, assessed, and CAB-approved changes.
  - Major: High-risk, significant impact on integrations or procurement process. CAB and Business Executive approval
  - Emergency: Urgent fix to resolve system outage, security, or compliance issue. These will require post-implementation CAB review.

9.1.7. **Performance Monitoring & Optimization**

- Continuous monitoring of uptime, response times, and integrations.
- Periodic (as agreed by both parties) performance reports and dashboards.
- Automated alerts for outages, slowdowns, or failed transactions.

9.1.8. **Data Security & Compliance Maintenance**

- Proactive monitoring for vulnerabilities and threats.
- Quarterly security compliance reports (as stipulated in Section 3.8 of the Tender Scope of Work).
- Access reviews and penetration testing at agreed intervals.
- Sensitive data is the intellectual property (IP) of ESKOM and must be protected at all times, the solution must have the capability to be persistently accessed remotely to safeguard and protect data if at risk.

- Data that is at end-of-life must be able to be deleted/purged so that it is not accessible to unauthorised persons. Audit logs and certificates to be made available as proof of data deletion/purging.
- Data Protection: 100% encryption of data in transit and at rest, aligned with industry and Eskom's standards (refer to Section 3.8 of the Tender Scope of Work).
- Data Deletion/Purging: All end-of-life data must be securely deleted/purged within a defined policy window of Eskom's request.
- Audit Evidence: Certificates of deletion and audit logs must be made available to Eskom within a defined window of completion.
- Compliance: Continuous adherence to POPIA, GDPR, ISO 27001, and Eskom Information Security Policy (32-85).

9.1.9. **User Training & Knowledge Base**

- Initial onboarding training for Eskom users.
- Periodic refresher or new feature training.
- Online knowledge base, FAQs, and user manuals.
- Role-based training for the procurement practitioner community.
- Training must be delivered via a mix of live (in-person or virtual) sessions and recorded e-learning modules as per Eskom's training standards.
- Comprehensive manuals, quick reference guides, and e-learning content.
- Updated materials provided within 5 working days of each major release or feature update.
- Access to an online knowledge base, FAQs, and vendor's learning portal.
- Refresher training provided for new features/releases.
- Refresher training to be provided periodically as agreed upon by both parties.
- Satisfaction Rating**:** 90% positive feedback score on training sessions (measured via post-training survey).
- The following deliverables are required:
  - Training Plan (aligned to project phases and user roles).
  - Training Materials (manuals, guides, e-learning).
  - Training Attendance Registers and Completion Reports.
  - Post-training Feedback Surveys and Summary Reports.

9.1.10. **Supplier Training & Knowledge Base**

The SaaS eProcurement solution will be utilized by Eskom's vendors throughout the Source to Pay process. Therefore, it is essential to provide effective and efficient training and support on an ongoing basis. The list below is indicative and not exhaustive. Detailed requirements will be discussed as part of the design workshop once the successful vendor is onboarded.

- **Onboarding Training**
  - Guidance on supplier registration, profile management, and compliance verification (e.g., CSD, B-BBEE, ESG requirements).
  - Step-by-step process for tender participation, reverse auctions, bid submissions, and contract acceptance.

- **Transaction Training**
  - How to acknowledge POs, submit invoices, and track payment status.
  - Handling communications, disputes, and updates through the system.
- **Training Materials for Suppliers**
  - Supplier-specific user guides, FAQs, and video tutorials in multiple formats (PDF, e-learning).
  - Self-service portal with multilingual support.
  - Quick reference guides tailored for SMEs and rural suppliers with limited digital literacy.
  - Training Materials updated content must be provided within 5 working days of system changes/releases.
- **Ongoing Support**
  - Webinars and live sessions during initial rollout and after major system updates.
  - Supplier Service Desk (email, chat, phone) for technical and functional queries.
  - Supplier Service desk operating hours are Mon–Fri 07:00–17:00, excl. public holidays).

- **Supplier Training Deliverables**
  - Supplier Training Plan (aligned to onboarding waves and Eskom sourcing calendar).
  - Supplier Training Materials (manuals, quick guides, e-learning, webinars).
  - Supplier Service Desk SLA Reports.
  - Supplier Training Attendance & Completion Reports.
  - Supplier incident prioritisation is as follows:
    - P1: Complete outage affecting multiple suppliers or tenders.
    - P2: Major functional impact (cannot submit bid, update profile).
    - P3: Moderate issue (report error, catalog issue).
    - P4: Informational or minor requests.

