Eskom	Request for Proposal	KZNOU

Title: **Request for Proposal for Central East Cluster -KZN for Guarding and Security Technology - Pietermaritzburg, Empangeni and Newcastle Zones.**

Document Identifier:

Alternative Reference Number: **N/A**

Area of Applicability: **KZNOU**

Functional Area: **Security**

Revision: **12**

Total Pages: **59**

Next Review Date: **N/A**

Disclosure Classification: **Controlled Disclosure**

Compiled by	Functional Responsibility	Authorized by
Musa Mchunu	**Phumla Siswana**	**Brenda Cebekhulu**
Security Manager KZNOU	**SHEQS Manager Central East Cluster**	**Senior Manager Business Enablement**
Date: 27.10.2026	Date: 28.10.2026	Date: 06 November 2026

Content

Page

1. Introduction 3
2. Supporting Clauses 3
   - 2.1 Scope 3
     - 2.1.1 Purpose 3
     - 1.1.2. Applicability 3
     - 1.1.3. Effective date 4
   - 2.2 Normative/Informative References 4
     - 2.2.1 Normative 4
     - 2.2.2 Informative 4
   - 2.3 Definitions 4
   - 2.4 Abbreviations 5
   - 2.5 Roles and Responsibilities 5
   - 2.6 Process for Monitoring 7
   - 2.7 Related/Supporting Documents 7
   - 2.9. Contract Duration 9
   - 4. Scope of Work 35
5. Acceptance 59
6. Revisions 59
7. Development Team 59
8. Acknowledgements(if applicable) 59

TABLE

Table 1: Pietermaritzburg Zone substations/Area offices/offices and network infrastructure (268 sites) 23

Table 2:Empangeni Zone substations/Area offices/offices and network infrastructure (148 sites) 28

Table 3: Newcastle Zone substations/Area offices/offices and network infrastructure (188 sites).. 31

Innovation and Improvement KPIs ..... **Error! Bookmark not defined.**

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

1. Introduction

Eskom Holdings SOC Ltd invites qualified and experienced service providers to submit proposals for the provision of outcome-based physical guarding services and technology solutions at Eskom facilities within the Central East Cluster-KZN Zones. The objective is to enhance security outcomes through the integration of advanced technology, innovation, and measurable performance metrics. The contract will focus on delivering physical guarding services, technology-driven solutions, and continuous improvement to ensure the safety and protection of Eskom's assets, personnel, and operations.

This contract will include (TaaS). The successful service provider will be required to maintain the installed system and train all relevant stakeholders on the installed security system equipment.

2. Supporting Clauses

2.1 Scope

2.1.1 Purpose

The purpose of this document is to procure outcome-based security services that integrate advanced technology solutions with physical guarding measures to protect Eskom facilities within the Central East Cluster -KZN Zones through measurable performance outcomes. This is a five-year contract, with payments distributed equally over the contract period.

All equipment, technology and systems supplied and installed under this contract shall remain vested in the Service provider for the duration of the contract. Upon expiry of the contract and successful completion of the handover process, ownership shall transfer to Eskom at no additional cost. The Service provider shall remain responsible for all maintenance, licensing, insurance, replacement and operational support until ownership is formally transferred to Eskom

The technology installed must comply with Eskom technical standards as a minimum requirement, with higher specifications preferred where technically and commercially viable. Tenderers may submit proposals for multiple zones; however, successful bidders will be permitted to operate in a single zone only.

1.1.2. Applicability

This document shall apply to Central East Cluster -KZN Zones.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

1.1.3. Effective date

This document is effective from the date of signature.

2.2 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] ISO 9001 Quality Management Systems

[2] 559-970769434 Scope of Work Statements for Guarding Contracts – Guideline Document

[3] 240-102220945 Specification for Integrated Access Control System for Eskom sites

[4] 240-91190304 Specification for CCTV Surveillance with Intruder Detection

[5] 240-86738968 Specification for Integrated Security Alarm System for Protection of Eskom Installations and its subsidiaries

[6] 240-170000096 Physical security integration standard

[7] 240-170000257 Technical Evaluation Criteria for the Integrated Security System

[8] 240-170000691 Standard for Intrusion pre-detection systems used at Eskom sites

[9] 240-78980848 Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom installations and its subsidiaries

[10] 240-171000171 Commissioning guideline for secondary plant physical security system

[11] 240-180100001 Secondary Plant Security Systems Maintenance Procedure

2.2.2 Informative

[12] N/A

2.3 Definitions

Definition	Explanation
Tender	Refers to an open or closed competitive request for quotations / prices against a clearly defined scope / specification.
Integrated Access Control System	It is an electronic system that aims to collaborate and align efforts across the logical and physical security domains to standardise access control within Eskom.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Definition	Explanation
Control Centre	Where alarms and CCTV footage are monitored and needed response/s initiated from. The alarms and CCTV footage can be aggregated to a national security control centre that can initiate requisite actions from a national perspective.

2.4 Abbreviations

Abbreviation	Explanation
OBC	Outcome-Based Contract
CCTV	Closed Circuit Television
GPS	Global Positioning System
KPI	Key Performance Indicator
RFP	Request for Proposal
SSP	Security Solutions Physical
PFMA	Public Finance Management Act
EPSCMP	Eskom Procurement and Supply Chain Management Procedure

2.5 Roles and Responsibilities

a) **Eskom responsibilities**

a. Appoint the Contract Manager, Service Manager and other authorised representatives responsible for contract administration, operational coordination and acceptance of deliverables.

b. Provide the Service provider with approved site information, access requirements, applicable Eskom standards, risk assessments and the agreed rollout priorities necessary for implementation.

c. Review and approve the Service provider's implementation plan, technical designs, integration architecture, commissioning records and handover documentation before the relevant work proceeds or is accepted.

d. Coordinate access to Eskom sites and facilitate engagement with relevant site owners, zone Security Managers, Information Technology, Telecommunications and other affected stakeholders.

e. Monitor the Service provider's performance against the scope, rollout plan, service levels and key performance indicators, and issue instructions, early-warning

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

responses and corrective-action requirements through the authorised Eskom representative.

f. Provide authorised Eskom personnel for user acceptance testing, operational monitoring, training and formal handover of the installed systems and associated records.

b) **successful bidder responsibilities**

i. Use the latest approved revision of this document and comply with all applicable legislation, contractual requirements, Eskom standards, approved designs and authorised instructions.

ii. Prepare and submit for Eskom's approval a detailed, risk-based implementation and rollout plan covering design, installation, integration, testing, commissioning, training, maintenance and handover activities for the awarded zone.

iii. Supply, install, configure, integrate, test, commission, operate and maintain the physical guarding and security technology solutions required under the contract.

iv. Establish and operate the centralised control room where this forms part of the awarded scope, and ensure that all designated alarms, video feeds, access-control systems and communication links are securely integrated and continuously available.

v. Where the Service provider is appointed for a zone but not for establishment of the centralised control room, connect and maintain the zone's alarms, video feeds and related systems to the Eskom-approved centralised control room in accordance with the approved integration requirements and or link such alarm, video feeds and related systems to his own control room until Eskom control room is ready to connect such systems.

vi. Provide suitably qualified, competent and appropriately registered personnel, together with all required licences, equipment, software, warranties, support services and statutory certifications for the duration of the contract.

vii. Maintain complete and accurate design, asset, configuration, maintenance, incident, performance and training records, and submit reports in the form and frequency required by Eskom.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

viii. Promptly notify the Eskom Service Manager of risks, delays, defects, security incidents, integration constraints or other matters that may affect cost, time, performance or continuity of service, and implement approved corrective measures.

ix. Protect Eskom information and system data, provide authorised Eskom personnel with secure real-time monitoring access, and comply with Eskom information-security requirements and applicable data-protection legislation.

x. At contract expiry or termination, complete the formal handover of all applicable assets, data, licences, credentials, warranties, manuals, system backups, records and operational knowledge in accordance with the contract's ownership and handover provisions.

2.6 Process for Monitoring

Monitoring will be conducted through a layered governance structure to ensure compliance with PFMA, EPSCMP, the Constitution and alignment with Eskom's long-term security objectives:

- **Contract Manager**: Oversees contract execution, tracks supplier performance against agreed outcomes and enforces consequence management.
- **SCM Oversight**: Designs and governs the procurement process, ensuring compliance with PFMA and procurement regulations.
- **Internal Audit Review**: Provides independent assurance through periodic reviews of performance data, risk management and governance controls.
- **Line Division Managers**: Provide operational input and day-to-day monitoring, supporting continuous improvement and identifying areas for enhancement.

2.7 Related/Supporting Documents

The successful bidder or bidders will be required to provide comprehensive security services across the three Central East Cluster -KZN Zones, subject to operational requirements. Services must be tailored to four distinct risk tiers, each with unique threat profiles and operational challenges.

The site-classification framework below defines the minimum-security outcomes required across the Central East Cluster -KZN Zones. It must be read together with the scope of work, technology integration requirements, service-level expectations, and KPI framework contained in this document.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

2.8. Classification of Sites

Tier 1: High-Risk Critical Infrastructure

- **Sites**: Key substations, national control centres, Regional Distribution Centres (RDCs) /Warehouse.
- **Threat Profile**: Organised crime syndicates; coordinated theft, vandalism and sabotage; sophisticated external attacks; insider-enabled security breaches; cyber-physical compromise of integrated security systems; violent intrusion; protest action and civil unrest; and deliberate disruption of critical electricity infrastructure and essential services.

- **Operational Challenge**:
- Continuous 24/7 protection
- Maximum security protocols
- Zero tolerance for service disruption

Tier 2: Critical Operational Sites (Medium–High Risk)

- **Sites**: Distribution substations, Customer Network Centres (CNCs), regional offices, warehouses, walk-in centres, training centres
- **Threat Profile**: Copper theft syndicates, equipment vandalism, opportunistic crime, protest action
- **Operational Challenge**:

- Effective security coverage
- Cost optimization without compromising safety
- Scalable response strategies

Tier 3: Standard Operational Sites (Low–Medium Risk)

- **Sites**: Mini substations, customer hubs, secondary facilities
- **Threat Profile**: Opportunistic theft, vandalism, trespassing, protest action

- **Operational Challenge**:

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

- Basic security measures
- High cost-efficiency
- Preventive deterrence

Tier 4: Low-Risk Remote Sites (Minimum Security)

- **Sites**: Vacant properties, remote mini-substations, low-value storage units
- **Threat Profile**: Trespassing, minor vandalism, environmental hazards, protest action
- **Operational Challenge**:

- Remote monitoring solutions
- Minimal physical presence
- Budget-conscious surveillance

2.9. Contract Duration

The contract for the provision of services shall be scheduled for a period of five years.

2.10. Documentation

Prior to installation, the service provider shall produce a technical design that shall be signed off for acceptance by a suitably qualified Eskom engineer. The service provider shall maintain full documentation of which sites have undergone installation, what equipment has been installed, the configuration of the systems, as well as a system backup. A copy of the backups of the systems shall be given to Eskom for archiving and disaster management preparations. After installation, the service provider shall produce all applicable operator, maintenance and technical manuals. The Service provider shall submit all applicable operator, maintenance and technical manuals to Eskom after installation and commissioning, and before final acceptance of the relevant system or site. The manuals shall be updated following any system modification or upgrade, and a complete and current set shall be included in the final handover documentation at contract expiry or termination.

