Eskom	SCOPE OF WORK	DUVHA POWER STATION

Title:	**PROVISION OF SECURITY SERVICES, MAINTENANCE, REPAIR AND INSTALLATION OF SECURITY TECHNOLOGY AND SYSTEMS AT DUVHA POWER STATION FOR A PERIOD OF 36 MONTHS**	Document Identifier:	**559-478084838**
		Alternative Reference Number:	**N/A**
		Area of Applicability:	**Duvha Power Station**
		Functional Area:	**Security**
		Revision:	**1**
		Total Pages:	**43**
		Next Review Date:	**July 2029**
		Disclosure Classification:	**CONTROLLED DISCLOSURE**

Compiled by	Functional Responsibility	Authorised by
……..	……..	……..
Magnificent Ndlovu	**Timothy Hlatshwayo**	**Robert Hlahu**
Officer Security Systems	**Officer Security operations**	**Manager Security**
Date: 16.03.2026	Date: 16.03.2026	Date: 16.03.2026

CONTENTS PAGE

1. INTRODUCTION

Duvha Power Station is designated as a National Key Point in terms of the NKP Act of 1980 / Critical Infrastructure Act 8 of 2019. It is therefore subjected to be safe guarded by trained security officers who have been trained on the following aspects which are NKP Act, PSIRA Act, Firearm Act, SASSETA Act of 1998,) and Critical Infrastructure Act. This scope of work is for the purpose of outlining the Physical Security resources that is needed to protect and enhance the current security measures on site.

The station utilises contract physical security services to supplement the existing security inhouse resources for the protection of both NKP and Non NKP areas. It is therefore essential for Duvha Power Station security to provide the scope of work that will prescribe the requirements of procuring the security services. In addition, the station must ensure that the contracted security service providers meet the contractual agreements, compliance requirements, training, and performance standards required by incorporating the principles of Outcome Based Contracts (OBCs) for physical security services into practice. In order to guarantee that security service providers produce quantifiable results in line with Eskom's security goals. The emphasis is on increasing the efficacy of security, incorporating technologically advanced solutions, and stimulating innovation while guaranteeing cost effectiveness and value for money.

It is therefore the primary responsibility of the service provider to ensure that each security officer assigned to security duties shall comply and provide quality and professional service as stipulated in Eskom Procedures and Regulations.

2. SUPPORTING CLAUSES

2.1 Scope

The scope of work (SOW) specifies the required services to be rendered by the Supplier for a period specified and conditions for the acceptance of such a contract.

2.1.1 Purpose

The purpose of the scope of work is to procure a security services that is aligned to the outcome-based contract model to protect Eskom Duvha Power Station assets and personnel through measurable performance outcomes. The Scope of Work (SOW) for an Outcomes-Based contract goes beyond listing services. It clearly defines the results to be achieved, the assets to be protected, the underlying principles, and the specific activities required to deliver those outcomes.

2.1.2 Applicability

This document shall apply throughout Duvha Power Station Security Department.

2.1.3 Effective date

This document shall be effective from date of authorisation.

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] ISO:14001, Certified Environmental Management

[3] ISO:27001, Certified Information Security Management

[4] SANS 10142-1 (SABS 0142-1), The wiring of premises – Part 1: Low-voltage installations.

[5] SANS 10222-5-1-1 (SABS 0222-5-1-1), Electrical security installations – Part 5-1-1: CCTV installations – CCTV surveillance systems for use in security applications – Operational requirements.

[6] SANS 10222-5-1-2 (SABS 0222-5-1-2), Electrical security installations – Part 5-1-2: CCTV installations – CCTV surveillance systems for use in security applications – System design requirements.

[7] SANS 10222-5-1-3 (SABS 0222-5-1-3), Electrical security installations – Part 5-1-3: CCTV installations – CCTV surveillance systems for use in security applications – Installation, planning and implementation requirements.

[8] 240-86738968, Standard for Security Alarm Systems for Protection of Eskom Installations and its Subsidiaries

[9] 240-55410927, Cyber security standard for Operational Technology

2.2.2 Informative

[1] Act of 1980: National Key Point Act

[2] Act of 1998: Safety and Security Sector Education and Training Authority Act

[3] Act 56 of 2001: Private Security Industry Regulations Act.

[4] Act 60 of 2000: Firearm Control Act

[5] Act 13 of 2009: Civil Aviation Act

[6] Section 71 of Act 13 of 2009: Civil Aviation Authority Act

[7] Act 8 of 2019: Critical Infrastructure Act

2.3 Definitions

Definition	Explanation
NKP	National Key Point means any place or area which has under Section 2 of the Key Point Act 102 of 1980 been declared a National Key Point.
NKP Owner	In relation to a place or area declared a national key point under section 2, includes but not limited to any person under whose control or management such place or area is
Chief Security Officer	means a person appointed as chief security officer in terms of regulation 9(1)(a) or 9(3), or a person designated in such capacity in terms of regulation 9(2);

Definition	Explanation
OBC Contract	An Outcome Based Contract is a type of agreement where the payment and evaluation are tied to the achievement of specific, measurable results rather than just the completion of the task or delivery of service
Contractor / Supplier	The Contractor / Supplier who is awarded the contract and will deliver the services outlined in the document.
Employer	Refers to Eskom, Camden Power Station
Services Manager	The employee nominated by Eskom, Camden Power Station who manage the above listed TSC3 contract for the stated goods / Services strictly in accordance with the conditions of contract stated in the Contract Data
Consequence	The outcome of an event that affects objectives.
Divisional security manager	The Security Middle Manager (Task Grade M17 and above) responsible at divisional level for co-ordinating and advising on the security function in that division or business.
2-Man rule	A security officer may not be posted at any post alone nor may a security officer go out on patrol (vehicle and foot) alone there must always be a minimum of two security officers
Asset	Anything that has tangible or intangible value to the organisation.
Competence	Ability to apply knowledge and skills to achieve intended results.
Security Vetting	Also referred to as security screening is the prescribed and systematic process of investigation (vetting investigation) followed in determining a person's security competence. Security vetting can be done pre- or post-employment.
Contract	means an agreement between two or more parties, one being Eskom, with the intention of creating rights and obligations with legal consequences or effect, as amended from time to time.
Incident	Event with consequences which have the capacity to cause loss of life, harm to assets, physical security breach, loss of assets, or negatively affect human rights and/or the fundamental freedoms of internal or external stakeholders, or any event that poses a threat to the security of an organization’s assets.
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.
Non-compliance	Means the non-fulfilment of applicable legislative, regulatory, or organisational requirement such as Eskom’s approved security policies, standards, directives, procedures, work instructions, and standard operating procedures.
Non-performance	Means a non-fulfilment of applicable performance standards and Eskom’s approved security policy standards, directives, procedures, work instructions, and standard operating procedures.