9.1.11. **Application Support Staff Training (Super Users / Eskom IT)**

The Service Provider shall provide advanced training for Eskom application support staff, covering:

- System Administration: User provisioning, role-based access control, workflow configuration, and approval chain management.
- Configuration Management: Supplier onboarding rules, business rule updates, validation checks, and catalogue management.
- Monitoring & Troubleshooting: Reviewing system health dashboards, responding to common user queries, and escalating incidents.
- Integration Oversight: Monitoring API/integration status with SAP S/4HANA, Vendor Master Data, finance, and regulatory reporting systems.
- Release & Change Management: Reviewing release notes, performing UAT, and supporting Eskom's Change Advisory Board (CAB).
- Reporting & Analytics: Generating SLA, procurement performance, and compliance reports.

- Initial Training: All Eskom application support staff trained no later than 30 days prior to solution go-live.
- Refresher Training: Conducted annually, and after each major system release/upgrade.
- Training Materials: Updated administrator manuals, system configuration guides, and integration playbooks delivered within 5 working days of new release.
- Knowledge Transfer: 100% of Eskom's nominated support staff must complete knowledge transfer sessions during implementation.
- Satisfaction Rating: Minimum 90% satisfaction score from Eskom application support staff on training effectiveness.

9.1.12. **Dedicated Account Management**

- Named Service Manager accountable for SLA delivery.
- Monthly service review meetings.
- Quarterly strategic reviews on adoption, risks, and improvements.

9.1.13. **Solution Integration**

- Backward Compatibility: APIs must remain stable across releases (no breaking changes without a notice period agreed by both parties).
- Performance: APIs must meet agreed SLAs for uptime and response times (refer to section 3.10 of the Tender Scope of Work).
- All APIs must use OAuth2/SAML for authentication and TLS 1.2+ encryption.
- Support Eskom's integration partners and resolve API-related issues under the SLA timelines.

9.1.14. **Solution installation**

- The eProcurement solution shall be delivered as a cloud-based service, accessible via modern web browsers and secure mobile applications, without requiring any software to be pre-installed on Eskom devices.
- The Service Provider must ensure compatibility with Eskom's standard operating environments (desktop, mobile, and network security policies). Where local components are required (e.g., browser plug-ins, API connectors, or mobile apps), they must be lightweight, secure, and fully supported.
- The Service Provider shall provide Eskom with secure administrator access to the eProcurement SaaS solution via a web-based management console.
- Administrator roles and permissions must be configurable to support segregation of duties (e.g., procurement, finance, IT security).
- Access must be controlled through role-based access controls (RBAC), multi-factor authentication (MFA), and audit logging and comply with Eskom's standards.
- Eskom administrators shall have the capability to:
  - Configure workflows, approval chains, and user roles.
  - Manage supplier onboarding and data validation processes.
  - View, generate, and export reports and audit logs.
  - Monitor solution performance and SLA dashboards.
  - Administrator access shall not require pre-installation of any component on Eskom devices.

- All access must comply with Eskom Information Security Policy (32-85), POPIA, and GDPR.

## 9.2. Hours of Service

9.2.1. The eProcurement solution is classified as a mission critical system and thus must have 24X7 availability.

9.2.2. Operating hours for support of supplier related issues are Monday to Friday from 08h00 – 16h00 excluding public holidays.

9.2.3. Eskom may request support on public holidays, and weekends as and when required.

## 9.3. Service Portal

9.3.1. Service Provider will provide an SLA and management dashboard in the form of an online secure portal. The portal will provide executive summary reports on the environment. The content will be agreed between the parties.