2.11. Technology Implementation

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Within the period specified in the contract data or applicable Task Order, the Service provider shall submit a detailed implementation plan to the Eskom Service Manager for written approval. No installation work may commence until Eskom has approved the relevant technical design, implementation plan and Task Order and has confirmed site access. The plan shall specify the implementation sequence for each site, prioritised according to the approved site risk tier, threat assessment and operational requirements, and shall include milestones, responsibilities, resource requirements, dependencies, installation dates, integration, testing, commissioning, training and handover activities. Any proposed deviation from the approved plan shall be supported by an early-warning notification and shall require the Service Manager's prior written approval.

2.12. Performance review meeting

The Eskom Service Manager shall convene and chair a formal performance review meeting once every calendar month. The Service provider's authorised contract representative and relevant operational and technical representatives shall attend. Relevant Eskom representatives, including the Contract Manager, zone Security Manager, site owner and assurance functions, may attend where required. The Service provider shall submit the monthly performance report, KPI scorecard and all supporting evidence to the Service Manager at least three working days before the meeting.

The meeting shall review performance against the scope, Task Orders, approved implementation plan, service levels and KPIs; security incidents and losses; guard deployment; response times; system availability and faults; maintenance; compliance; risks and early warnings; corrective actions; implementation progress; stakeholder feedback; and invoicing support. Decisions and actions shall be recorded in formal minutes and an action register identifying the responsible person and due date. The Service provider shall submit the draft minutes and updated action register to the Service Manager within two working days after the meeting for confirmation.

The Service Manager may convene an additional ad hoc performance meeting on reasonable notice, or immediately where a serious incident, material risk, service failure or operational emergency requires urgent attention. The Service provider's failure to attend, submit required reports or implement agreed corrective actions shall constitute non-performance and may result in escalation or contractual remedies. Participation in a performance review meeting shall not limit or waive any contractual right or remedy available to Eskom.

2.13. Termination due to poor performance

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Any termination for poor performance shall be administered strictly in accordance with NEC3 Term Service Contract core clauses 90 to 93, as amended by the Contract Data and any applicable Z clauses. Poor performance shall not, by itself, constitute an additional ground for termination. Eskom may rely on the applicable Service provider-default reason in clause 91 only where the verified failure amounts to a substantial failure by the Service provider to comply with its obligations to Provide the Service.

Where the Service Manager considers that such a substantial failure has occurred, the Service Manager shall notify the Service provider of the default in writing, identify the contractual obligation not complied with and state that the failure is considered substantial. The Service provider shall promptly take corrective action and provide the Service Manager with the supporting recovery information required for monitoring. The Service provider shall have the four-week period prescribed by the NEC3 TSC to put the default right, unless the contract has been validly amended to provide otherwise.

If the Service provider does not put the notified default right within that period, the Employer may notify the Service provider and the Service Manager that it wishes to terminate for the applicable reason stated in the NEC3 TSC termination table. The Service Manager shall issue a termination certificate promptly only if the stated reason complies with the contract. Termination takes effect when the termination certificate is issued and shall not be effected merely through a KPI score, performance-review decision, warning, non-conformance notice or instruction to stop work.

Upon issue of the termination certificate, the Parties and the Service Manager shall follow the procedures applicable to that termination reason under clause 92, including cessation of the affected Service where required, protection of the Affected Property, removal or handover of Equipment and other items as instructed, delivery of records, data, licences, credentials, manuals and system backups, and reasonable cooperation necessary to maintain security-service continuity. Any instruction for continued or transition services shall be given and assessed in accordance with the contract.

The amount due on termination shall be assessed in accordance with clause 93 and the payment basis linked in the NEC3 TSC termination table to the certified reason for termination. Service credits, deductions, withholding, set-off, recovery of losses or termination of an individual Task Order may be applied only where expressly permitted by the contract. Nothing in this clause creates an automatic right to terminate after three consecutive months of KPI failure or permits the Service Manager to terminate the contract on behalf of the Employer.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

2.14. Early Termination of Contract

Any early termination shall be effected only for a reason permitted under NEC3 Term Service Contract clauses 90 and 91, as amended by the Contract Data and applicable Z clauses, and in accordance with the notice and termination-certificate procedure prescribed by the contract. The Employer may terminate for a reason available to it under the termination table. The Service provider may terminate only for a reason expressly available to the Service provider under that table; the Service provider may not terminate merely by giving notice for convenience.

Termination shall take effect only when the Service Manager issues the termination certificate. Following certification, the Parties and the Service Manager shall apply the procedures in clause 92 and the assessment of the amount due in clause 93 corresponding to the certified termination reason.

Assets supplied and owned by the Service provider shall not transfer automatically on early termination. Where Eskom requires such assets for continuity of the Service, the Service Manager may instruct their protection, continued use, removal or handover only to the extent permitted by the applicable clause 92 procedure. Eskom may acquire Service provider-owned assets only through the payment basis applicable under clause 93 or under a separate written sale agreement concluded by authorised representatives of both Parties. Any agreed purchase price shall be supported by an independent valuation using the asset register, age, condition, remaining useful life and verifiable depreciation methodology, and shall exclude amounts already recovered through the Prices.

Pending completion of the termination procedures and any agreed transition arrangements, the Service provider shall protect the Affected Property, preserve all Eskom data and records, and cooperate in the orderly transfer of security operations in accordance with the contract.

2.15. Surges and emergencies

The Service provider shall maintain the preparedness, contingency arrangements and standby capability stated in the Service Information and applicable Service Level Agreement. A surge or emergency deployment shall be initiated only by an instruction from the Service Manager, except where immediate action is reasonably necessary to protect life, Eskom personnel, the Affected Property, critical infrastructure or continuity of electricity supply and it is impracticable to obtain the instruction beforehand. In such circumstances, the Service provider shall take only the minimum reasonable action required to contain the immediate risk and shall notify the Service Manager without delay.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

2.15.1. Support obligations and contract administration

The Service Manager's instruction shall identify the event, affected location, required outcome, resources or capabilities required, commencement time, expected duration, reporting arrangements and any operational constraints.

The Service provider shall acknowledge the instruction promptly, deploy within the response period stated in the Service Level Agreement, keep contemporaneous records of personnel, equipment, time, incidents and costs, and provide status updates at the frequency directed by the Service Manager.

The Service provider shall give an early warning as soon as it becomes aware of any matter that could increase the Prices, delay performance or impair the Service. Where the instruction changes the Service Information, it shall be administered as a compensation event under NEC3 TSC clause 60.1(1) and the applicable clauses 61 to 65. Where Option X19 applies and the work constitutes a separate task, the Service Manager shall issue a Task Order in accordance with X19 and the approved Task Order process. No additional payment is due for surge or emergency capability already included in the Prices. Additional instructed work shall be assessed using the applicable Price List rates or, where no applicable rate exists, Defined Cost plus the Fee in accordance with the contract.

An oral emergency direction shall be confirmed in writing by the Service Manager as soon as practicable and shall not remove the requirement to follow the applicable NEC3 TSC notification, quotation and assessment procedures.

2.15.2. Definition of Surges

For purposes of this contract, a **surge** means a temporary, material increase in the volume, geographic coverage, operating hours, resource levels or response capability required to Provide the Service above the normal operational baseline stated in the Service Information, Price List, applicable Task Order or approved deployment plan.

A surge is planned or time-limited additional demand and does not, solely by reason of increased workload, constitute an emergency. The Service Manager shall determine whether the additional

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

requirement falls within the priced baseline capability or requires an instruction changing the Service Information or, where Option X19 applies, a separate Task Order.

The instruction shall define the scope, affected sites, required resources, commencement time, expected duration, reporting requirements and demobilisation criteria.

Repeated, foreseeable or continuing demand shall not be treated indefinitely as a surge and shall be reviewed for incorporation into the Service Information and Prices through the applicable NEC3 TSC procedure. Surges may arise from, among other things:

- security incidents or threats to Eskom infrastructure.
- labour unrest, protests, or civil disturbances in affected areas.
- major public events or seasonal spikes requiring heightened protection.
- network failures, vandalism, or sabotage resulting in increased demand for guarding and monitoring.
- natural disasters, extreme weather, or other force majeure events impacting the operational environment.

2.15.3. Definition of Emergencies

For purposes of this contract, an **emergency** means a sudden, unforeseen or rapidly escalating event that presents an actual or imminent material threat to life, public safety, Eskom personnel, the Affected Property, critical electricity infrastructure, security-system integrity or continuity of electricity supply and requires immediate action that cannot reasonably await the normal instruction, quotation or Task Order process.

An increase in workload, staffing demand or geographic coverage shall not constitute an emergency unless it meets this threshold.

The Service Manager shall determine whether an event is to be administered as an emergency and shall issue an instruction defining the immediate protective outcome, affected location, authorised resources, reporting requirements and, where practicable, the expected duration. Where delay in obtaining an instruction would materially increase the risk, the Service provider shall take only the minimum reasonable action necessary to preserve life, protect the Affected Property, contain the threat and maintain essential security services, and shall notify the Service Manager without delay.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The Service provider shall maintain contemporaneous records of the event, decisions, deployment, time, resources and costs. Once the immediate threat has been stabilised, any continuing or additional work shall be confirmed by a written Service Manager instruction and administered under the applicable NEC3 TSC compensation-event procedure or, where Option X19 applies and the work constitutes a separate task, through a Task Order. Emergencies may include, but are not limited to:

- fire, flood, storm, or similar natural disasters
- major equipment failure, explosions, or hazardous incidents.
- criminal acts such as theft, arson, sabotage, or violent attacks directed at Eskom assets or personnel.
- any event threatening continuity of electricity supply or posing a risk to public safety.

2.15.4. Response Times and Flexibility

Before the starting date, the Service provider shall submit for the Service Manager's acceptance a surge and emergency response plan aligned with the Service Information and Service Level Agreement.

The plan shall define, for each site-risk category and event type, the notification channel, acknowledgement time, mobilisation time, arrival-on-site or remote-intervention time, required capability, escalation route, backup arrangements and reporting frequency.

Response time shall be measured from the time the Service provider's designated control point receives the Service Manager's instruction or, where immediate protective action is permitted under section 2.14.3, from the time the Service provider first becomes aware of the event.

Compliance shall be evidenced by time-stamped control-room logs, communication records and GPS or system records, as applicable.

The Service provider shall maintain the minimum standby resources and contingency arrangements included in the Prices and shall deploy them within the corresponding SLA period. Any requirement to increase staffing, equipment, geographic coverage or operating hours beyond the priced baseline shall require a Service Manager instruction and shall be administered under the applicable NEC3 TSC compensation-event procedure or, where Option X19 applies, through a Task Order.

The Service provider shall promptly notify the Service Manager of any actual or anticipated inability to meet a response time, give an early warning where the matter could increase the Prices, delay performance or impair the Service, and implement the agreed mitigation or recovery measures.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Redeployment or upscaling shall not reduce security below the approved minimum at another Eskom site without the Service Manager's prior written acceptance. The instruction or Task Order shall state the review point and demobilisation criteria, after which the Service provider shall return resources to the approved baseline unless otherwise instructed.