2.4 Abbreviations

Abbreviation	Description
BOQ	Bill of Quantities
CCTV	A system consisting of camera equipment, storage, monitoring and associated equipment for transmission and controlling purposes.
FCA	Firearm Control Act
NKP Act	National Key Point Act
JPC	Joint Planning Committee
GSR	Government Security Regulator
PSIRA	Private Security Industry Regulatory body.
SASSETA	Safety and Security Sector Education and training Authority
SOW	Scope of Work
SANDF	South African National Defence Force
APA	Animal Protection Act
SOP	Standard Operating Procedure
SHE	Safety Health and Environment
OHS	Occupational Health and Safety
TRA	Threat Risk Assessment

2.5 Roles and Responsibilities

[1] Security Department shall compile the scope of work for the provision of physical security services

[2] Security department shall use this document for the procurement of contract of physical security guarding.

2.6 Process for Monitoring

This document shall be subjected to internal reviews. Security department will ensure compliance and implementation to this document.

2.7 Related/Supporting Documents

N/A.

3. SCOPE OF WORK

3.1 Services Required Covered in the Scope of Work

The scope of work is for the provision of security services, maintenance, repair and installation of security technology and systems at Duvha Power Station for a period of 36 months. This shall include but not limited to the following:

[1] The Provision of Armed Guards (Static, mobile and Access Control) at various location that are part of the NKP on a 24-hour basis

[2] The Provision of Armed Security Officers for the patrolling, escort and response to any security threats on a 24-hour basis- Vehicle patrols

[3] Provide Guard monitoring/clocking system at various locations that will be monitored on site

[4] Provision and Maintenance security alarm systems & licences, access control systems, CCTV maintenance, two-way radio licence, electronic key systems & licence fees for the duration of the services

3.1.1. Access control duties

Access control activities consist of the control and management of the movement of assets, goods/ equipment, employees, visitors and contractors entering Duvha Power Station by:

a) Checking employee access, visitors, asset and vehicle permit for validity against date of issue or expiry date and where required against identity document.
b) Eskom Employees and contractors to be identified positively by means of valid Eskom Duvha issued permit.
c) Preventing access if permits are not valid, withdraw permits and referring permit holders to the permit office
d) Checking material, equipment removal permits and verifying content and signatures
e) Confiscating items not described on the removal permit and hand in for safekeeping.
f) Refusing exit with goods if removal permit is not signed by the authorised manager and reporting deviations to the supervisor for investigation and corrective action.
g) Completing relevant records and registers.
h) Conducting 100% searches on employees, visitors, vehicles, equipment by means of physical inspections, x-ray equipment, belly scope (search mirror) metal detectors, alcohol testers in accordance with standard operating procedures
i) Reporting incident and equipment failure to the supervisor.
j) Visitor to be identified positively by means of valid SA ID, passport, drivers licence.
k) Visitor confirmation process must be adhered to before access is granted.
l) Visitors must be escorted or accompanied by a host.
m) Locking and securing gates after hours.
n) Screening of persons and articles/parcels using electronic equipment ensuring prohibited items are not brought on site
o) 100% Alcohol testing of all personnel for possibility of being under the influence, by use of

breathalysers. Also carrying out random checks on the site when required.

p) Conducting thorough searching to all persons coming in and/or leaving site either manually or electronic aids such as x-ray, belly scope (search mirror)

q) All security guards must familiarise themselves with the site-specific procedures on access control including identifying of persons entering and searching of vehicles

r) Ensure that the gates (where applicable) are kept closed and always locked to prevent unauthorized entry.

s) Using metal detectors and mirrors to prevent personnel from removing items from the site or bring them onto site without authorisation.

t) Ensure that **ONLY** authorised Eskom employees and contractors shall enter the assigned areas.

u) Ensure declaration, recording and movement control of equipment and material, and where material cannot be accounted for, unauthorised and not declared and confiscated for investigation purposes. Such must be reported immediately to Eskom shift Supervisor.

v) Ensure 100% of electronic access control points is functional & automated at all times

w) Zero manual overrides without prior Eskom Security Manager/Officer Ops and Officer Investigation approval.

NB: Should there be any unauthorized property found in the possession of persons entering and exiting the mentioned areas, Eskom Security (Security Manager, Officer Investigation or Supervisor on duty) shall be contacted for further investigation.

3.1.2. Static guarding and foot and vehicle patrolling duties

The provision of static armed trained guards to perform guarding duties at a National Key Point and Non-National Key Point areas.

a) The contractor shall safeguard critical Eskom assets within areas mentioned on the scope and report any suspicious activities or criminal activity within their vicinity to Eskom Security Supervisor on duty and or Officer Security Operations.

b) The specific plant areas where the resources shall be deployed and shall focus on are outlined as stated below, this might change during the deployment period as certain risks become known or evolve.

c) To guard the buildings and patrol the outside of the buildings.

d) Keep records of employees/visitors and contractors accessing the buildings/ areas.

e) Report any suspicious activities at Duvha Power Station security control room.

f) Always maintaining communication with control centre.

g) Responding to dispatch instructions from control centre according to situation and standard operating procedures on site.

h) Checking security systems (doors, gates, fences, alarms, equipment, lights etc) for visible

defects and reporting immediately to supervisor.

i) Monitoring and reporting the movement of suspicious vehicles, people.

j) Observing surroundings with special attention to potential attack routes.

k) Monitoring and reporting suspicious activities and/or occurrences to control centre.

l) Ensuring fully compliant to all Eskom policies, procedures and relevant legislations.