## 9.4. Key Performance Indicators (KPIs)

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

| KPI ID | KPI | Service description - 24x7 service | Priority | Service Target (Time) | Service Target (%) | Measurement Period |
|---|---|---|---|---|---|---|
| DPEP001 | Service Desk Availability | 24 X7 hours of operation | | | 99% | Monthly |
| DPEP002 | Call Response First Contact | % of calls answered within 20 seconds | | 20 seconds | 80% | Monthly |
| DPEP003 | First Contact Resolution | % of issues resolved without escalation | | | 80% | Monthly |
| DPEP004 | Service Desk Ticket Closure Quality | % of tickets closed with complete documentation | | | 95% | Monthly |
| DPEP005 | Escalation Handling | % of escalations handled within SLA | | | 100% | Monthly |
| DPEP006 | Customer Satisfaction (CSAT) | User satisfaction rating (post-ticket survey) | | | 90% | Monthly |
| DPEP007 | Incident Mean Time to respond (MTTr) | Mean Time to respond to an incident within % targets | P1 | 15 minutes | 100% | Monthly |
| | | | P2 | 15 minutes | 99% | Monthly |
| | | | P3 | 30 minutes | 99% | Monthly |
| | | | P4 | 30 minutes | 99% | Monthly |
| DPEP008 | Incident Mean Time to Resolve (MTTR) | Mean Time to resolve incidents within % targets | P1 | 4 hours | 100% | Monthly |
| | | | P2 | 6 hours | 99% | Monthly |
| | | | P3 | 8 hours | 99% | Monthly |
| | | | P4 | 16 hours | 99% | Monthly |
| DPEP009 | Problem Detection Time (via monitoring tools) | Time from incident trend identification to problem record creation | P1 | ≤ 4 hours | 99% | Monthly |
| | | | P2 | ≤ 8 hours | 99% | Monthly |
| | | | P3 | ≤ 24 hours | 99% | Monthly |
| | | | P4 | ≤ 3 business days (72 hours) | 99% | Monthly |
| DPEP010 | Problem Record Accuracy | Percentage of problem records correctly categorized and linked to related incidents | | | ≥ 95% | Monthly |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPEP011 | Problem Logging Compliance | % of problems logged in compliance with process standards | | | ≥ 98% | Monthly |
| DPEP012 | RCA Completion Time | Average time to complete root cause analysis after problem detection | P1 | ≤ 5 business | 90% | Monthly |
| | | | P2 | ≤ 10 business days | 90% | Monthly |
| | | | P3 | ≤ 15 business days | 90% | Monthly |
| | | | P4 | ≤ 20 business days (or by next scheduled maintenance cycle) | 90% | Monthly |
| DPEP013 | Repeat Problem Rate | % of problems recurring after closure | | | ≤ 2% | Monthly |
| DPEP014 | Root Cause Prevention Index | % of problems prevented through proactive measures | | | ≥ 20% year-on-year improvement | Monthly |
| DPEP015 | Request Logging Time | Time from when user submits a request to when it is recorded in the system | | ≤ 30 minutes | 90% | Monthly |
| DPEP016 | Request Acknowledgement Time | Time to confirm receipt of request to end user | | ≤ 2 business hours | 90% | Monthly |
| DPEP017 | Request Fulfilment Time | Time to fulfil a service request | P1 | ≤ 4 hours | 90% | Monthly |
| | | | P2 | ≤ 1 business day | 90% | Monthly |
| | | | P3 | ≤ 3 business days | 90% | Monthly |
| | | | P4 | ≤ 5 business days | 90% | Monthly |
| DPEP018 | Request Backlog Rate | % of open requests older than SLA threshold | | | ≤ 5% of monthly total | Monthly |
| DPEP019 | Scheduled Maintenance Notification | Minimum time vendor must notify Eskom before scheduled maintenance | Planned Maintenance | ≥ 10 business days for planned maintenance | 100% | Monthly |
| | | | Emergency Maintenance | ≥ 48 hours for emergency maintenance | 100% | Monthly |
| DPEP020 | Change Approval Compliance | % of maintenance activities approved through Eskom's Change Advisory Board (CAB) | | | 100% | Monthly |
| DPEP021 | Adherence to Approved Maintenance Window | % of maintenance activities executed within approved timeframes | | | ≥ 95% | Monthly |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPEP022 | Maintenance Overrun Rate | % of maintenance events exceeding agreed window | | | ≤ 2% | Monthly |
| DPEP023 | Post-Maintenance Uptime | Availability of the eProcurement system after maintenance completion | | | 99% | Monthly |
| DPEP024 | System Stability Period | Period of uninterrupted operation following maintenance | | ≥ 72 hours post-maintenance | 99% | Monthly |
| DPEP025 | Defect Introduction Rate | % of post-update incidents caused by maintenance or updates | | | ≤ 2% of total incidents per month | Monthly |
| DPEP026 | Critical Security Patch Application Time | Time to apply vendor-released critical patches | | ≤ 5 business days after release | 99% | Monthly |
| DPEP027 | Non-Critical Patch Application Time | Time to apply regular patches or functional updates | | ≤ 15 business days after release | 99% | Monthly |
| DPEP028 | Change Logging Time | Time taken to log a change request (CR) after submission by requestor | | ≤ 1 business day | 95% | Monthly |
| DPEP029 | Change Categorisation Accuracy | % of changes correctly classified as Standard, Normal, or Emergency | | | ≥ 98% | Monthly |
| DPEP030 | Change Impact Assessment Completion | % of CRs with full business, technical, and risk assessments completed prior to CAB review | | | 100% | Monthly |
| DPEP031 | Change Implementation Success Rate | % of changes deployed successfully without rollback or service disruption | | | ≥ 98% | Monthly |
| DPEP032 | Emergency Change Success Rate | % of emergency changes implemented without causing incidents or rework | | | ≥ 95% | Monthly |
| DPEP033 | Change Scheduling Compliance | % of changes executed within approved maintenance/change window | | | ≥ 95% | Monthly |