2.15.5. Compensation and Cost Recovery

Surge and emergency services included in the Service Information, Service Level Agreement, Price List, accepted Task Order or Service provider's priced standby obligations are included in the Prices and do not entitle the Service provider to additional payment.

Additional payment arises only where the Service Manager gives an instruction that changes the Service Information and the event is notified and administered as a compensation event under NEC3 TSC clauses 60 to 65, or where Option X19 applies and the Service Manager issues a Task Order for a separate task. The Service provider shall comply with the applicable notification time limits and shall not assume that an instruction, emergency response, early warning, operational request or expenditure automatically creates an entitlement to additional payment.

Where a compensation event is notified, the Service provider shall submit its quotation within the period required by the contract and shall include the forecast effect on the Prices, the timing of the Service and any Key Dates, together with assumptions and sufficient supporting detail. The quotation shall be assessed using the applicable Price List rates where the contract requires their use or, where applicable, forecast Defined Cost plus the Fee in accordance with the selected main Option, the Schedule of Cost Components and the Contract Data. The assessment shall avoid duplication of amounts already included in the Prices, standby allowances, overheads, insurance, licences, maintenance obligations or any other priced provision.

For immediate emergency action taken before a written instruction could reasonably be obtained, the Service provider shall notify the Service Manager without delay and provide contemporaneous records showing the event, necessity of the action, personnel, equipment, time, location, quantities, third-party charges and resulting costs.

The Service Manager shall determine whether the work is within the existing Prices, is to be instructed as a change to the Service Information or is to be administered under an Option X19 Task Order. Costs incurred without contractual entitlement, adequate records or the required notification are not recoverable merely because they were incurred.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The Service provider shall not delay action required to protect life or the Affected Property while awaiting agreement of a quotation. Any quotation acceptance or Service Manager assessment shall be implemented in accordance with the NEC3 TSC compensation-event procedure. Acceptance of a quotation confirms the contractual assessment of the compensation event and is not approval of an invoice or evidence that the work has been completed.

2.16. Invoicing and Payment

Payment shall be administered in accordance with NEC3 Term Service Contract clauses 50 to 52, the selected Main Option, the Contract Data and any applicable Z clauses. The Service provider shall submit an application for payment on or before each assessment date stated in the Contract Data. The application shall show the amount the Service provider considers due at the assessment date, broken down by applicable Price List items, Service provided under issued Task Orders, implemented compensation events, applicable taxes and any other amount expressly permitted by the contract. The Service Manager's obligation to assess the amount due at each assessment date is not suspended or deferred solely because the Service provider has not submitted an application or because supporting information is incomplete.

2.16.1. Supporting documentation

Each application shall be supported by the relevant Service Manager instructions, issued Task Orders, verified attendance and deployment records, approved timesheets where applicable, system-availability and maintenance records, delivery or acceptance evidence, KPI scorecards, compensation-event references, accepted quotations or Service Manager assessments, and any other substantiation required by the Service Information or Contract Data. Submission of supporting records does not constitute acceptance of the Service or agreement that an amount is due. Where information is missing or cannot be verified, the Service Manager shall make the assessment using the information reasonably available and may correct the amount in a later assessment in accordance with the contract.

2.16.2. Assessment and certification

At each assessment date, the Service Manager shall assess the amount due as the Price for Service Provided to Date under the selected Main Option, plus other amounts to be paid to the Service provider, less amounts to be paid by or retained from the Service provider under the contract. The assessment shall include implemented compensation events and Service provided under issued Task Orders as applicable, take account of amounts previously certified, and apply only those additions, deductions or retentions expressly permitted by the contract. Unless the Contract Data or

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

an applicable Z clause validly provides otherwise, the Service Manager shall certify the amount due within one week after the assessment date. The Service Manager may correct a previous assessment in a later payment certificate as permitted by the NEC3 TSC.

2.16.3. Invoice submission: Following receipt of the Service Manager's payment certificate, the Service provider shall submit a valid tax invoice for the amount certified. The invoice shall quote the contract number, purchase order number, assessment period, payment-certificate reference and all information required by applicable tax legislation and Eskom's approved invoice process and shall be submitted through the channel and to the address stated in the Contract Data or notified in writing. These administrative requirements do not alter the assessment date, the certification period, the final date for payment or the Service provider's entitlement to interest under the NEC3 TSC unless the Contract Data or an applicable Z clause expressly provides otherwise.

2.16.4. Payment and interest: Eskom shall pay the amount due within the period stated in the Contract Data. Unless the Contract Data or an applicable Z clause validly provides otherwise, payment is due within three weeks after the assessment date. Interest shall be payable in accordance with NEC3 TSC clause 51 on late payment and on any underpayment corrected in a later certificate. Payment does not constitute acceptance of defective or incomplete Service, waiver of any contractual right, or confirmation that supporting information was accurate.

2.16.5. Incomplete, incorrect or disputed submissions: If an application or invoice is incomplete, inaccurate, duplicated, unsupported or submitted through an incorrect channel, the Service Manager or Eskom shall notify the Service provider of the deficiency, and the Service provider shall correct it promptly. A deficient application or invoice does not remove the Service Manager's obligation to assess and certify the amount due within the contractual timetable. Any disagreement regarding an assessment or amount due shall be dealt with under the contract's dispute-resolution procedure and shall not entitle the Service provider to suspend or reduce the Service except where the contract expressly permits.

2.16.6. Deductions and financial controls: Low service damages may be deducted only where Secondary Option X17 has been selected, and the applicable service level and amount are stated in the contract. Any other service credit, Price List adjustment, retention, contractual deduction, recovery of overpayment or set off may be applied only where expressly permitted by the NEC3 TSC, the Contract Data, an applicable Z clause or applicable law, and shall be reflected transparently in the Service Manager's assessment and payment certificate. The Service provider shall maintain accurate financial and performance records and make them available for audit in accordance with the contract. Changes to banking details shall be accepted only through Eskom's prescribed

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

verification process and shall not be implemented solely on the basis of an invoice or informal communication.

2.17. Technology Ownership

This section shall be read with NEC3 Term Service Contract core clauses 70 to 72, 80 to 86 and 90 to 93, the selected Main Option, the Contract Data, the Service Information and applicable Z clauses. The Service Information shall include a Technology Asset Transfer Schedule identifying each asset category, title holder during the service period, risk allocation, insurance responsibility, transfer status, transfer trigger, licence requirements, residual-value treatment and handover evidence. If there is any conflict, the NEC3 TSC conditions as validly amended take precedence.

2.17.1. Classification and title during the contract

The Technology Asset Transfer Schedule shall distinguish between Equipment used by the Service provider to Provide the Service and Plant and Materials intended to form part of the Affected Property or to transfer to Eskom. Unless the Contract Data, Service Information, an issued Task Order or an authorised amendment to the contract states otherwise, Service provider Equipment and Service provider-supplied technology shall remain owned by the Service provider during the service period. Connection, installation, commissioning, payment for the Service or use by Eskom does not of itself transfer title. No side agreement or informal communication changes ownership unless incorporated through the contract's authorised amendment and communication procedures.

2.17.2. Risk, insurance and Service provider obligations

Ownership, risk and insurance are separate matters. The Parties' risks and the required insurances shall be those stated in NEC3 TSC clauses 80 to 86, the Insurance Table, Contract Data and applicable Z clauses, irrespective of title. The Service provider shall perform the financing, licensing, warranty, maintenance, repair, replacement, cybersecurity, support and obsolescence-management obligations stated in the Service Information and included in the Prices. Removal, disabling, substitution or disposal of installed technology shall be governed by the Service Information and any instruction the Service Manager is authorised to give under the contract. The Service provider shall not encumber any asset identified for transfer to Eskom.

2.17.3. Eskom access and operational rights

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The Service Information shall state Eskom's required real-time, secure and role-based access to surveillance, alarm, access-control and related systems, together with the required interfaces, connectivity, credentials, audit trails, cybersecurity controls and continuity arrangements. These requirements are included in the Prices to the extent stated in the Service Information. Any later instruction changing those requirements shall be administered under the applicable NEC3 TSC compensation-event procedure. Eskom's access and use do not of themselves transfer title or alter the contractual allocation of risk.

2.17.4. Asset register and configuration control

The Service provider shall maintain and submit to the Service Manager, at the intervals stated in the Service Information and before handover, a current asset and configuration register recording each item's NEC classification, location, description, make, model, serial number, title holder, risk and insurance responsibility, installation and commissioning date, condition, warranty, licence, maintenance history, configuration, replacement status and transfer status. Review, comment or acceptance of the register by the Service Manager does not transfer title, risk or liability or relieve the Service provider of its obligations.

2.17.5. Eskom data and information

As expressly provided in the Service Information and applicable data-processing provisions, Eskom owns its source data and all surveillance recordings, access-control records, alarm and incident data, reports, system logs and configurations created specifically for Eskom, except for embedded Service provider or third-party intellectual property identified in the contract. The Service provider acts as custodian and authorised processor only for purposes of Providing the Service and shall not assert a lien over, withhold, exploit, disclose, delete or retain Eskom data except as permitted by the contract or required by law. Storage, access, backup, retention, export, incident notification and secure destruction shall comply with the Service Information, POPIA and applicable Eskom information-security requirements.

2.17.6. Intellectual property and licences

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Pre-existing intellectual property remains with its owner. The Contract Data, Service Information and applicable Z clauses shall identify all intellectual-property rights, source-code or escrow requirements, third-party licences, subscriptions, warranties and support agreements needed to operate, maintain, modify and support technology during and after handover. For assets identified for transfer, the Service provider shall procure for Eskom, from the transfer date, the perpetual or other expressly stated rights required for Eskom and its replacement service providers to operate and support the systems. The Service provider shall disclose before installation any non-transferable, time-limited or restrictive licence. No broader right is created by this section unless expressly stated in the contract.

2.16.7. Transfer at expiry

Only Equipment, Plant and Materials expressly identified for transfer in the Technology Asset Transfer Schedule shall pass to Eskom. The transfer trigger and date shall be the objective condition stated in that schedule, which may include expiry of the service period, completion of specified tests, correction of notified Defects, delivery of required records and confirmation by the Service Manager where the contract expressly grants that function. The Prices include the agreed acquisition or residual value, transferable warranties and licences, documentation, training and planned handover; transfer therefore occurs without further payment except where the contract expressly states otherwise. Assets shall transfer free of liens and encumbrances.

2.17.8. Handover, testing and Defects

The Service provider shall submit the handover plan by the date stated in the Service Information. The plan shall cover asset verification, condition assessment, testing, correction of notified Defects, licence transfer, data export, backup and restoration testing, cybersecurity checks, administrator credentials, manuals, as-built records, training and knowledge transfer. Testing, notification and correction of Defects shall follow the NEC3 TSC procedures, and any periods stated in the Contract Data and Service Information. A handover record evidences compliance and transfer where the contract so provides but does not constitute a general final-acceptance certificate or relieve the Service provider of obligations that expressly survive transfer.

2.17.9. Early termination

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Service provider-owned Equipment and technology do not transfer automatically on early termination. Their protection, use, removal or transfer shall follow NEC3 TSC clauses 90 to 93, the procedure and payment basis applicable to the certified termination reason, the Contract Data and applicable Z clauses. Eskom may acquire Service provider-owned assets only where the applicable termination procedure and payment basis permit it or through an authorised amendment or purchase agreement that does not contradict the termination provisions. Any separate purchase price shall be supported by verifiable valuation and shall exclude amounts already recovered through the Prices.