3.1.3. Supervision – NKP and Non NKP

a) The Supervisor must be knowledgeable about the conditions and the scope of work contained in this contract and be capable of rendering the service.

b) All deployed guards must be supervised by a PSIRA Grade B supervisor. The supervisors must ensure that guards deployed at remote sites or areas with transport challenges are assisted to reach the sites.

c) Standard Operating procedures / work instructions to be drafted for manned / deployed areas & communicated to on duty personnel for adherence.

d) The posting of guards is required to be done by the Supervisor at all sites (the practice of “self-posting” is not permitted). All equipment must be tested during each shift change.

e) Inspection of the Occurrence Book daily (postings to be acknowledged and specified in the OB for each posting site and, to be logged in detail), and escalating OB risks to the Eskom Officer Security Ops / Security Manager.

f) Submissions of shift posting sheets and patrol reports to Eskom Security Supervisor

g) To submit vehicle log /check sheet as per the site requirements.

h) Update guards with new communication/other risks on daily requirement/posting.

i) The Employer may, having stated reasons, instruct the contractor to remove a key person.

j) Monitor all contract security guards and report all their needs to the Site Supervisor.

k) Provide vehicle tracking reports on a weekly basis to correlate patrols conducted.

l) The contractor may not replace any of the key persons, without prior written notice to the Project Manager/Security Manager.

m) All equipment must be tested during every shift change, and all defective or unserviceable equipment must be replaced immediately.

n) The posting of security personnel is required to be done by the Supervisor at all sites (the practice of "self-posting" is not permitted).

o) Report all incidents immediately as per applicable incident reporting procedures and submit a report to the Security Manager.

p) The contractor may not replace any of the key persons, without prior written notice to the Project Manager/Security Manager.

q) Ensuring guards are trained according to site standard operating procedures and

r) conducting on job training.

3.2 Contract Manager/ Site Manager

[1] Grade 12/NCV4/NSC3/N3

[2] Minimum two years previous work experience in security management

[3] Relevant Management qualification

[4] Psira Grade A.

[5] National Key Point (NKP) training/registration

[6] SAPS Firearm competency for Business Purposes: Handgun, Rifle and Shotgun

[7] Computer literate

[8] Security Clearance Certificate- not older than 30 days

3.3 Security Supervisor

[1] Security Clearance Certificate- not older than 30 days

[2] Grade 12/NCV4/NSC3/N3

[3] Psira Grade B certificate and ID card

[4] National Key Point (NKP) training/registration

[5] Be able to communicate, read and write in English.

[6] Must be computer literate

[7] Minimum two years' experience as security supervisor

[8] SAPS Firearm competency for Business Purposes: Handgun, Rifle and Shotgun

[9] Must have undergone Regulation 21 training and continue to do so for at least once per year for the duration of the service.

3.4 Security Officers- NKP and Non NKP- Static and vehicle patrol

[1] Security Clearance Certificate- not older than 30 days

[2] Grade 12/NCV4/NSC3/N3

[3] Psira Grade C certificate and ID card

[4] Driver's licence- for vehicle patrollers

[5] National Key Point (NKP) training/registration

[6] Be able to communicate, read and write in English.

[7] Minimum one year experience in security guarding, patrolling and access control.

[8] SAPS Firearm competency for Business Purposes: Handgun, Rifle and Shotgun

[9] Must have undergone Regulation 21 training and continue to do so for at least once per year for the duration of the service.

3.5 Safety Officer

[1] Security Clearance Certificate- not older than 30 days

[2] Grade 12/NCV4/NSC3/N3/

[3] SAMTRAC

[4] Be able to communicate in English.

[5] Minimum two years' experience as safety officer

[6] Psira Grade C

3.6 Technical Supervisor

[1] Security Clearance Certificate- not older than 30 days

[2] Grade 12/NCV4/NSC3/N3

[3] Security installer certificate/Relevant qualification

[4] Avigilon certification – or to be completed with three months after appointment.

[5] Psira Grade B certificate and ID card

[6] Working at Height certificate

[7] Be able to communicate, read and write in English.

[8] Must be computer literate

[9] Minimum three years' experience as a technician supervisor/project supervisor

3.7 Technician

[1] Security Clearance Certificate- not older than 30 days

[2] Grade 12/NCV4/NSC3/N3

[3] Security installer certificate/Relevant qualification

[4] Avigilon certification a – or to be completed with three months after appointment.

[5] Psira Grade C certificate and ID card

[6] Be able to communicate, read and write in English.

[7] Must be computer literate

[8] Minimum two years' experience as a technician

[9] Working at heights certificate

Note: *Contractor employees should not have been convicted of any criminal offence and should disclose all pending criminal prosecutions against them. Non-disclosure of such will result in the officers' immediate removal from Eskom site or duties*.

3.8 Contract Management and Accountability

[1] Regular performance reviews will be conducted to assess the achievement of outcomes.

[2] Failure to meet agreed-upon outcomes will result in penalties, performance improvement plans, or contract termination.

[3] Service providers must continuously propose and implement innovative solutions to improve security outcomes.

3.9 Incident Response, Reporting and Investigation

[1] All incidents and response to incidents must be handled according to the relevant Standard Operating Procedures (SOPS) and/or work instructions for each site.

[2] All incidents and response must be reported immediately to the Eskom control room.

[3] The SAPS must be contacted immediately only for criminal incidents or suspected ongoing criminal activities.

[4] Daily status reports are to be supplied by the service provider.

[5] All security threats, must be responded to within five (5) minutes (NKP areas) and eight (7) minutes Non NKP areas without compromising safety of people, animals and property. This must be verifiable through GPS tracking and Control room logs

[6] The contractor is to ensure that all involved personnel are available for relevant court proceedings, incident investigations and assist Eskom and the SAPS in their investigations as and when required.

[7] All incidents (including incidents in terms of the Occupational Health and Safety Act), should be reported immediately and a preliminary investigation report provided within **24 hours** as well as a final Incident investigation report within **Seven (7) days.**

3.10 Operational requirements

3.10.1 Supervisor and Patrol Vehicle Operational Requirement- Armoured Vehicle

The nature of duties shall entail but shall not be limited to the following:

[1] Supervisor must be able to respond to any security threats spotted by Drone team.

[2] All Supervisors must always have handcuffs, two-way radio, and torches.

[3] The vehicle must be 3 Channel Dash Cam Front, Rear and Inside, 1080P Dash Cam IR Night Vision and Loop Recording.

[4] Vehicles must be fitted with siren, horn and security strobe lights.

[5] Vehicle must have charging provision for torches and cell phones.

[6] Supervisor Vehicle must be 4X4 double cab and 4X4 Club cab for patrolling vehicles

[7] The Contractor must always report to Eskom security shift Supervisor on duty.

[8] Vehicle must be fitted with a GPS tracking device to provide accurate location, speed, and direction of the vehicle.

[9] GPS tracking device must be Geo-fenced according to geographical boundaries of operational area of responsibility.

[10] All Supervisors must have work issued cell phones to be used when two-way radio network fails.

[11] Patrolling, monitoring, and safeguarding of affected critical and vulnerable areas in and around the plant and other random proactive patrols.