| DPEP034 | Change Documentation Completeness | % of CRs with complete technical, test, rollback, and communication plans | | | 100% | Monthly |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPEP035 | Unplanned Change Rate | % of changes implemented outside of approved process or without CR record | | | 0% | Monthly |
| DPEP036 | System Availability (Uptime) | % of time the eProcurement platform is fully operational and accessible to users | | | ≥ 99.7% | Monthly |
| DPEP037 | Monitoring & Alert Detection Accuracy | % of real performance degradations accurately detected by monitoring tools | | | ≥ 95% | Monthly |
| DPEP038 | Alert Response Time | Time to acknowledge and act on critical performance alerts | P1 | ≤ 15 minutes | 90% | Monthly |
| | | | P2 | ≤ 30 minutes | 90% | Monthly |
| | | | P3 | ≤ 4 hours | 90% | Monthly |
| | | | P4 | ≤ 8 hours | 90% | Monthly |
| DPEP039 | Data Breach Prevention Rate | % of months without any confirmed data breach or leak (internal or external) | | | 100% (Zero data breaches) | Quarterly |
| DPEP040 | Data Encryption Compliance | % of sensitive data (at rest & in transit) encrypted using approved standards (AES-256, TLS 1.3 +) | | | 100% | Monthly |
| DPEP041 | Data Masking Coverage Rate | % of sensitive data fields masked or anonymised in all non-production environments (test, dev, UAT, training) | | | 100% | Monthly |
| DPEP042 | Unmasked Data Exposure | Incidents<br>Number of incidents where unmasked data was exposed in non-production environments | | | 0% | Monthly |
| DPEP043 | Access Control Compliance | % of users with least-privilege access rights based on roles | | | ≥ 98% | Monthly |
| DPEP044 | Multi-Factor Authentication (MFA) Enforcement | % of privileged users with MFA enabled | | | 100% | Monthly |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPEP045 | POPIA Compliance Rate | % of data processing activities compliant with POPIA (collection, storage, retention, deletion) | | | 100% | Monthly |
| DPEP046 | GDPR / International Compliance | % of cross-border data transfers adhering to applicable regulations | | | 100% | Monthly |
| DPEP047 | Security Event Detection Time | Time from occurrence of a security event to detection by monitoring tools | P1 | ≤ 15 minutes | 100% | Monthly |
| DPEP048 | Incident Response Time | Time from detection to containment of critical security incident | P1 – P4 | ≤ 1 hour | 100% | Monthly |
| DPEP049 | Incident Resolution Time (P2–P4) | Time to fully resolve and verify closure of non-critical security incidents | P2 – P4 | ≤ 24–72 hours | 98% | |
| DPEP050 | Backup Success Rate | % of scheduled backups successfully completed | | | 100% | Monthly |
| DPEP051 | Backup Encryption Compliance | % of backup data encrypted during storage and transmission | | | 100% | Monthly |
| DPEP052 | Data Recovery Time Objective (RTO) | Maximum time to restore critical eProcurement data after an incident | | ≤ 4 hours | 98% | Monthly |
| DPEP053 | Data Recovery Point Objective (RPO) | Maximum tolerable data loss measured in time | | ≤ 15 minutes | 100% | Monthly |
| DPEP054 | Data Retention Compliance | % of data retained and purged according to Eskom policy (end-of-life or contract closure) | | | 100% | Monthly |
| DPEP055 | Vulnerability Scan Compliance | Frequency and completeness of vulnerability scans (infrastructure + applications) | | | 100% | Monthly |
| DPEP056 | Critical Vulnerability Remediation Time | Time to patch high-risk vulnerabilities (CVSS > 8) | | ≤ 5 business days | 100% | Monthly |
| DPEP057 | Medium-Risk Vulnerability Remediation Time | Time to patch moderate-risk vulnerabilities | | ≤ 15 business days | 100% | Monthly |
| DPEP058 | Security Patch Compliance Rate | % of systems patched within SLA | | | ≥ 98% | Monthly |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPEP059 | SOC 1 and 2 Report Submission and Review | Timeous submission of comprehensive SOC 1 and 2 reports for review by Eskom | | | 100% | Annually |
| DPEP060 | Cyber breach formal communication | Formal communication to Eskom of cyber breach incidents | | ≤ 24 hours | 100% | Monthly |
| DPEP061 | Security impacting change communication | Formal communication to Eskom of any significant changes to the business, platform and hosting service provider or any change that could have an impact the security assessment conducted and the auditor's opinion on the SOC audit | | 1 calendar month | 100% | Monthly |
| DPEP062 | Training Plan Submission Compliance | % of training plans (curricula, schedules, materials) submitted and approved before go-live or release | | ≤ 30 days before training start | 100% | On request |
| DPEP063 | Curriculum Coverage Rate | % of business processes and modules covered by training content | | | 100% | On request |
| DPEP064 | Training Resource Readiness | Availability of certified trainers, venues, systems, and materials by training start date | | | 100% | On request |
| DPEP065 | Training Delivery SLA Compliance | % of scheduled training sessions delivered on time | | | ≥ 95% | On request |
| DPEP066 | Training Completion Rate | % of enrolled users completing mandatory training (end-users, suppliers, support staff) | | | ≥ 95% | On request |
| DPEP067 | Supplier Training Coverage | % of active suppliers trained on portal usage, onboarding, and compliance processes | | | ≥ 90% of active suppliers | On request |
| DPEP068 | Refresher Training Delivery Frequency | Frequency of refresher or update training (new features, compliance updates) | | | 100% | Quarterly |