2.17.10. Exit and transition obligations

The Service Information shall define and price the planned exit and transition Service, including delivery of data in an open and secure format, transfer or revocation of access rights, return of Eskom property, data migration, secure deletion and certification, assistance to a replacement service provider and continuity arrangements. On expiry or termination, the Service provider shall perform those stated obligations and comply with authorised instructions given under the contract. Any additional transition work not included in the Prices shall be instructed and assessed only in accordance with the applicable NEC3 TSC procedure.

3. Scope and Risk Levels

The scope of this engagement covers all three zones within the Central East Cluster -KZNfacilities, categorized by their risk levels and corresponding minimum-security requirements as detailed below:

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Table 1: Pietermaritzburg Zone substations/Area offices/offices and network infrastructure (268 sites).

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 4	**63 substations**	**Outcome:** Detect and deter unauthorised entry, trespassing, opportunistic theft and vandalism, and enable the control room to verify an alarm event remotely within the response time stated in the Service Level Agreement. Verified incidents shall be recorded, classified and escalated, and the appropriate response resource shall be dispatched in accordance with the approved incident-response procedure. **Integrated Video Alarms:** Motion or perimeter breach detection with immediate video verification capabilities. **24/7 Remote Monitoring:** Centralized monitoring of alarms and video feeds. **Tiered Armed Response:** Pre-arranged rapid armed response services triggered by verified alarms, with defined Service Level Agreements (SLAs). Note: Deployments shall occur as and when required, in response to operational requirements

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 2	3 Area offices 1 Warehouse 2 Training Centres 16 Customer Network Centres 10 Walk in Centres 1 Control Centre 1 Radio Site	**Outcome:** Prevent unauthorized access, detect and deter criminal activity, and enable swift, coordinated response. **Comprehensive CCTV Surveillance:** High-definition cameras with analytical capabilities (e.g., motion, loitering) covering critical areas. **Advanced Integrated Alarm Systems:** Multi-layered sensors (e.g., perimeter, vibration, volumetric) linked to the CCTV and access control. **Integrated Access Control:** Card/biometric access for all entry/exit points, with audit trails and remote management capabilities. **24/7 Centralized Monitoring:** Dedicated control room operators for continuous oversight, alarm management, and dispatch. **Rapid Armed Response:** Priority armed response with shorter SLAs, pre-identified routes, and site familiarization.
		On-site Deterrence: Visible, uniformed Security Guards (C-grade, ideally armed or with clear escalation protocols to armed response) for access control and initial visual deterrence during vulnerable periods (e.g., peak crime times, specific operational windows). Their primary role is access management and observation, relying on technology and armed response for engagement. Note: Deployments shall occur as and when required, in response to operational requirements

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 3	**36 Substations**	**Outcome:** Maximize prevention of sophisticated attacks, ensure immediate detection, and enable overwhelming response to protect critical assets. **AI-Powered Advanced Surveillance:** High-definition cameras with AI analytics for anomaly detection, facial recognition (where permissible), object tracking, and predictive analysis, integrated with a Public Address (PA) system for audio warnings. **Multi-Layered Perimeter Défense:** Advanced sensors (e.g., fibre optic fence, ground radar, thermal imaging) coupled with physical hardening measures. **Robust Integrated Access Control:** Biometric systems, anti-pass back, and visitor management. **24/7 Dedicated Monitoring & Intelligence:** Proactive monitoring by highly trained operators, leveraging security business intelligence feeds for pre-emptive actions. **Immediate Armed Response:** Direct armed response deployment with the shortest possible SLAs, possibly including dedicated on-call teams or co-location agreements. **Highly Trained On-site Security Guards (Armed Recommended):** Visible, well-trained and armed security personnel (or highly trained unarmed guards supported by immediate armed response presence) to provide a robust physical barrier, rapid initial response, and

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
		coordination with external armed response. Patrols should be intelligence driven. Note: Deployments shall occur as and when required, in response to operational requirements.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 3&4	**All Feeder Lines, Pole Mounted Transformers, Reclosers, lines in operation and lines not in operation linked to substations**	**Outcome:** Detect and deter widespread opportunistic theft and vandalism across distributed assets, enabling targeted intervention. **Targeted Drone Surveillance:** Regular or on-demand drone patrols with high-resolution and thermal imaging to identify suspicious activity or damage along lines and at remote assets. **IoT/Smart Sensor Deployment:** Intelligent sensors on high-value pole-mounted transformers and reclosers to detect tampering, removal, or unusual activity, providing real-time alerts. **GPS Tracking & Asset Tagging:** For portable or high-value components. **Proactive Remote Monitoring:** Alerts from sensors and drone feeds are centralized for analysis and dispatch. **Mobile Armed Response:** Dedicated mobile armed response teams covering specific geographic clusters, dispatched based on alerts, and utilizing intelligence-led patrols. **Community Engagement & Whistleblower Programs:** Encouraging public reporting of suspicious activity. Note: Deployments shall occur as and when required, in response to operational requirements

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Table 2:Empangeni Zone substations/Area offices/offices and network infrastructure (148 sites)

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 4	**32 Substations**	**Outcome:** Deter casual intrusion and enable rapid incident verification. **Integrated Video Alarms:** Motion or perimeter breach detection with immediate video verification capabilities. **24/7 Remote Monitoring:** Centralized monitoring of alarms and video feeds. **Tiered Armed Response:** Pre-arranged rapid armed response services triggered by verified alarms, with defined Service Level Agreements (SLAs). Note: Deployments shall occur as and when required, in response to operational requirements

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 2	**1 area Office** **1 Empangeni Warehouse** **56 Substations** **18 Network Centre** **6 Hubs** **6 Radio Site**	**Outcome:** Prevent unauthorized access, detect and deter criminal activity, and enable swift, coordinated response. **Comprehensive CCTV Surveillance:** High-definition cameras with analytical capabilities (e.g., motion, loitering) covering critical areas. **Advanced Integrated Alarm Systems:** Multi-layered sensors (e.g., perimeter, vibration, volumetric) linked to the CCTV and access control. **Integrated Access Control:** Card/biometric access for all entry/exit points, with audit trails and remote management capabilities. **24/7 Centralized Monitoring:** Dedicated control room operators for continuous oversight, alarm management, and dispatch. **Rapid Armed Response:** Priority armed response with shorter SLAs, pre-identified routes, and site familiarization. **On-site Deterrence:** Visible, uniformed Security Guards (C-grade, ideally armed or with clear escalation protocols to armed response) for access control and initial visual deterrence during vulnerable periods (e.g., peak crime times, specific operational windows). Their primary role is access management and observation, relying on technology and armed response for engagement. Note: Deployments shall occur as and when required, in response to operational requirements

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 3	**28 Substations**	**Outcome:** Maximize prevention of sophisticated attacks, ensure immediate detection, and enable overwhelming response to protect critical assets. **AI-Powered Advanced Surveillance:** High-definition cameras with AI analytics for anomaly detection, facial recognition (where permissible), object tracking, and predictive analysis, integrated with a Public Address (PA) system for audio warnings. **Multi-Layered Perimeter Défense:** Advanced sensors (e.g., fibre optic fence, ground radar, thermal imaging) coupled with physical hardening measures. **Robust Integrated Access Control:** Biometric systems, anti-pass back, and visitor management. **24/7 Dedicated Monitoring & Intelligence:** Proactive monitoring by highly trained operators, leveraging security business intelligence feeds for pre-emptive actions. **Immediate Armed Response:** Direct armed response deployment with the shortest possible SLAs, possibly including dedicated on-call teams or co-location agreements. **Highly Trained On-site Security Guards (Armed Recommended):** Visible, well-trained and armed security personnel (or highly trained unarmed guards supported by immediate armed response presence) to provide a robust physical barrier, rapid initial response, and coordination with external armed response. Patrols should be intelligence driven. Note: Deployments shall occur as and when required, in response to operational requirements

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Table 3: Newcastle Zone substations/Area offices/offices and network infrastructure (188 sites)

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 4	**71 Substations**	**Outcome:** Deter casual intrusion and enable rapid incident verification. **Integrated Video Alarms:** Motion or perimeter breach detection with immediate video verification capabilities. **24/7 Remote Monitoring:** Centralized monitoring of alarms and video feeds. **Tiered Armed Response:** Pre-arranged rapid armed response services triggered by verified alarms, with defined Service Level Agreements (SLAs). Note: Deployments shall occur as and when required, in response to operational requirements

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 2	**2 Area Offices** **1 Warehouse** **79 Substations** **11 Control Network Centre** **7 Radio Site**	**Outcome:** Prevent unauthorized access, detect and deter criminal activity, and enable swift, coordinated response. **Comprehensive CCTV Surveillance:** High-definition cameras with analytical capabilities (e.g., motion, loitering) covering critical areas. **Advanced Integrated Alarm Systems:** Multi-layered sensors (e.g., perimeter, vibration, volumetric) linked to the CCTV and access control. **Integrated Access Control:** Card/biometric access for all entry/exit points, with audit trails and remote management capabilities. **24/7 Centralized Monitoring:** Dedicated control room operators for continuous oversight, alarm management, and dispatch. **Rapid Armed Response:** Priority armed response with shorter SLAs, pre-identified routes, and site familiarization. **On-site Deterrence:** Visible, uniformed Security Guards (C-grade, ideally armed or with clear escalation protocols to armed response) for access control and initial visual deterrence during vulnerable periods (e.g., peak crime times, specific operational windows). Their primary role is access management and observation, relying on technology and armed response for engagement. Note: Deployments shall occur as and when required, in response to operational requirements

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 3	**17 Substations**	**Outcome:** Maximize prevention of sophisticated attacks, ensure immediate detection, and enable overwhelming response to protect critical assets. **AI-Powered Advanced Surveillance:** High-definition cameras with AI analytics for anomaly detection, facial recognition (where permissible), object tracking, and predictive analysis, integrated with a Public Address (PA) system for audio warnings. **Multi-Layered Perimeter Défense:** Advanced sensors (e.g., fibre optic fence, ground radar, thermal imaging) coupled with physical hardening measures. **Robust Integrated Access Control:** Biometric systems, anti-pass back, and visitor management. **24/7 Dedicated Monitoring & Intelligence:** Proactive monitoring by highly trained operators, leveraging security business intelligence feeds for pre-emptive actions. **Immediate Armed Response:** Direct armed response deployment with the shortest possible SLAs, possibly including dedicated on-call teams or co-location agreements. **Highly Trained On-site Security Guards (Armed Recommended):** Visible, well-trained and armed security personnel (or highly trained unarmed guards supported by immediate armed response presence) to provide a robust physical barrier, rapid initial response, and coordination with external armed response. Patrols should be intelligence driven. Note: Deployments shall occur as and when required, in response to operational requirements

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Network Infrastructure Tier 3&4	**All Feeder Lines, Pole Mounted Transformers, Reclosers, lines in operation and lines not in operation linked to substations**	**Outcome:** Detect and deter widespread opportunistic theft and vandalism across distributed assets, enabling targeted intervention. **Targeted Drone Surveillance:** Regular or on-demand drone patrols with high-resolution and thermal imaging to identify suspicious activity or damage along lines and at remote assets. **IoT/Smart Sensor Deployment:** Intelligent sensors on high-value pole-mounted transformers and reclosers to detect tampering, removal, or unusual activity, providing real-time alerts. **GPS Tracking & Asset Tagging:** For portable or high-value components. **Proactive Remote Monitoring:** Alerts from sensors and drone feeds are centralized for analysis and dispatch. **Mobile Armed Response:** Dedicated mobile armed response teams covering specific geographic clusters, dispatched based on alerts, and utilizing intelligence-led patrols. **Community Engagement & Whistleblower Programs:** Encouraging public reporting of suspicious activity. Note: Deployments shall occur as and when required, in response to operational requirements

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

4. Scope of Work

4.1. Physical Security Services

The Service provider Provides the physical security Service at the sites and for the periods identified in the Site Service Schedule, issued Task Orders and accepted deployment plan. The Prices include all personnel, supervision, relief resources, uniforms, personal protective equipment, vehicles, communications, licences, permits, consumables and other resources required to meet the stated service levels. A requirement outside the priced baseline is implemented only by a Service Manager instruction and, where applicable, the NEC3 TSC compensation-event procedure or an Option X19 Task Order.