[12] Supervisor will escort the fuel oil trucks, diesel trucks and coal trucks movements from entering the gate through the delivery value chain until they exit the station and any other suspicious vehicle/person.

[13] Supervisors must keep evidence of incidents that occurred and must be available to testify during disciplinary proceedings and in court.

[14] Supervisors shall monitor critical outside key points such as Overland Conveyor belt infrastructure, Raw water dam, AWR Ash dam, Sewerage treatment plant, Coal stock yard, Ash pipe lines, and perimeter fence to prevent act of criminality such as plant tempering, vandalism, unauthorised access, unauthorised removal of copper cables, other asset and equipment, bypassing security measures, security breaches, security incidents and industrial actions.

[15] Monitor all access route leading to the station during public disorder situations and emergencies.

[16] Compile situational reports and do daily briefings and de-briefings on location (issuing of tasks).

[17] Supervisor on duty must always carry Firearm and firearm permits as per the Firearm control Act.

[18] Supervisor should have undergone Regulation 21 training and continue to do so for at least once every 12 months for the duration of the service

[19] Both foot and vehicle patrols teams, shall provide a real time guard monitoring or guard patrol capability. The service provider and the system shall be capable of generating monthly reports, in line with service delivery.

3.10.2 Patrol Areas and Access Control Points

Areas to patrol shall cover or be selected from the following but not limited to:

[1] Main Entrance and Truck Delivery/Contractors gate

[2] Ash Dam

[3] AWR Sub-station,

[4] Ash Dam offices

[5] NKP and Non NKP Perimeter fence

[6] Coal Plant (Stockpile)

[7] Sewage plant

[8] Station parking areas.

[9] Roshcon

[10] All Dams

[11] Main entrance (reception, exit, entrance)

[12] Coal Truck gate.

[13] Overland Conveyor belt infrastructure

[14] Diesel and Oil Trucks from security main gate to weigh bridge and to offloading bays.

[15] All Duvha Sub-stations

[16] Cable Tunnel- Plant Unit 1 – 6

[17] Ash Pipelines.

[18] Driefontein Dam

[19] The entire Duvha Power Station.

[20] Eskom Village

[21] Sannishof residential

4. ADDITIONAL REQUIREMENTS INCLUDING TECHNOLOGY

4.1 Armoured guard house

[1] The supplier shall provide ten [10] armoured guard houses at NON NKP area and shall be responsible for the maintenance of any repairs and defects for the duration of the contract at the following site:

- AWR X 1
- Raw Water dam X 1
- Sewage Plant X 1
- Driefontein dam X 1
- Overland Conveyor belt X 3
- Roschcon X 1
- Main entrance gate X 1- newly erected fence
- Coal gate X 1

[2] The employer shall provide the specifications of the guard house required

[3] The employer shall provide electrical point once the guard houses are delivered.

[4] All the supplied guard houses shall become the property of the employer at the end of the service

[5] **Armoured guard house features:**

a) Level B6 ballistic protection including floor and roof.
b) ISO container bocks allow stacking and mounting on towers.
c) Size: 3x2.4m Guard house - 3 845 kg
d) Forklift pockets for easy handling.
e) Integrated window grids
f) Gunports in all windows
g) Integrated commercial air-conditioning system.
h) Intercom systems
i) Escape hatch on roof.
j) Documentation slot
k) Double manual interior lock
l) External padlock provision with anti-jam feature to prevent lock in
m) Provision for fitment of
n) two-way Radio’s
o) Security flood light or LED lights X 4
p) Antenna’s

NB: The contractor must ensure that all the guard houses are provided with : 2 standard chairs, 2 door standard wooden cupboards for storage and a wooden standard table.

4.2 Electronic key management systems

[1] The supplier shall provide the electronic key management cabinet system, and shall be responsible for repairs, maintenance and licensing of the systems for the duration of the service.

The system requirements:

1 X Stores 40 keys with breathalyser attached

1 X Fleet department = 120 keys- with breathalyser attached

1 X Security reception = 120 keys with breathalyser attached

2 X Security Operations =40 keys

[2] **Key features**

a) Automated issuing & returning
b) Industrial-grade robust construction
c) Personalised access parameters (one-key or multiple removal)
d) Multiple authentication methods (RFID; Fingerprint; PIN; Finger vein; QR)
e) Personalised & live key audit trails (Via cabinet; software; email)
f) Remote management software
g) Personalised security alerts & alarms
h) Individually locked key slots
i) Incorrect key return signals
j) Advanced license management module
k) Curfews: Dedicated time and dates
l) Co-Authorisation: Multiple user identification before release and return
m) Battery Backup
n) On-board Memory (zero data loss)
o) Industrial-grade ID Plugs (fobs)
p) High-durability permanent key seals
q) Access control integration (Employee data sync; turnstile blocking; license/permit management; offline access)

[3] **Hardware Security**

a) Internal door hinges with minimal tolerances,
b) Alarm contacts for unauthorised entry,
c) Vandalism-resistant internal control unit.

[4] **Certifications & Compliance**

a) ISO:9001- Certified Quality Management,
b) ISO:14001- Certified Environmental Management,

c) ISO:27001- Certified Information Security Management,

[5] **Remote Access & Reporting**

a) Remote access via web and dedicated mobile ecos App,

b) Automated email reports and alerts,

c) Real-time monitoring,

d) Video call verification at cabinet

[6] **Software**

a) ISO 27001 Information Security Management Certification
b) Integration into existing access control system, including turnstile blocking and employee data sync.
c) License and permit management (Up to 100 per employee)
d) Full system diagnostics and reporting remotely for quick fault detection.
e) Curfews on keys & Co-authorisation / Lockout functionalities
f) Automatic key audit registers and reports via email
g) Fleet tracking and reporting
h) Mileage records
i) Fuel level and litres refuelled records
j) Breakdown and maintenance reports
k) Independent from IT infrastructure
l) Built-in LTE modem – unlimited data on own network
m) Automatic cloud updates
n) ISO 27001 Information Security Management Certification

5. MAINTENANCE OF SECURITY SYSTEMS

5.1 CCTV Maintenance

5.1.1 Executive Summary

Maintaining the existing CCTV systems is therefore essential. Reliable, real-time monitoring enables the control room to respond swiftly to incidents, protecting infrastructure and personnel. Immediate maintenance of these systems must be treated as a priority to ensure optimal protection of critical assets and safeguard the safety of employees.