| | | | | | | |
|---|---|---|---|---|---|---|
| DPEP069 | Change/Release Training Delivery Time | Time to deliver training for new functionality after release | | ≤ 10 business days post-release | 100% | Quarterly |
| DPEP070 | Knowledge Base Update Compliance | % of new FAQs, guides, or videos uploaded to the self-service portal within SLA after system change | | ≤ 3 business days | 100% | Quarterly |
| DPEP071 | Training Feedback (Satisfaction) Score | Average satisfaction rating from participants | | | ≥ 90% positive | Quarterly |
| DPEP072 | Supplier Service Desk Availability | % of scheduled hours the service desk is operational and reachable by suppliers | | during supplier service desk operating hours | ≥ 99% | Monthly |
| DPEP072 | Multichannel Responsiveness | Availability of multiple support channels (phone, email, portal, chat) | | | 100% | Monthly |
| DPEP073 | First Contact Resolution (FCR) Rate | % of supplier issues resolved during first interaction | | | ≥ 80% | Monthly |
| DPEP074 | Incident Acknowledgement Time | Time to acknowledge receipt of supplier issue<br>≤ 30 minutes (P3–P4) | P1–P2 | ≤ 15 minutes | ≥ 95% | Monthly |
| | | | P3 – P4 | ≤ 30 minutes | ≥ 95% | Monthly |
| DPEP075 | Supplier Incident Resolution Time | Time to resolve a supplier incident | P1 | **≤ 4 hours** | ≥ 95% | Monthly |
| | | | P2 | **≤ 8 business hours** | ≥ 95% | Monthly |
| | | | P3 | **≤ 2 business days** | ≥ 95% | Monthly |
| | | | P4 | **≤ 5 business days** | ≥ 95% | Monthly |
| DPEP076 | Escalation Compliance Rate | % of escalations performed within SLA when required | | | 100% | Monthly |
| DPEP077 | Supplier Satisfaction (CSAT) Score | % of positive feedback from supplier users | | | ≥ 90% | Monthly |
| DPEP078 | Knowledge Transfer (KT) Compliance | % of KT sessions conducted as part of project handover or staff transition | | | 100% | Quarterly |
| DPEP078 | Quarterly Skills Matrix Review | A review of application support team competence levels | | | 100% | Quarterly |