Guard deployment: The Service provider provides PSIRA-registered personnel of the grades, competencies, shift patterns, post numbers, operating hours and firearm status stated for each site in the Site Service Schedule. Every post is continuously filled during the scheduled period by an authorised and site-inducted person. Absence, lateness or replacement is recorded and remedied within the applicable service level. The Service provider does not reduce or redeploy the approved baseline without the Service Manager's instruction or acceptance where the contract requires it.

Access control: The Service provider applies Eskom's approved access-control, search, key-control, visitor, vehicle and service provider-management procedures at every designated entry and exit point. Identity, authority and access rights are verified before entry; exceptions are escalated; and time-stamped access records are retained and submitted in the format and period stated in the Service Information.

Patrols and inspections: The Service provider performs patrols at the routes, frequencies, time windows and control points stated in the Site Service Schedule. Completion is evidenced by an electronic guard-tour system, GPS record or other accepted time-stamped record. Missed, incomplete or abnormal patrols are reported immediately, investigated and corrected. Vulnerabilities requiring physical, procedural or technology changes are notified as an early warning where they may increase the Prices, delay performance or impair the Service.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Incident response: The Service provider maintains 24-hour alarm-verification, dispatch and armed-response capability in accordance with the site-risk tier and Service Level Agreement. Response time is measured from the recorded dispatch time to confirmed arrival at the incident location. The Service provider records the event, preserves the scene, protects life and Eskom property, notifies the designated Eskom representative and SAPS where required, and submits preliminary and final incident reports within the stated periods.

Emergency management: The Service provider implements the accepted emergency and surge response plan, maintains the priced standby capability, follows the incident-command and escalation structure, supports evacuation and business-continuity measures, and liaises with emergency services through authorised channels. Additional resources beyond the priced baseline are instructed and assessed in accordance with section 2.15 and the NEC3 TSC.

Control-room operations: For the duration of the contract, the Service provider shall connect and continuously monitor all alarms, CCTV cameras, access-control systems, intrusion-detection devices and any other security technology installed or supported under the contract through the Service provider's control room. The Service provider shall establish and maintain a dedicated Eskom monitoring desk, staffed by suitably trained operators on a 24-hour basis, with dedicated workstations, displays, communications, incident-management capability, secure connectivity, system-health monitoring, recording capacity, resilience and cybersecurity controls as specified in the Control Room Interface Schedule. The Service provider shall provide Eskom with authorised real-time access to relevant alarms, video feeds, incident records and system-health information.

Migration to Eskom's control room: If Eskom's newly established control room is ready for operational use before expiry of the contract, the Service provider shall, on instruction from the Service Manager and in accordance with the approved migration plan, link and migrate all installed and monitored security systems from the Service provider's control room to Eskom's control room. The Service provider shall provide all interfaces, configurations, network information, licences, credentials, system backups, data mappings, as-built records and technical support included in the Prices for the planned migration; conduct end-to-end integration, failover, cybersecurity and operational acceptance testing; train authorised Eskom personnel; and maintain parallel monitoring until the Service Manager confirms that the Eskom control room is operationally ready and the migration has been successfully completed. The migration shall not interrupt monitoring, recording, alarm handling, dispatch or incident response. Any requirement that changes the stated Control Room Interface Schedule or falls outside the priced migration obligation shall be administered through the applicable NEC3 TSC instruction and compensation-event procedure.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Records and performance evidence: The Service provider maintains auditable deployment, access, patrol, incident, dispatch, response, control-room and compliance records and submits daily exceptions and monthly performance reports to the Service Manager. Records are retained, protected and made available for verification in accordance with the Service Information, POPIA and Eskom information-security requirements.

4.2. Technology Integration Services

The Service provider supplies, installs, configures, integrates, tests, commissions and supports only the technology identified for each site in the Site Technology Schedule, approved design and issued Task Order. The schedule states the minimum functional outcomes, capacity, availability, retention, interoperability, resilience and cybersecurity requirements. Technology not identified in the priced baseline is not deployed without a Service Manager instruction and the applicable NEC3 TSC procedure.

Design and approval: Before installation, the Service provider performs the required site survey and submits the technical design, bill of materials, coverage plan, network architecture, power and backup design, cybersecurity controls, integration method, test scripts and implementation programme for acceptance by the Service Manager and relevant Eskom technical authority. Acceptance does not relieve the Service provider of responsibility for the design or compliance with the contract.

CCTV and video surveillance: Cameras, recording platforms and analytics meet the applicable Eskom specifications and the measurable image-quality, field-of-view, low-light, storage, retention and availability criteria stated in the Site Technology Schedule. Coverage includes the designated perimeter, access points and critical areas, with privacy masking and lawful monitoring controls where required.

Intrusion detection and alarms: Detection devices are selected from the approved design according to the site threat and environment and are zoned, supervised and integrated for time-stamped alarm generation, video verification, health monitoring and dispatch. False-alarm performance and detection testing comply with the acceptance criteria stated in the Service Information.

Electronic access control: The Service provider provides the card, biometric or other approved authentication technology, anti-passback, visitor management, audit trail and remote administration functions stated in the Site Technology Schedule. Personal information and biometric data are processed only for approved purposes and in accordance with POPIA and Eskom requirements.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Drone services: Drone operations are provided only were identified in the priced schedule or instructed under an issued Task Order. The Service provider obtains and maintains all required aviation approvals, operator certificates, remote-pilot competencies, aircraft registrations, insurance and site or airspace permissions; submits an approved flight and safety plan; observes weather and operational limitations; protects recorded data; and provides the images, flight logs, findings and incident notifications stated in the Task Order.

Analytics and automated decision support: Analytics are limited to use cases approved in the Service Information. The Service provider states the detection objective, configuration, accuracy threshold, false-alarm tolerance, human-review process, data sources, audit trail and privacy controls. Facial recognition, behavioural profiling or predictive analysis is not activated unless expressly authorised following Eskom legal, privacy, cybersecurity and technical approval.

Integration: All new systems integrate with the Eskom-approved control room identified in the Control Room Interface Schedule using approved, documented and supportable interfaces. The Service provider supplies the required hardware, software, licences, interface documentation, network configurations and data feeds included in the Prices. Systems support the auxiliary sensors and open interfaces identified in the approved design; no undisclosed proprietary restriction may prevent operation, maintenance or future authorised integration.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Service provider control-room monitoring and migration: For the duration of the contract, the Service provider shall link all alarms, CCTV cameras, access-control systems, intrusion-detection devices and any other security technology installed or supported under the contract to the Service provider's control room and shall provide a dedicated Eskom monitoring desk staffed by suitably trained operators on a 24-hour basis. The Service provider shall provide secure connectivity, dedicated workstations, displays, communications, incident-management capability, recording, system-health monitoring, resilience and cybersecurity controls in accordance with the Control Room Interface Schedule, together with authorised real-time Eskom access to relevant alarms, video feeds, incident records and system-health information. If Eskom's newly established control room is ready for operational use before expiry of the contract, the Service provider shall, on instruction from the Service Manager and in accordance with the approved migration plan, link and migrate all installed and monitored security systems from the Service provider's control room to Eskom's control room. The Service provider shall provide the interfaces, configurations, network information, licences, credentials, system backups, data mappings, as-built records, training and technical support included in the Prices for the planned migration; conduct end-to-end integration, failover, cybersecurity and operational acceptance testing; and maintain parallel monitoring until the Service Manager confirms that Eskom's control room is operationally ready and the migration has been successfully completed. The migration shall not interrupt monitoring, recording, alarm handling, dispatch or incident response. Any requirement that changes the Control Room Interface Schedule or falls outside the priced migration obligation shall be administered through the applicable NEC3 TSC instruction and compensation-event procedure.

Existing systems: The Service provider completes and submits a condition, ownership, compatibility, cybersecurity and lifecycle audit of existing or inactive systems before proposing reuse, upgrade or recommissioning. Only work expressly included in the Site Technology Schedule is in the priced baseline. Additional remedial or replacement work is undertaken only following a Service Manager instruction, notified compensation event or issued Task Order, as applicable.

Testing and commissioning: Commissioning includes factory or bench tests where required, installation inspection, functional and integration tests, alarm and response simulation, failover and recovery tests, cybersecurity checks, data-retention verification, user training and submission of as-built records, configurations, backups, asset-register entries and manuals. The relevant system enters operational service only after the objective acceptance criteria in the test plan have been met and the Service Manager has confirmed the contractual record.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

4.3. Maintenance and Support

The Service provider maintains all security technology, control-room infrastructure, interfaces and supporting services identified in the Site Technology Schedule, Control Room Interface Schedule, Asset and Maintenance Schedule and issued Task Orders so that each system achieves the availability, functionality, fault-response and restoration requirements stated in the Service Level Agreement.

The maintained scope includes site devices, alarms, CCTV, access control, intrusion detection, recording platforms, dedicated Eskom monitoring-desk workstations and displays, communications, network links, interfaces, licences, system-health monitoring, backup power, resilience arrangements and all connections between installed site technology, the Service provider's control room and Eskom's newly established control room.

Maintenance included in the Prices comprises labour, call-out, travel, tools, test equipment, consumables, routine spares, software and firmware support, licences, vendor support, warranty administration, lifecycle replacement, temporary protection and planned migration support expressly allocated to the Service provider.

4.3.1. Maintenance plan and asset scope

Before the starting date, the Service provider submits a maintenance plan for acceptance by the Service Manager. The plan identifies every asset and service in the Site Technology Schedule, Control Room Interface Schedule, Asset and Maintenance Schedule and issued Task Orders; its criticality; preventive-maintenance frequency; inspection and test method; competent person; required spares; maintenance window; temporary protection; escalation route; and required record. Acceptance does not relieve the Service provider of responsibility for Providing the Service.

4.3.2. Availability and downtime measurement

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Availability is measured for each asset class over the calendar-month assessment period using the single Availability and Fault Matrix referenced in section 4.7. Downtime begins at the earlier of automatic system detection or receipt of a fault report at the Service provider's control room and ends only when the affected security function has been permanently restored, tested and returned to service. The matrix defines treatment of degraded or partially functioning systems, dependencies and permitted exclusions. Exclusions are limited to accepted planned-maintenance windows and events expressly allocated to Eskom or otherwise excluded by the contract, supported by time-stamped evidence. Failures of Service provider-provided communications, utilities, redundancy or subservice providers are not excluded. Third-party network or utility failures are excluded only where the relevant service is not a service provider obligation, and the Service provider has implemented the required resilience and escalation measures.