5.1.2 Types of maintenance to be performed:

5.1.2.1 Preventative maintenance

For CCTV is a proactive approach that ensures surveillance equipment remains reliable, secure, and fully operational. It involves scheduled activities designed to reduce the risk of system failures and extend the lifespan of cameras, recorders, and related components. By consistently maintaining CCTV systems, organizations can minimize downtime, avoid costly repairs, and maintain high security standards.

5.1.2.2 DVR/NVR

- The Contractor shall conduct monthly inspections to verify that all recording servers are operational and actively recording. Any faults or interruptions shall be reported immediately and rectified in accordance with the maintenance protocol.
- The Contractor shall perform monthly checks to ensure that all recording servers have sufficient

available storage capacity to maintain uninterrupted recording functionality. Any risk of data loss due to insufficient space shall be proactively addressed in accordance with the maintenance protocol.

- The Contractor shall ensure monthly that the server cabinet is cleaned and maintained in a dust-free condition monthly, in accordance with prescribed IT hygiene standards.
- The Contractor shall verify and adjust monthly the system time on all recording servers to ensure alignment with the access control system time. Any discrepancies shall be corrected promptly to maintain synchronization across all platforms.
- The Contractor shall carry out general fault finding and undertake necessary repairs. Where repairs are not immediately feasible, the Contractor shall provide written recommendations for corrective action, including estimated timelines and resource requirements.

5.1.2.3 Servers and Workstation

- The Contractor shall verify monthly that all servers are online and actively recording. Any server found to be offline, or malfunctioning shall be reported immediately and restored to full operational status in accordance with the maintenance protocol.
- The Contractor shall conduct monthly inspections to verify that all recording drives have sufficient available storage capacity to support uninterrupted recording operations. Any risk of data loss due to inadequate free space shall be identified and addressed promptly in accordance with the maintenance protocol.
- The Contractor shall ensure that the PC cabinet is cleaned monthly and maintained free of dust, debris, or any contaminants that may compromise equipment performance or safety.
- The Contractor shall verify monthly and adjust the system time on all relevant PCs to ensure synchronization with the access control system. Any discrepancies shall be corrected promptly to maintain accurate event logging and system integrity.
- The Contractor shall perform general fault diagnosis and undertake necessary repairs to restore full functionality. Where immediate repair is not feasible, the Contractor shall provide written recommendations for corrective action, including the nature of the fault, proposed solutions, and estimated timelines for resolution.
- The Contractor shall inspect all relevant cabling monthly to ensure that connections are secure, intact, and free from damage or interference. Any loose or faulty cables shall be reported and rectified promptly in accordance with the maintenance protocol.
- The Contractor shall verify the operational status of the mouse, keyboard, and display screen during each scheduled maintenance visit. Any faults or malfunctions shall be reported and addressed in accordance with the maintenance protocol.
- The Contractor shall verify monthly that all surveillance camera feeds are fully visible and functioning within the Security Control Room. Any missing, obscured, or malfunctioning feeds shall be reported immediately and rectified in accordance with the maintenance protocol.
- Operating system software upgrades shall be performed as necessary to ensure system stability, security, and compatibility with supported applications.
- Customization of software-generated reports shall be provided to meet user-specific requirements and operational needs.

5.1.2.4 Cameras/Housing

- During routine maintenance, ensure all cameras are properly focused and aligned, and that each lens is clean and free of dust.

- Clean camera lenses and housings during each scheduled maintenance day.
- Ensure all critical surveillance cameras remain active and are continuously displayed on control room monitors.
- Carry out general fault diagnosis and perform necessary repairs or provide recommendations for corrective action.
- Inspect the interior of each camera enclosure monthly to ensure it is clean and free of moisture.
- Verify that pan, tilt, zoom, and focus functions are fully operational on all PTZ cameras.
- Ensure each camera's field of view is adjusted to meet the customer's specific monitoring requirements.
- Relocation/adding cameras strategically to cover blind spots.

5.1.2.5 Monitors/computer peripherals

- Check all control room monitors daily during maintenance to ensure display images are clear and free from distortion.
- Adjust and verify contrast and brightness settings on all monitors to ensure optimal display quality.
- Conduct general fault diagnosis, perform repairs where possible, and provide recommendations for unresolved issues.
- Clean all monitor screens, control panels, and keyboards on every scheduled maintenance.

5.1.2.6 Alarm Systems

- Ensure that all alarm systems are functional and correctly received by the control room.
- To test and maintain your alarm system for optimal performance.
- Perform monthly sensor checks, verify monitoring communication and inspect backup power.
- Perform repairs where possible and provide recommendations for unresolved issues.

5.1.2.7 Power/Cabling

- Conduct general fault diagnosis, perform repairs where possible, and provide recommendations for unresolved issues.
- All UPS and their batteries to be inspected on every schedule maintenance.
- Inspect cabling on all security devices to ensure connections are secure and cables are in good condition.
- Inspect all power connections to security devices, control panels, and auxiliary systems.
- Ensure AC plugs are firmly seated in outlets or power strip.
- Check for signs of overheating, discoloration, or wear around plugs and sockets.
- Confirm no exposed wires or damaged insulation.

5.1.2.8 Network

The Contractor shall be responsible for the ongoing maintenance of the fibre optic network infrastructure. This includes routine inspections, fault detection and resolution, cleaning of termination points, testing of signal integrity, and timely replacement of damaged or degraded components. All maintenance activities

shall be documented, and any network disruptions or risks shall be reported immediately to the Client with proposed corrective actions.

NB: Fibre breaks or faults are to be treated as priority 1 calls or incidents.

5.1.3 Corrective maintenance

- In CCTV refers to unscheduled repair work carried out when a fault or failure is detected in the surveillance system. Its purpose is to restore cameras, recorders, or supporting equipment back to proper working condition.
- The equipment may be checked, serviced and adjusted as required for proper operation.
- Any defective components that are replaced or repaired shall be retained by the Employer and shall not be removed, reused, or disposed of by the Contractor without prior written consent.
- All work performed under this Agreement shall take place during standard working hours, defined as 07:00 to 16:00 Monday to Thursday and 07:00 to 12 on Fridays, or on an alternative day mutually agreed upon by both parties, excluding recognized public holidays.
- In event of breakdowns, technicians must be available for support and restore the system on a 24-hour basis.
- The contractor shall be responsible for minor installations, relocations, and replacements of security devices, as required, to eliminate blind spots and ensure continuous coverage.

5.1.4 Defects

The Contractor shall promptly repair all defects raised, in accordance with the timelines and standards stipulated in this Agreement.