## 9.5. Overall SLA Achievement Report

9.5.1. If any KPI is violated during a reporting period, that KPI's SLA will be marked as failed for that period.

9.5.2. In instances where there are no requests or incidents, the affected KPI will not be measured and will be reported as a no event and/or no action required.

## 9.6. Service Performance Management

9.6.1. Service Performance Management begins three months after service starts and will ensure monthly service levels meet or exceed the standards set out in section 9.4– Key Performance Indicators. Service levels are monitored throughout the contract period.

9.6.2. The Service Provider will submit monthly management reports to Eskom by the 5th of each month, covering the previous month’s operations. Reports will be customisable to Eskom’s needs and include, but are not limited to, the following:

- Monthly SLA Performance Report
- Quarterly Service Review Report
- Annual Sla compliance Report
- Incident Management Report
- Problem Management Report
- Change Management Report
- Release and Deployment Report
- Supplier Reports
- Security SOC reports
- Customer and Supplier satisfaction reports
- Training reports
- Data privacy compliance reports

| Eskom | Services and Service Levels | APPENDIX C |
|---|---|---|

| Report Name | Purpose / Description | Key Contents / Metrics | Frequency |
|---|---|---|---|
| **1. SLA & Performance Reports** | | | |
| Monthly SLA Performance Report | Tracks service level compliance and breaches | SLA KPIs, uptime %, incidents, breaches, root causes, service credits | Monthly |
| Quarterly Service Review Report | Reviews SLA trends, risks, and improvements | KPI trends, risk summary, improvement actions, audit status | Quarterly |
| Annual SLA Compliance Report | Year-end SLA summary for executive oversight | Annual KPI averages, service credits, audit results, recommendations | Annually |
| **2. Incident, Problem & Change Reports** | | | |
| Incident Management Report | Tracks incidents and response/resolution performance | Incident count by priority, MTTR, root causes, SLA adherence | Weekly / Monthly |
| Problem Management Report | Analyses recurring or systemic issues | Problem log, RCA summary, workaround success, permanent fix rate | Monthly |
| Change Management Report | Monitors changes and related risk outcomes | Approved vs rejected changes, success rate, rollback rate | Monthly |
| Release & Deployment Report | Communicates new releases and post-deployment results | Release list, testing results, performance validation, rollback outcomes | Per Release |
| **3. Data Security, Privacy & Compliance Reports** | | | |
| Security Incident Report | Documents cybersecurity or data breach events | Incident summary, response actions, RCA, impact analysis | As Occurred |
| Data Security Compliance Report | Monitors adherence to POPIA, ISO 27001, and Eskom ICT policy | Encryption status, patch compliance, vulnerability findings | Quarterly |
| Backup & Recovery Validation Report | Verifies success of data backup and restore tests | Backup completion %, RTO/RPO results, restore test outcomes | Monthly / Quarterly |
| Data Masking Compliance Report | Confirms masking of sensitive non-production data | Masking coverage %, incidents, validation results | Quarterly |