4.3.3. Preventive maintenance

The Service provider performs inspection, testing, cleaning, calibration, battery, storage, communications, failover, backup-power, software-health and cybersecurity checks at the frequencies stated in the Asset and Maintenance Schedule and manufacturer requirements. Planned interruptions require the Service Manager's prior acceptance, advance notification and activation of the stated temporary protection. Completed work, test results, identified faults and non-compliance are recorded in the maintenance-management system and reported in accordance with section 4.3.14.

4.3.4. Fault classification, timing and corrective maintenance

Every fault or failure is logged at the earlier of automatic detection or report to the Service provider's control room with a unique reference, affected asset, site, timestamp, source, impact and initial classification. The Availability and Fault Matrix defines critical, major and minor faults and the acknowledgement, remote-diagnosis, attendance, temporary-restoration and permanent-restoration periods for each class. All periods run from that initial timestamp. The Service provider diagnoses, contains, repairs or replaces, tests and returns the system to service, provides updates at the stated frequency and escalates any anticipated breach. A failure of a system is recorded as a fault or failure; non-compliance with the Service Information is notified and corrected as a Defect in accordance with the NEC3 TSC. These terms are not interchangeable.

4.3.5. Temporary protection and continuity

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The contingency plan identifies for each critical security control the approved temporary measure, activation trigger, maximum activation period, minimum capability and evidence of implementation. Where a fault reduces a required control, the Service provider activates the applicable temporary measure within the period stated in the Availability and Fault Matrix and maintains it until permanent restoration. Measures may include intensified monitoring, mobile surveillance, temporary detection, additional patrols or guarding. Temporary protection included in the priced contingency and standby baseline forms part of the Prices; additional measures arise only through an authorised Service Manager instruction and the applicable NEC3 TSC procedure.

4.3.6. Restoration, repair and replacement

Temporary restoration means an approved interim arrangement that reinstates the required security outcome pending permanent work. Permanent restoration means repair or replacement followed by successful functional, integration, recording, failover and cybersecurity testing. An obsolete, unsupported, repeatedly failing or irreparable asset is replaced within the period stated in the schedule where lifecycle replacement is included in the Technology-as-a-Service Prices. Temporary restoration does not stop the permanent-restoration clock unless the Availability and Fault Matrix expressly provide otherwise.

4.3.7. Cybersecurity maintenance

The Service provider continuously monitors relevant vulnerabilities and vendor advisories; maintains supported operating systems, firmware, applications, malware protection, certificates and secure configurations; classifies patches by criticality; tests changes in an appropriate environment; maintains backup and rollback arrangements; obtains approvals required by Eskom change control; and reports cybersecurity incidents and material vulnerabilities within the periods stated in the Service Information. Unsupported or end-of-support software or firmware is not used unless the Service Manager has accepted a time-bound risk treatment supported by compensating controls. Critical security patches included in the maintenance baseline are applied within the prescribed period and do not constitute a compensation event merely because the Service provider omitted them from its Prices.

4.3.8. Warranty and vendor support

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The Service provider remains responsible for fault containment, temporary protection and restoration within the Service Level Agreement even where an OEM, supplier or subservice provider must honour a warranty. Warranty administration does not extend the restoration period. The Service provider maintains the support contracts, escalation paths and vendor access necessary to meet the Service and enforces warranties without prejudicing Eskom's transferable rights.

4.3.9. Spares and ownership

The Service provider maintains the minimum critical-spares stock and replenishment periods stated in the Asset and Maintenance Schedule. Each spare is recorded as Service provider Equipment or as Plant and Materials identified for transfer in the Technology Asset Transfer Schedule. Use, replacement and replenishment are recorded against the asset register. At expiry or termination, only spares expressly identified for transfer pass to Eskom in accordance with section 2.17; all other Service provider Equipment is dealt with under the contract.

4.3.10. Patches, licence renewals, lifecycle replacement and upgrades

Routine patches, signature updates, licence and subscription renewals, minor supported-version updates, lifecycle replacements, obsolescence management and other maintenance obligations included in the Technology-as-a-Service baseline are included in the Prices and are not compensation events merely because the Service provider failed to price them. A material upgrade, new functionality or Service Manager instruction that changes the Service Information is administered under the applicable NEC3 TSC compensation-event procedure or, where Option X19 applies, through an issued Task Order.

4.3.11. Control-room integration and migration maintenance

The Service provider maintains the dedicated Eskom monitoring desk, control-room workstations, displays, recording platforms, communications, network configurations, interfaces, backup power, resilience and all links between site technology and the Service provider's control room. When systems are migrated to Eskom's newly established control room, the Service provider maintains both environments and all interconnecting services during parallel operation, resolves faults across the end-to-end service, and continues monitoring, recording, alarm handling, dispatch and incident response without interruption until the Service Manager confirms successful completion of the operational acceptance tests. Planned migration support identified in the Control Room Interface Schedule is included in the Prices.

4.3.12. Training and competency

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

For maintenance and support, the Service provider maintains a competency matrix for technicians, control-room operators, system administrators and Eskom system users and provides the OEM, cybersecurity, network, safety and system-specific training stated in the Training Schedule. Wider guarding, armed-response and drone competencies are governed by section 4.1 and the same Training Schedule. No person performs regulated or specialist work without current required competency. Attendance, assessment, certification and refresher records are submitted monthly.

4.3.13. Repeated failures, Defects and corrective action

A repeated or critical fault requires root-cause analysis and a corrective-action report within the period stated in the Availability and Fault Matrix. Where the failure also constitutes non-compliance with the Service Information, the Service Manager may notify a Defect under the NEC3 TSC. Corrective action includes containment, permanent remedy, responsible persons, target dates and verification evidence and does not replace the Service provider's obligation to meet the fault-restoration service level.

4.3.14. Records, reporting and early warning

The Service provider maintains time-stamped asset-health, availability, fault, work-order, parts, patch, licence, warranty, technician, cybersecurity and test records throughout the contract. Reporting follows the monitoring cycle in section 2.6: immediate notification of critical failures and security incidents; daily exception reporting; weekly trend and open-fault review; a monthly performance scorecard covering availability, planned and unplanned downtime, fault response and restoration, temporary measures, repeat failures, preventive-maintenance completion, spares and SLA compliance; and a quarterly lifecycle, capacity and obsolescence review. The Service provider gives an early warning as soon as it becomes aware of any matter that may increase the Prices, delay restoration, impair availability or affect continuity of the Service.

4.3.15. KPI and contractual consequence alignment

The Availability and Fault Matrix in the Service Level Agreement is the single source for technology availability, functionality, fault classification, temporary-restoration and permanent-restoration targets. Section 4.7 KPI tables shall measure performance using the same definitions, formulas, exclusions, timestamps and evidence and shall not create overlapping or conflicting targets. A KPI failure gives rise to a deduction or low service damages only where the contract expressly provides the applicable mechanism, including Option X17 where selected and completed.

4.4. Technology Roadmap

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The Service provider shall develop, maintain and implement a Technology Roadmap aligned with the Site Technology Schedule, approved implementation plan, site-risk tiers, Asset and Maintenance Schedule, Control Room Interface Schedule, Technology Asset Transfer Schedule and section 4.7 value-realisation measures. Roadmap preparation, quarterly review and annual update are included in the Prices; acceptance of the roadmap does not authorise deployment, change the Service Information or alter the Prices.

4.4.1. Submission and review: The Service provider shall submit the initial Technology Roadmap to the Service Manager within the period stated in the Service Information and before the first technology deployment. The Service provider shall report progress quarterly and submit an updated Roadmap annually and whenever a material change in threat, technology support status, legislation, Eskom architecture or operational requirements affects the approved approach.

4.4.2. Minimum content: The Roadmap shall identify planned deployments, lifecycle replacements, integration and migration activities, capacity requirements, obsolescence risks, licence and support dependencies, cybersecurity and privacy requirements, expected benefits, costs, milestones, responsible persons, decision points and measurable success criteria. It shall distinguish between obligations included in the Technology-as-a-Service Prices and proposed additional work.

4.4.3. Scalability and interoperability: Proposed solutions shall meet the measurable capacity, performance, availability, retention, resilience and interface requirements stated in the Service Information and shall support expansion without undisclosed proprietary restrictions. A future increase in sites, users, devices, storage, geographic coverage or functionality is not included unless expressly stated in the priced baseline or instructed under the applicable NEC3 TSC procedure.

4.4.4. Pilots and innovation: No pilot, proof of concept or new technology is deployed solely because it appears in an accepted Roadmap. Implementation requires a Service Manager instruction or issued Task Order supported by an approved business case, defined scope, funding basis, technical design, cybersecurity and privacy assessment, legal and regulatory review, test plan, success criteria, data-management controls, operational owner and exit or scale-up decision. The Service provider shall report pilot results against the approved criteria before wider deployment.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

4.4.5. Contract administration and value realisation: Lifecycle replacement and maintenance already included in the Prices do not become compensation events merely because they are recorded in the roadmap. A Service Manager instruction changing the Service Information is administered under the NEC3 TSC compensation-event procedure or, where Option X19 applies, through an issued Task Order. Benefits claimed for approved changes shall be measured using the agreed baseline, evidence and section 4.7 value-realisation indicators.

4.5. Community and Stakeholder Involvement

The Service provider shall conduct community, law-enforcement and stakeholder engagement only in accordance with a Stakeholder Engagement and Information-Sharing Plan accepted by the Service Manager. The plan shall identify authorised representatives, approved communication channels, geographic areas, objectives, planned activities, personal-information controls, source-protection measures, escalation routes, records and reporting requirements. The Service provider shall not represent itself as speaking on behalf of Eskom or disclose Eskom information without written authority.

4.5.1. Community liaison: The Service provider shall maintain constructive engagement with approved community structures surrounding protected sites, provide approved awareness messages on electricity-infrastructure protection and safety, and operate approved channels for receiving reports of suspicious activity. Community-sourced information shall be recorded, evaluated, protected and routed to the Service provider’s control room and authorised Eskom representative in accordance with the incident-management and information-security procedures.

4.5.2. Personal information and confidential sources: The Service provider shall collect only information necessary for the approved purpose, protect source identities, restrict access, maintain an audit trail and process personal information in accordance with POPIA, the Service Information and Eskom requirements. Information shall be treated as unverified until assessed and shall not be used for unlawful surveillance, profiling, discrimination or unauthorised investigation.

4.5.3. Local participation: Local employment, skills transfer and procurement obligations apply only where measurable targets, eligibility rules and reporting requirements are stated in the Contract Data, Service Information or applicable procurement schedules. Recruitment, training and procurement shall comply with legislation, Eskom policies and the Service provider’s security, competency and vetting obligations.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

4.5.4. SAPS and other security stakeholders: The Service provider shall maintain the authorised communication and escalation protocols stated in the plan with the South African Police Service and relevant statutory agencies. Transnet, PRASA and other corporate or state-owned-entity security functions are treated as security stakeholders and not as law-enforcement agencies unless legislation provides otherwise. Security Business Intelligence or incident information is shared only through authorised, secure and lawful channels.