The following terms and conditions shall apply to the successful tenderer upon acceptance of the tender award:

- Working hours shall align with Eskom's standard working hours, as applicable at the time-of-service delivery.
- A daily timesheet, maintained by Eskom, shall be signed by both the technician and their assistant at the end of each maintenance day to confirm attendance and work performed.
- Job cards shall be submitted to and signed off by the designated Eskom supervisor at the conclusion of each maintenance day. No payment shall be processed without a duly completed and approved job card.
- Payment for hours worked shall only be made upon verification and signature by the designated Eskom supervisor.
- All travel-related costs shall be deemed included in the tendered price. No additional claims for travel expenses will be entertained.
- The Contractor shall be responsible for providing all personnel with the necessary Personal Protective Equipment (PPE) required to safely perform their duties, in accordance with applicable health and safety regulations.
- Under no circumstances shall personnel be permitted to travel in the rear cargo area of a Light Delivery Vehicle (LDV). All personnel and contractors operating on Eskom premises shall strictly adhere to Eskom’s Cardinal Rules and site-specific safety protocols.

5.1.5 Infrequent maintenance (applicable to all the systems)

Refers to work that falls outside the scope of routine scheduled systems maintenance. These activities are

typically unplanned and arise from unforeseen issues or specific service needs., ad hoc repairs, and the supply or replacement of consumables. Such services shall not be included in the fixed monthly maintenance charges and will instead be invoiced separately, based on a predetermined fixed rate per item or service rendered. All infrequent maintenance activities shall be documented and approved prior to execution. They include:

- Call-out services for urgent troubleshooting or system failures.
- Ad hoc repairs to address unexpected faults in cameras, recorders, cabling, or network components.
- Supply or replacement of consumables, such as power adapters, connectors, or storage drives.

Such services are not covered under fixed monthly maintenance charges. Instead, they are invoiced separately at a predetermined fixed rate per item or service rendered.

5.2 Callouts, Breakdowns and Repairs occurring after normal working hours

5.2.1 Standby/Callouts

The Contractor shall ensure availability of personnel to attend to breakdowns outside of normal hours. A weekly/monthly standby rooster must be provided. The standby team per week to be made of the following skills but additional resources maybe be requested depending on the size of the breakdown:

1 X Technician

NB: Only the employer shall authorise the call out after hours. Employer shall not be responsible for the cost of unauthorised call out.

- Requests for callouts during these hours must be submitted to the after-hours logging service, which will record the date and time of the call and notify the designated standby support personnel.
- Users may request changes or modifications to the location or operation of equipment.
- The Contractor shall provide all consumables required for the effective operation of the entire system, in accordance with the pricing outlined in the approved price schedule.
- Damage to equipment caused directly or indirectly by lightning shall be assessed by the Contractor, whose professional judgment shall determine the extent and nature of the damage.
- Equipment might damage due to negligence or wilful misconduct which will be subjected to assessment.

5.3 Spares and Vendor List

The Contractor shall submit to the Employer a complete list of additional spare parts required, including part numbers, quantities, and unit prices. This list shall be subject to the Employer's review and formal approval. Upon approval, the Contractor shall supply the listed spare parts as part of the Works, and the cost of these spares shall be borne by the Employer.

Furthermore, the Employer shall maintain an adequate inventory of spare parts, in accordance with the Original Equipment Manufacturers (OEM) recommendations, to ensure uninterrupted maintenance and operational reliability throughout the maintenance period.

5.3 Spares and Vendor List- Annexure A

No	Items
1	CCTV
2	2MP H6M Outdoor Mini-Dome with IR and 3.0mm Lens
3	2.0 MP; WDR; LightCatcher; Day/Night; Indoor/Outdoor Bullet
4	CAM; H5A IR PTZ; Pendant 2MP 40X 300m
5	PoE injector 802.3bt 90W Single Port
6	Schneider Circuit Breaker 3P 63A C 10KA DIN MCB 3M
7	Lambda SFP Module 1.25G LC Single Mode
8	SP PS 12VDC 10Amp Enclosed
9	Inverter 1000W PSW 12VDC Intell Charge
10	CBI SM 08 Fibre HDD Cable G657A1
11	TP-Link 24Port POE switch,8 Port POE and Fiber switch
12	2KVA and 3KVA Tower UPS Online
13	IP Horn Speaker that integrates with ACC.
14	Clearline 5 Way Multiplug Surge
15	Lambda Single Fan Unit & Plug
16	Patch Lead MM OM3 LC-LC Duplex
17	RJ45 connectors
18	RJ45 Boot
19	Mecer 43LF88
20	Codeless desktop mouse
21	Wireless keyboard

NB: Spares shall not be limited to the items listed above, and the Contractor shall be responsible for verifying and confirming the completeness of the list.

5.4 Access Control Systems Maintenance- Access Portal

- The Contractor shall verify the functionality of all access control components, including card readers, biometric scanners, keypads, and electronic door locks. This verification shall be conducted through scheduled testing procedures to ensure accurate operation, responsiveness, and integration with the central security system. Any faults, delays, or inconsistencies shall be documented and rectified promptly in accordance with the maintenance protocol.
- Check access logs for unusual activity or failed entry attempt.
- Ensure backup power systems (UPS or batteries) are charged and operational.
- Test emergency override mechanisms and fail-safe features.
- The Contractor shall ensure that all turnstiles are maintained in optimal working condition to support seamless and secure access control. This includes conducting regular inspections, testing mechanical and electronic components, performing preventative maintenance, and promptly addressing any faults or malfunctions. All service activities shall be documented, and any issues affecting performance or security shall be reported and resolved in accordance with the agreed maintenance protocol.
- Run system diagnostics to check for software or firmware issues.
- Maintain a secure backup of system configurations and user data.
- Server and the database must be updated as required.

- The Contractor shall routinely check all printers to ensure they are functioning correctly and producing output as required. This includes verifying print quality, paper feed mechanisms, toner or ink levels, network connectivity, and any error messages. Any issues identified shall be documented and resolved promptly to avoid disruption to operations.
- Inspect all workstations and connected peripherals to ensure they are fully operational.
- Verify current stock levels of cards and cartridges.
- The Contractor shall ensure that all boom gates are maintained in excellent working condition to facilitate smooth and secure operational flow. This includes routine inspections, lubrication of mechanical components, testing of control systems, and prompt repair or replacement of any faulty parts. Any issues affecting performance or security shall be reported immediately and addressed in accordance with the agreed maintenance schedule.
- Check the cabling to ensure they are secure and in good condition.
- The Contractor shall be responsible for the ongoing maintenance of the fibre optic network infrastructure. This includes routine inspections, fault detection and resolution, cleaning of termination points, testing of signal integrity, and timely replacement of damaged or degraded components. All maintenance activities shall be documented, and any network disruptions or risks shall be reported immediately to the Client with proposed corrective actions.