| Report Name | Purpose / Description | Key Contents / Metrics | Frequency |
|---|---|---|---|
| Audit & Compliance Report | Summarises audit results and remediation progress | Audit findings, closure rate, compliance score | Quarterly / Annually |
| **4. System Performance & Optimisation Reports** | | | |
| System Performance Dashboard | Provides real-time visibility of performance KPIs | Uptime %, latency, response times, resource utilisation | Real-time / Monthly |
| Integration & Batch Job Report | Tracks integration performance and job completion | Job success rate, retries, integration latency | Weekly / Monthly |
| Capacity & Resource Utilisation Report | Forecasts and monitors infrastructure resource use | CPU/memory trends, storage growth, utilisation % | Monthly / Quarterly |
| Optimisation & Tuning Report | Documents performance improvements and outcomes | Bottlenecks identified, optimisation actions, KPI gains | Quarterly |
| **5. Supplier Service Desk & Support Reports** | | | |
| Supplier Service Desk Performance Report | Measures responsiveness and support efficiency | Ticket volume, FCR rate, resolution times, CSAT | Monthly |
| Supplier Satisfaction (CSAT) Report | Captures supplier feedback and sentiment | Survey results, top issues, improvement plan | Quarterly |
| Recurring Issue Trend Report | Identifies common supplier pain points | Top recurring issues, trends, resolution actions | Monthly / Quarterly |
| **6. Training & Knowledge Transfer Reports** | | | |
| User Training Completion Report | Tracks Eskom user training coverage | Attendance, pass rates, satisfaction, modules completed | Per Training Cycle / Monthly |
| Supplier Training Coverage Report | Measures supplier training and enablement outcomes | No. of suppliers trained and the satisfaction score | Quarterly |
| Application Support Staff Training Report | Tracks support staff competence and certification | Completion %, assessment results, skills gaps | Quarterly |
| Knowledge Base Update Report | Ensures knowledge repository is current | Articles added, usage rate, review compliance | Monthly |

| Report Name | Purpose / Description | Key Contents / Metrics | Frequency |
|---|---|---|---|
| **7. Problem, Risk & Continuous Improvement Reports** | | | |
| Continuous Improvement Log / Tracker | Tracks improvement initiatives and outcomes | Improvement actions, status, measured benefits | Monthly / Quarterly |
| Risk & Issue Register Report | Summarises key operational and project risks | Risk severity, mitigation plan, ownership, trend | Monthly |
| Innovation / Automation Opportunities Report | Identifies potential areas for automation / AI | Proposed enhancements, cost-benefit, maturity | Quarterly / Annually |
| **8. Governance, Audit & Executive Oversight Reports** | | | |
| Monthly Governance Summary Pack | Consolidated summary of SLA and operational metrics | KPI summary, major incidents, service credits | Monthly |
| Quarterly Executive Dashboard | High-level SLA and risk summary for leadership | SLA overview, risk matrix, compliance summary | Quarterly |
| Annual Governance Report | Full-year governance and performance summary | SLA trends, audit outcomes, vendor performance rating | Annually |
| **9. Data Quality & Vendor Master Data Reports** | | | |
| Vendor Master Data Quality Report | Tracks accuracy and completeness of supplier data | Duplicate rate, missing fields, validation errors | Monthly |
| Vendor Data Stewardship Dashboard | Mon | | |

9.6.3. All the reports mentioned above must be available on the portal and be accessible.

9.6.4. Service-level reports will be compiled, and reports will be produced by the Service Provider and forwarded in electronic format to Eskom's representative monthly by the 5th (fifth) working day of the month for the previous month's operations.

9.6.5. Reports with drill-down facility on volumes per user, per cost centre, per department, per division, per cluster, per geographical area will be drawn electronically on a monthly basis and reviewed.

9.6.6. Eskom will require access to the Service Provider's Service management software to be able to verify billing schedules and invoices. This should be provided through an online web-based portal.

9.6.7. Data collected and proposals made as a result of audits will NOT be shared with other parties without Eskom's written consent.

9.6.8. The Service Provider will be responsible for monitoring and measuring its performance against the service levels in accordance with the methodology specified in section 9.4 – Key Performance Indicators.

9.6.9. Service-level reports will be compiled, and reports will be produced by the Service Provider and forwarded in electronic format to Eskom's representative on a monthly basis by the 5th working day of the month for the previous month's operations.

9.6.10. The Service Provider will provide an electronic portal showing the service offering for each service against the incident response and resolution times and request response times as defined in this SLA. The measurement report will show performance trending for the service offerings on a monthly basis. A six-month view should be made available to do the trend analysis.

9.6.11. Service-level breaches should be identified by the Service Provider in the service offering reports and, on the portal, 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.