4.5.5. Joint operations: Participation in roadblocks, inspections, raids or other statutory operations occurs only when lawfully requested by the competent authority, authorised by Eskom and included in the priced programme or instructed by the Service Manager. The Service provider acts within its legal powers and competency and does not exercise police or regulatory powers.

4.5.6. Scene and evidence preservation: Security personnel shall protect life, secure the scene, prevent contamination, preserve relevant recordings and records, maintain continuity and chain-of-custody documentation, and cooperate with SAPS or another competent investigator. Collection, seizure, forensic examination or investigation is undertaken only by authorised and competent persons. Incident reports shall be factual, time-stamped and supported by available records.

4.5.7. Reporting and priced scope: The Service provider shall maintain an engagement register and report planned activities, information received, referrals, outcomes, risks and lessons through the section 2.6 monitoring cycle. Activities identified in the accepted annual plan are included in the Prices. Additional campaigns, travel, joint operations or resources outside the priced programme require a Service Manager instruction and the applicable NEC3 TSC compensation-event or Task Order procedure.

4.6. Handover and Transition

Handover and transition shall be performed in accordance with section 2.17, the Technology Asset Transfer Schedule, Service Information, Control Room Interface Schedule and applicable NEC3 TSC provisions. This section defines the operational deliverables and does not create a general final-acceptance certificate, transfer Service provider Equipment not identified for transfer, or override the procedures and payment basis applicable to early termination.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

4.6.1. Planned expiry: The Service provider shall submit a detailed handover and transition plan by the date stated in the Service Information. The plan shall include milestones, accountable persons, asset and data verification, licence and warranty review, documentation delivery, testing, Defect correction, training, knowledge transfer, parallel operation, migration, acceptance evidence, secure deletion and demobilisation. Planned expiry handover and transition obligations stated in the Service Information are included in the Prices.

4.6.2. Eskom control-room migration: Where Eskom's newly established control room is ready before contract expiry, the Service provider shall perform the migration and parallel operation required by sections 4.1 to 4.3 and the approved migration plan. The Service provider shall maintain both environments and uninterrupted monitoring, recording, alarm handling, dispatch, incident response and maintenance until the objective end-to-end integration, failover, cybersecurity and operational tests have been completed and the Service Manager has confirmed the contractual record.

4.6.3. Assets and physical items: The Service provider shall verify the final asset register and hand over only the Equipment, Plant and Materials, spares, keys, tokens, certificates and other physical items identified for transfer in the Technology Asset Transfer Schedule. Service provider Equipment not identified for transfer remains subject to the contract's removal and termination provisions. Transferred assets shall meet the stated condition, testing, title and encumbrance requirements.

4.6.4. Documentation and records: The Service provider shall deliver current approved designs, as-built architectural, electrical and network drawings, configurations, asset and maintenance records, test and commissioning results, system backups, operator, maintenance and technical manuals, SOPs, emergency procedures, training records, warranties, licence information, support contacts and open-issue registers. Records shall be indexed, version-controlled and supplied in the open and secure formats stated in the Service Information.

4.6.5. Data transfer and retention: Eskom data shall be exported, verified and transferred in accordance with section 2.17.5, the approved retention schedule, lawful holds, POPIA and information-security requirements. The Service provider shall not transfer an undefined full historical archive where the retention schedule does not require it. Following Eskom's confirmation of successful transfer and expiry of any lawful retention duty, the Service provider shall securely delete residual Eskom data from Service provider-controlled environments and provide the required deletion certificate.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

4.6.6. Licences, intellectual property and support: Transfer or continuation of licences, subscriptions, warranties and support agreements shall follow section 2.17.6 and the Technology Asset Transfer Schedule. The Service provider shall disclose non-transferable or time-limited rights and implement the approved replacement, novation or successor-support arrangement. No broader intellectual-property right is transferred unless expressly stated in the contract.

4.6.7. Testing, Defects and acceptance evidence: Handover testing shall cover functionality, integration, alarm and video receipt, recording and retrieval, user access, backups and restoration, failover, cybersecurity, system health, reporting and continuity. Notified Defects are corrected in accordance with the NEC3 TSC and stated correction periods. The handover record identifies tests passed, documents delivered, training completed, assets transferred and outstanding items; it evidences compliance where the contract so provides but does not waive surviving obligations.

4.6.8. Training and knowledge transfer: The Service provider shall deliver the curricula, practical exercises, administrator and operator training, maintenance familiarisation, competency assessments and knowledge-transfer sessions stated in the Training Schedule to nominated Eskom personnel or an authorised successor service provider. Completion is evidenced by attendance, assessment results, training materials and sign-off by the authorised recipient.

4.6.9. Early termination: On early termination, the Service provider shall comply with NEC3 TSC clauses 90 to 93, the procedure and payment basis applicable to the certified termination reason, section 2.17.9 and authorised Service Manager instructions. The timing, asset treatment and transition work shall not be assumed to be the same as planned expiry. Additional transition Service is instructed and assessed only where the contract permits.

4.6.10. Decommissioning and additional work: Decommissioning, removal, data sanitisation or environmental disposal is performed only were stated in the priced exit scope or instructed by the Service Manager. The plan shall protect the Affected Property, preserve required records and data, maintain security continuity and comply with legal and environmental requirements. Work outside the priced handover and transition baseline is administered through the applicable NEC3 TSC instruction, compensation-event or Option X19 Task Order procedure.

4.7. Key Performance Indicators

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The Service provider's performance shall be measured against the indicators in this section, the Service Level Agreement and the schedules forming part of the Service Information. The KPI framework supports monitoring, corrective action and continuous improvement and does not create a payment deduction, low service damages, default or termination right unless the contract expressly provides the applicable mechanism.

4.7.1. KPI governance and measurement rules

Before the starting date, the Service provider shall submit the detailed KPI Measurement Schedule for acceptance by the Service Manager. For each KPI, the schedule shall state the definition, site and Tier applicability, baseline, target, numerator, denominator, assessment period, data owner, evidence source, permitted exclusions, calculation method, reporting frequency and corrective-action trigger. All site-risk references shall use Tiers 1 to 4 and the approved network-infrastructure classification.

Performance shall be supported by auditable, time-stamped source data. The Service Manager may verify reported results against control-room records, GPS data, electronic access and guard-tour records, maintenance systems, asset registers, incident reports, training records and financial evidence. Planned downtime, Employer-caused delay, unavailable site access, late Eskom information, instructed changes, compensation events, statutory approvals and other permitted exclusions are excluded only where the contract allows and the Service provider provides supporting evidence. The Service Manager may correct a previous result where later verified information shows that the original result was inaccurate.

Reporting follows section 2.6: critical events and failures are reported immediately; exceptions are reported daily; operational trends are reviewed weekly; formal KPI scorecards are assessed monthly; and risk, lifecycle, stakeholder and value-realisation trends are reviewed quarterly. A disagreement regarding a KPI result is first addressed through the performance-review process and, if unresolved, through the contract's dispute-resolution procedure.

4.7.2. Security outcome indicators

KPI	Requirement and measurement	Frequency
Security incidents and loss trend	Measure confirmed theft, vandalism, sabotage, trespass and security-related outage trends against the Service Manager-approved baseline for each Tier and network-infrastructure category. Report incident count, verified loss, outage impact,	Immediate, monthly and quarterly

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

KPI	Requirement and measurement	Frequency
	detection source and control failure. An incident is not attributed to Service provider failure unless evidence shows non-compliance with a contractual control materially contributed to the event or its impact.	
Detection and verification	Measure acknowledgement and remote verification from the earliest reliable timestamp of alarm activation, first observable system event or first report received by the Service provider's control room. Targets and Tier-specific times are stated in the SLA. Each verified incident is classified, recorded, escalated and linked to the required response action.	Real time and monthly
Incident reporting and corrective action	Measure completeness and timeliness of preliminary and final reports, scene preservation, notification, evidence continuity, root-cause analysis and closure of approved corrective actions within the periods stated in the SLA.	Per incident and monthly

4.7.3. Guarding and control-room service indicators

KPI	Requirement and measurement	Frequency
Guard-post coverage	Measure authorised and competent guard-hours actually provided divided by scheduled post-hours in the accepted deployment plan. Uncovered time, late relief, unqualified replacement and unauthorised redeployment are non-compliant hours. Mandatory posts shall be filled without interruption; the contingency plan shall provide immediate qualified relief.	Daily, weekly and monthly
Patrol and access-control compliance	Measure completed patrol control points, routes and time windows and compliant access transactions against the Site Service Schedule. Missed patrols, unverified access exceptions and incomplete records are reported and corrected.	Daily and monthly

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

KPI	Requirement and measurement	Frequency
Control-room service	Measure 24-hour staffing of the dedicated Eskom desk, alarm acknowledgement, verification, dispatch, escalation, incident-record completeness, system-health monitoring and authorised Eskom access against the Control Room Interface Schedule.	Real time and monthly
Armed-response performance	Measure from the time-stamped dispatch instruction to GPS-confirmed arrival at the incident location. The SLA states the target and compliance percentage for urban, rural and remote categories and each applicable Tier. The same response KPI shall not be duplicated elsewhere.	Per incident and monthly

4.7.4. Availability and Fault Matrix

The SLA Availability and Fault Matrix are the single source for end-to-end service availability, device availability, degraded operation, fault classification and response or restoration periods. It applies to site technology, communications, the dedicated Eskom monitoring desk, the Service provider's control room, interfaces and migration links.

Measure	Contract requirement
Availability	Measured monthly for each stated asset or service class as available time divided by required service time, using the downtime start, end, degraded-operation rules and permitted exclusions in sections 4.3.2 and the SLA.
Critical, major and minor faults	For each class, the Matrix states acknowledgement, remote diagnosis, attendance, temporary-restoration, permanent-restoration and update periods. Timing starts at the earlier of automatic detection or receipt of a fault report at the Service provider's control room.
Temporary protection	Measure activation of the approved temporary control within its stated period and maintenance of that control until permanent restoration.
Repeat failures	Measure timely root-cause analysis, approved corrective action and verified closure. A fault is treated as a Defect only where it also constitutes non-compliance with the Service Information.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

4.7.5. Compliance and competency indicators

The Service provider shall maintain continuous validity of all licences, registrations, permits and competencies required for deployed personnel and services, including PSIRA, firearm, SACAA, OEM, first-aid and role-specific requirements where applicable. Mandatory Eskom induction and site authorisation shall be completed before deployment. Measure monthly validity scheduled internal audits, timely submission of evidence, closure of non-conformances and cooperation with Eskom or authorised assurance reviews. An external audit is a Service provider KPI only where it is expressly included and priced in the Service Information.

4.7.6. Implementation and migration indicators

Measure completion of Service provider-controlled milestones in the accepted implementation plan, issued Task Orders, testing and commissioning plans, Control Room Interface Schedule and migration plan. A milestone is included in the compliance calculation only where required site access, Eskom information, approvals and statutory permissions were available and it was not affected by an instructed change, compensation event or other Employer risk. Migration indicators include end-to-end integration, data and alarm continuity, failover, cybersecurity testing, training, parallel operation and uninterrupted monitoring until the Service Manager confirms the contractual record.