5.4.1 Maintenance service shall include:

- Breakdowns and repairs occurring during normal working hours.
- Management and implementation of all necessary upgrades and changes to software and firmware versions associated with the system infrastructure. This includes monitoring for updates released by vendors, assessing compatibility and impact, scheduling installations to minimize operational disruption, and ensuring all systems remain secure and fully functional post-update. Detailed records of all changes shall be maintained and submitted to the Client upon request.
- The ensuring of backups and keeping such backups in a safe place.
- The ongoing training of staff in the correct operating procedures of all relevant software and hardware systems. This includes initial onboarding, refresher sessions, and training updates following system upgrades or procedural changes. Training shall be tailored to user roles, documented appropriately, and conducted in a manner that ensures operational efficiency, system security, and compliance with organizational standards.
- Doing software maintenance such as creating new users and/or system layouts.
- Moving or removing of equipment or attachments thereto as may be required for maintenance.
- purposes.
- The servicing of parts as required during normal maintenance periods as a result of wear and tear or breakdown.
- The contractor shall be responsible for minor installations, relocations, and replacements of security devices, as required, to eliminate blind spots and ensure continuous coverage.

5.4.2 Spares for access control : Annexure B

No	Items
1	Access Control
2	EABR readers
3	Sigma light reader
4	EABR relays
5	Controller PC board for Centurion sec 2 boom

No	Items
6	Break glass units
7	Maglock heavy duty
8	Battery 12v 7.2ah
9	Network switch 48 port
10	Micro SD card 16gb
11	Molex Cat 6 rolls
12	HID access cards
13	Slim tag access cards
14	IMPRO ISR Card enroller
15	IMPRO MSO300 finger enrolment
16	Over-write switch
17	Repoo C260
18	Entrust Sigma DS2 single sided ID card printer
19	Zebra ZC100/ZC300 YMCKO, 200 Print ribbon

5.5 Intruder Alarm System Maintenance

Maintaining the intruder alarm system is essential, as its effectiveness relies on consistent reliability. Intruder alarms protect buildings and valuables against theft, but without proper maintenance the system may fail to activate during a break-in, leaving assets exposed and vulnerable.

5.5.1 Inspection (Weekly)

- Visual check of control panels for damage or tampering.
- Inspect sensors, detectors, and keypads for obstruction or wear.
- Visual check of beam transmitters and receivers for physical damage, misalignment, or obstruction.
- Inspect mounting brackets, poles, and housings for stability and corrosion.
- Verify cabling and connections are intact and secure.

5.5.2 Cleaning

- Clean lenses of transmitters and receivers to prevent false alarms caused by dust, insects, or moisture.
- Remove vegetation, spider webs, or debris that may obstruct the beam path.

5.5.3 Power Supply

- Confirm system is receiving mains power.
- Test battery backup; replace or recharge batteries if needed.
- Check fuses and power supply units for faults.

5.5.4 Testing (Monthly or as needed)

- Arm and disarm system to confirm proper operation.
- Test all sensors (motion, door/window contacts, glass break detectors).
- Verify alarm sirens and strobes activate correctly.
- Test beam alignment and sensitivity to ensure proper detection range.
- Simulate intrusion to confirm alarm activation.
- Verify integration with the main intruder alarm control panel.
- Check response time and communication with monitoring station (if applicable).

5.5.5 Software and Configuration

- Check system logs for errors or tampering attempts.
- Update firmware/software if required.
- Verify user codes and access permissions.

5.5.6 Preventive Maintenance

- Clean sensors and detectors to prevent false alarms.
- Ensure environmental factors (dust, moisture, temperature) are within safe limits.
- Replace worn components proactively.
- Adjust beam alignment if shifted due to weather, vibration, or tampering.
- Replace worn or damaged components proactively.
- Ensure environmental conditions (rain, fog, direct sunlight) are considered in beam positioning.
- The contractor shall be responsible for minor installations, relocations, and replacements of security devices, as required, to eliminate blind spots and ensure continuous coverage.

5.5.7 Documentation & Reporting

- Record all maintenance activities and test results.
- Provide a compliance certificate or service report.
- Recommend upgrades or replacements if system performance is compromised.

5.5.8 Spares List- Intruder Alarms: Annexure C

No	Items
1	Control Panel with 3 inputs, 2 outputs.
2	Alpha Keypad
3	LSH20 Control Panel Battery
4	AA Cell Lithium - Peripherals Battery
5	Outdoor Motion Viewer - PIR Detector with Camera
6	Outdoor Siren with Strobe
7	D Cell - Alkaline Battery

No	Items
8	Outdoor and indoor

NB: Spares shall not be limited to the items listed above, and the Contractor shall be responsible for verifying and confirming the completeness of the list.

6. DOCUMENTATION (APPLICABLE TO ALL SECURITY SYSTEMS)

[1] The Contractor shall upgrade and/or replace all existing manuals and documentation to accurately reflect the current versions of software and hardware installed as part of the Works.
[2] All documentation shall be:
- Comprehensive and complete.
- Up-to-date and current.
- Aligned with the actual configuration and functionality of the systems provided.

[3] The format, content, layout, and overall quality of all documentation shall be subject to the Employer's review and formal approval.
[4] The Contractor shall incorporate any revisions or enhancements as required by the Employer to ensure:
- Clarity and ease of use
- Practical usability for operations and maintenance staff
- Compliance with project standards and contractual requirements

[5] In cases where design drawings are not available, the contractor shall study the system design and prepare the required drawings.

7. TRAINING

[1] All training provided by the Contractor shall be delivered exclusively in the form of on-the-job training. The training must be of a standard sufficient to ensure that the Employer's personnel are fully competent to perform complete system maintenance, fault diagnosis, and full system reconfiguration by the conclusion of the contract period.

[2] The Contractor shall develop and implement a formal training program, which must be reviewed and approved by the Employer's designated representative. Such approval shall confirm that the training has been delivered satisfactorily and that the required competency standards have been met.

8. MANUALS

The manuals shall include the following:

1) An overview of the CCTV and intruder detection system, including the equipment block schematic

2) The functions and features of each item of equipment.

3) Individual operating instructions for each item of equipment.

4) Detailed operating instructions for all modes of operation of the CCTV system.