9.6.12. Actual levels of service will be compared with agreed-on target levels on a monthly basis 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.

9.6.13. Eskom shall have the right on written notice to change, add or delete any of the service level(s) during the term of this contract. The Service Provider has 60 days of receipt of notice to implement and report on the new service level(s).

9.6.14. Eskom may propose new Service Levels and/or new Key Performance Indicators ("KPI") (if required) by sending a written request to the Service Provider at least 60 (sixty) days prior to the date that Eskom requires such additional Service Levels or KPIs (as applicable) to be effective.

9.6.15. Such written requests (which may contain multiple additions) may not occur more than twice in a calendar year.

9.6.16. Once the Parties have agreed to the relevant changes (if any) such changes will follow the Contract Change Control process.

## 9.7. Service Level Review

9.7.1. Eskom and Service Provider will hold monthly service-level review meetings to discuss the level of service offering. Meetings will be scheduled by Eskom.

9.7.2. This SLA is a dynamic document and will be periodically reviewed biannually and/or changed when the following events occur:

9.7.3. Eskom's expectations and/or needs have changed.

9.7.4. 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.

9.7.5. Customer satisfaction survey will be conducted by Service Provider twice a year in close cooperation with Eskom to determine a level of customer satisfaction.

## 9.8. Excuse of Performance

9.8.1. The Service Provider shall be relieved from performing its directly affected obligations under this Agreement (an "Excused Event") to the extent that such non-performance results directly from Eskom's failure to perform any of its obligations or dependencies (each an "Eskom Dependency").

9.8.2. For purposes of this clause, an Eskom Dependency includes any problem, issue, risk, or actual, potential, envisaged, or impending delay (including those caused by Eskom's third-party suppliers) that prevents or materially delays the Service Provider from performing its obligations.

9.8.3. The Service Provider must escalate to Eskom any Eskom Dependency which it is unable to resolve within forty-eight (48) hours of becoming aware of such issue and shall provide Eskom with a monthly summary of all such escalations.

9.8.4. Following escalation, the Service Provider shall promptly submit a proposed mitigation plan for Eskom's approval, which shall list all foreseeable tasks, activities, workarounds, or circumvention measures required to address or mitigate the Eskom Dependency.

9.8.5. The Service Provider shall use Commercially Reasonable Efforts to continue performing its unaffected obligations and to minimise the impact of any non-performance caused by the Eskom Dependency.

9.8.6. The Service Provider shall recommence full performance of its obligations immediately once the relevant Eskom Dependency has been resolved.

## 9.9. Penalties and Recoveries

9.9.1. Eskom will do everything within its mandate, powers, services, and capacity to ensure that customer service is the first priority and that all users of managed print services are constantly satisfied with the service.

9.9.2. 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.

9.9.3. If Service Provider fails to exceed performance target in any full calendar month, penalties will be applicable. Penalties or any recoveries will be enforced, should Service Provider breach any of the KPIs set out in this agreement. The penalties will be enforced according to the weighting of each specific KPI.

9.9.4. The penalty will be calculated according to weighting percentage for the failed KPI in that reporting month. The following will apply:

- If the weighing is high, the penalty will amount to 5% of the service bill,
- if the weighting is medium the penalty will amount to 3% of the service bill.
- If the weighting is low, there will be no penalty incurred.
- If more than one KPI is failed in a reporting period, the penalty will not be more than 10% of the service bill.

9.9.5. Breaches in service are defined as not meeting agreed KPIs over a month's time. Breaches will be recorded, classified, and reviewed on a monthly basis utilising the service-level management process.

9.9.6. The penalties will be recoverable in the form of a credit note against the reporting month's Billable Schedule.

9.9.7. Breaches reports and opportunities for improvement will be made available in the monthly service performance report by Service Provider.

This agreement constitutes the sole agreement between Service Provider 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.

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

**Service Provider Responsible Manager** (*responsible for signing the contract on behalf of the Service Provider)*

Signed this …….. day of ……..……..... 20 …… at

……..…… (*Place*)

(*Full name*)…… (*Signature*) ……on

behalf of …….. **(supplier/contractor)**

Witnesses

1. ……
2. ……

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

Signed this …… day of ……...20……

at ……..…… (*Place*)

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

Witnesses

1. ……
2. ……..