4.7.7. Stakeholder and community indicators

Stakeholder satisfaction shall be measured using a methodology accepted by the Service Manager before the baseline survey, including the respondent group, questions, scoring method, minimum response rate, treatment of non-responses and exclusion of matters outside the Service provider’s control. Community and stakeholder performance shall also measure completion of the accepted engagement plan, authorised referrals, protection of personal information and confidential sources, lawful participation in joint activities, and timely reporting through section 2.6.

4.7.8. Value-realisation indicators

Value realisation shall be assessed against a Service Manager-approved baseline and shall consider total cost of ownership, implementation and lifecycle cost, avoided or reduced verified losses, reduced outage impact, productivity, response improvement, asset life, approved risk reduction and benefits attributable to the Service provider. No automatic guard-force or cost-reduction percentage applies. A change to the approved minimum guard deployment occurs only after commissioned and stable technology, updated risk assessment, proven response capability and an authorised contract change.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Innovation performance is measured by the proportion of approved roadmap initiatives and pilots that meet their pre-approved technical, operational, cybersecurity, privacy, financial and user-outcome criteria. The Service provider is not required to deploy a new technology merely to satisfy an annual count, and no unapproved technology is included in the KPI result.

4.7.9. Corrective action and consequence management

A missed KPI is recorded, verified and managed through the section 2.6 non-conformance and corrective-action process. The Service provider shall provide containment, root-cause analysis, responsible persons, completion dates and evidence of closure within the specified periods. Repeated or material failure is escalated in accordance with sections 2.12 and 2.13 and the NEC3 TSC.

A KPI result does not of itself constitute a Defect, substantial failure, payment deduction or termination reason. Low service damages apply only where Secondary Option X17 is selected, and the relevant service level and amount are completed in the contract. Any other service credit, deduction, Price List adjustment or payment consequence applies only where expressly stated in the NEC3 TSC, Contract Data or applicable Z clause and is reflected in the Service Manager's assessment and payment certificate.

4.8. Site Evaluations and Operational-Readiness Verification

Pre-award due diligence: Pre-award inspection or evaluation of a tenderer's capability forms part of the procurement evaluation process and shall be conducted in accordance with the published tender criteria. It may verify information submitted in the tender, including relevant experience, proposed control-room capability, statutory registrations, firearm compliance, vehicle availability, OEM certifications and technology capability. A pre-award evaluation does not constitute acceptance of the future Service or relieve the successful tenderer of any contractual obligation.

Post-award operational readiness: After award and before the starting date, and before Eskom systems are connected to the Service provider's control room, the Service Manager shall arrange an operational-readiness verification. The Service provider shall provide access to the facilities, systems, records, personnel and demonstrations reasonably required to verify readiness against the Service Information, Control Room Interface Schedule, Site Service Schedule, Site Technology Schedule, Training Schedule and accepted mobilisation plan.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Minimum verification scope: The assessment shall verify the dedicated Eskom monitoring desk; 24-hour staffing and supervision; control-room accreditation where required; alarm, CCTV, access-control and incident-management capability; recording and retention; secure connectivity; system-health monitoring; cybersecurity controls; backup power, redundancy, disaster recovery and business continuity; dispatch and escalation arrangements; lawful firearm licences, permits, competencies, storage and registers; authorised, roadworthy, insured and fit-for-purpose owned or leased vehicles; applicable PSIRA, SACAA, OEM and other statutory or technical certifications; critical spares; and the availability of competent personnel and subservice providers.

Testing and evidence: The Service provider shall demonstrate end-to-end alarm receipt, video verification, incident logging, communication, dispatch, failover, recovery and Eskom-authorised access using the accepted readiness test plan. Results, evidence, non-conformances, responsible persons and due dates shall be recorded in an operational-readiness report. Review, witnessing or acceptance by the Service Manager does not relieve the Service provider of responsibility for Providing the Service.

Correction and re-verification: The Service provider shall correct identified non-compliance within the period stated by the Service Manager and submit evidence of closure. Where a failed requirement materially affects safe or reliable commencement, the affected Service or connection shall not commence until the stated readiness criterion is met or an authorised temporary arrangement is accepted. Any effect on the Prices, Key Dates or starting date is administered only in accordance with the NEC3 TSC.

Ongoing verification: Eskom may conduct announced or unannounced compliance and readiness inspections during the contract in accordance with the Service Information. The Service provider shall maintain continuous compliance and provide reasonable access to relevant sites, records, systems and personnel.

4.9. Price Adjustment and Annual Rates

The Prices and any adjustment to them shall be governed only by the selected NEC3 TSC Main Option, the Contract Data, the Price List and any applicable Z clause. No rate increases automatically by reason of a Government Gazette notice, collective agreement, inflation, exchange-rate movement or other cost change unless the contract expressly provides an adjustment mechanism or the event is otherwise dealt with under the NEC3 TSC.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Statutory labour adjustments: Where the Contract Data or an applicable Z clause provides for adjustment arising from a statutory security-sector wage determination, the adjustment shall apply only to the labour cost component expressly identified in the Price List and from the effective date stated in the relevant instrument or contractual mechanism. The Service provider shall submit the published determination, affected categories, base rates, weighting, calculation and evidence that the increase has been implemented for the relevant personnel.

Formula and evidence: The applicable base date, indices, weighting of labour, equipment, fuel, technology, licences and other cost components, frequency of adjustment, treatment of decreases and effective date shall be those stated in the Contract Data or applicable Z clause. Any request shall be fully substantiated and verified before implementation.

No duplication: No cost may be recovered more than once through indexation, statutory adjustment, Price List revision, compensation event, Task Order rate or another contractual mechanism. Lifecycle replacement, licence renewal, maintenance, standby and other obligations already included in the Prices remain included notwithstanding a general cost increase.

Contract administration: A price adjustment takes effect only through the mechanism stated in the contract and does not require an informal annual renegotiation. Any instruction changing the Service Information is administered separately under the NEC3 TSC compensation-event procedure or, where Option X19 applies, through an issued Task Order.

4.10. Monthly Payment and Invoice Administration

This section supplements, and does not replace or amend, section 2.16 and NEC3 TSC clauses 50 to 52. The assessment date, certification period, final date for payment and interest entitlement are those stated in the Contract Data and applicable Z clauses. An Eskom administrative process, submission channel or supporting-document requirement does not postpone or alter those contractual dates unless the contract expressly provides otherwise.

Application for payment: The Service provider shall submit its application for payment on or before each assessment date stated in the Contract Data. Where Eskom uses a 15th-to-14th operational reporting period, that period is used only for supporting measurement and reconciliation unless it is expressly stated as the contractual assessment cycle in the Contract Data. The application shall contain the breakdown and supporting evidence required by sections 2.16.1 and 2.16.2.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Assessment and certification: The Service Manager shall assess and certify the amount due at each assessment date in accordance with section 2.16, even where the Service provider's application or records are incomplete. Missing or unverifiable information may affect the amount assessed, and the Service Manager may correct a previous assessment in a later certificate as permitted by the NEC3 TSC.

Tax invoice: Following receipt of the payment certificate, the Service provider shall submit a valid tax invoice only for the certified amount through Eskom's approved electronic or other notified invoicing channel. The invoice shall include the contract number, purchase order number, assessment period, payment-certificate reference, applicable tax information and any other administrative information stated in the Contract Data or Eskom's notified invoice requirements. An electronic tax invoice is acceptable where it complies with applicable law and Eskom requirements; an original paper invoice is required only where the Contract Data expressly states this.

Incomplete or incorrect invoice: Eskom shall notify the Service provider promptly of an incomplete, inaccurate, duplicated or incorrectly submitted invoice, and the Service provider shall correct it without delay. An invoice defect does not remove the Service Manager's obligation to assess and certify within the contractual timetable and does not extinguish interest payable under the NEC3 TSC where the contractual requirements for interest are met.

Payment, deductions and set-off: Eskom shall pay the amount due within the period stated in the Contract Data. A service credit, low service damages, deduction, recovery of overpayment or set-off may be applied only where expressly permitted by the NEC3 TSC, completed Contract Data, applicable Z clause or law and shall be shown transparently in the Service Manager's assessment and payment certificate.

Banking details and fraud controls: The Service provider shall maintain correct banking and tax information through Eskom's prescribed verification process. A change to banking details shall not be actioned solely on the basis of an invoice, email or informal communication and shall not alter the contractual assessment or payment timetable.

a) Eskom's property in possession of the service provider

Eskom's property supplied to the Service Provider for the execution of their duties remains the property of Eskom and will at any time be available for inspection by an Eskom Representative. Any such property in the possession of the SP on completion of the agreement will be returned to Eskom in the same working condition as handed to the Service Provider.

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

The Service Provider will always be responsible for any loss of or damage to Eskom property in his possession, and if required Eskom will deduct the loss of such equipment if the service provider fails to compensate Eskom once a final investigation report from Eskom has been submitted.

b) Task order instruction

A Task Order will be issued by the Eskom Security Contract Manager/Supervisor or persons appointed in consultation with the Eskom Security Contract Manager.

Any specific requirements related to the quality standards for the services required will be included in the Task Order. Any constraints relevant to the services shall be timeously communicated with the Service Manager and mitigations thereof approved by the Service Manager .

Service provider must prepare three quotes after they received the task instruction (with full details of the scope of work) as per agreed price structure.

Once quote is approved by the Eskom Contract Manager/Supervisor, the Task Order instruction will be issued to the Service provider for commencement and will include the following: A detailed scope/description of the guarding services required – to be performed by the Service provider (deliverables), manpower required, grades, operational equipment, start and end date; and PO Number.

The Service provider is only allowed to proceed with the task instruction once it complies with all the requirements as described above i.e. PO number, start and end dates.

Both parties to reply / respond within 12 hours for acceptance of quote and task instructions.

The requested services can only commence after official approval by the Eskom Representative (Eskom Security Contracts /Site Owner/Requestor) has been granted; this approval will be in the form of a signed-off task instruction by the Eskom Contract Manager/Supervisor.

The Service provider is expected to return a copy of signed task instruction for record that both parties have accepted this request.

Service provider to inform the Eskom Security Contract Manager/Supervisor by immediately submitting an early warning notification of any material deviation from the originally approved task instruction should there be changes to the initial approved task order value and/or time as indicated in the originally approved task order.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30

Acceptance and approval of such and Early Warning must first be obtained from Eskom Security Manager/Contracts Manager for any changes on the Task Order before the work can continue.

Task Order template will be provided to the Service provider after the signing and acceptance of this contact.

5. Acceptance

This document has been seen and accepted by:

Note: Initials not acceptable

Full Name and Surname	**Designation**
Brenda Cebekhulu	Senior Manager Business Enablement
Phumla Siswana	Middle Manager SHEQS
Remone Govender	Senior Manager SSP

6. Revisions

Date	**Rev.**	**Compiler**	**Remarks**
July 2025	1	Musa Mchunu	First issue
August 2026	2	Musa Mchunu	Second Issue

7. Development Team

The following people were involved in the development of this document:

- Adolph Lekganyane – Middle Manager Security
- Musa Mchunu - Security Manager KZNOU
- Nthabeleng Motloung – Senior Advisor SSP

8. Acknowledgements(if applicable)

N/A

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of Eskom Holdings SOC Ltd, © copyright Eskom Holdings SOC Ltd, Reg No 2002/015527/30