5) Software/Applications manuals

6) Specialised item manuals where appropriate

7) Training Schedule for protective service personnel

9. PERFORMANCE

[1] The Contractor guarantees that the CCTV system shall perform in full compliance with the Employer's specified performance requirements. This guarantee encompasses, but is not limited to:
- Functionality: All cameras, recorders, and associated equipment shall operate as intended, delivering the required surveillance coverage.
- Reliability: The system shall consistently perform without undue failures or interruptions.
- Efficiency: Configurations and integrations shall be optimized to ensure effective operation and resource utilization.
- Compliance: All components shall meet the technical specifications and standards outlined in the contract.

[2] The Contractor shall be fully responsible for ensuring that all hardware, software, configurations, and integrations conform to the agreed standards and deliver the expected operational outcomes.

10. COMPLETION

[1] Upon termination of this Agreement, the Contractor shall demonstrate that the CCTV system operates at a level equal to or exceeding the performance and functionality established at the time of installation. This demonstration shall include:
- Verification of operational parameters: Confirming that all cameras, recorders, and associated equipment function within the specified tolerances.
- Validation of configurations: Ensuring that system settings, integrations, and network connections remain aligned with contractual requirements.
- Assessment of system outputs: Reviewing recorded footage, monitoring capabilities, and reporting functions to confirm compliance with original specifications or any approved enhancements implemented during the contract period.

[2] The demonstration shall be conducted in the presence of the Employer's designated representative and formally documented to certify that the system meets or exceeds the agreed standards.

11. TESTS AND QUALITY CRITERIA

[1] The Contractor shall develop a comprehensive maintenance testing and quality assurance plan that outlines all procedures and checks to be conducted during each CCTV system maintenance activity. This plan shall include:
- Detailed methodologies: Step-by-step procedures for testing system components, configurations, and integrations.
- Acceptance criteria: Clear standards against which system performance and reliability will be measured.
- Frequency of checks: Defined intervals for inspections, testing, and verification activities.
- Documentation protocols: Requirements for recording test results, corrective actions, and approvals.

[2] The proposed plan shall be submitted to the Employer for review and formal approval prior to implementation. The Contractor shall ensure that all maintenance activities are carried out in strict adherence to the approved plan, thereby maintaining system integrity, operational reliability, and compliance with contractual performance standards.

12. REPRESENTATIVES

[1] The Employer reserves the right to appoint one or more representatives from the Engineering and Maintenance Departments to inspect all components and activities undertaken during CCTV system maintenance operations, and to witness any tests specified under this Agreement.

[2] The presence or participation of the Employer's representatives during such inspections or tests shall not, under any circumstances, relieve the Contractor of any contractual obligations, responsibilities, or liabilities relating to the performance, quality, or compliance of the Works.

[3] The Contractor remains fully accountable for ensuring that all maintenance activities and system outputs meet the agreed standards and contractual requirements.

13. TWO-WAY RADIO SYSTEMS

The supplier shall provide **15 two-way** radio (Halo SS-70- display) and shall be responsible for maintenance, repairs inclusive of the current two-way radios (**33** two-way radios, **7** vehicle base radios and control base radio) and licence/subscription fees of the current halo radio despatcher system for the duration of the service.

The radio features are as follows:

[1] Portable – small in size

[2] Network Support: 2G,3G, 4G LTE

[3] Dual SIM card slot: Micro SIM card with auto switching between networks.

[4] Voice Recording,

[5] Real Time GP's Tracking

[6] Emergency button (panic)

[7] Nationwide communication (GSM Network)

[8] Live monitoring on the Dispatcher system- web based/software application.

[9] Icasa approved.

[10] Compatible for use within Power Stations plant environment

[11] Able to receive phone calls.

[12] Call back functionality

[13] Group call functionality

[14] unlimited coverage

14. 2D VEHICLE SCANNER

The supplier shall provide 16 X 2D vehicle scanning devices for various identified sites. The contractor shall supply and manage the server and be responsible for repairs, replacement, maintenance and licence of the system for the duration of the service.

a) Device features:

b) Verify authenticity of visitors' information

c) Track time spent on premises

d) Load and save regular visitors

e) Capture personal details in seconds

f) Safeguard information electronically

g) Set automated reports or pull instantly as needed

h) POPI compliant

i) Training and support included

j) Data storage for up to 5 years

k) A user-friendly, web-based interface

l) Automated back end and device syncing

m) Ability to scan and read the bar codes on the documents and transfer to the connected computer

NB The contractor shall handover the server and the 2d scanners to the employer at the end of the service and shall ensure that the integrity of the information is not compromised in any way.

15. BODY CAMERAS

Body cameras (HD Video Recording, water resistance and dust resistance body cameras with docking system) supplied by contractor to each on duty security officer to be carried on their person for the duration of shift duties as per assigned access control, static guarding, patrol & alarm response duties, as per paragraph 2 scoped areas. These cameras must always be 100% functional & available. Cameras & docking stations must have video download integration though software (DEMS) to securely transfer and manage the data.

16. MOBILE CAMERAS AND TRAP CAMERAS

16.1 Mobile cameras

The company will be required to provide mobile surveillance cameras as per the BOQ as and when required. As per the identified security threat condition. A 12-to-48- hour notice to the Security service provider will be given to ensure availability of security surveillance system. Requests be made by the duly appointed Service Manager. Solar Generator Trolley mobile cameras: the service provider should supply as and when required the high performance, portable power solution designed mobile cameras equipped with powerful solar panels. With a robust and weatherproof design bult to withstand tough condition and provide dependable power when needed.

16.2 Trap Cameras

The employer shall provide 10 trap cameras. The contractor shall be responsible for the repairs, maintenance, hydra system licence subscription fees and support for the trap cameras for the duration of the services.

NB: Supplier advised to conduct site walk prior for quotation on technology proposal

Maintenance, repairs, and licence/subscription costs of all items listed under will be at the cost of the supplier throughout the contract period and as such will remain the property of Eskom. Eskom will only take over the administration, maintenance, repairs, and licence/subscription costs upon the expiry of the contract.

17. FIREARMS

[1] Only Eskom approved firearms namely, 9mm pistols shall be allowed for usage in terms of this contract.

[2] Supervisor must have the following in his/her possession whilst on duty: firearm competency certificates, ID card, PSIRA Card, daily firearm permits for the specific firearm in possession thereof.

[3] Security Company is responsible for providing firearms, ammunition, firearm safe and registers as per Firearm Control Act 60 of 2000 this includes issuing of firearm permit whilst on duty:

a) Only company firearms licensed in the security service providers name may be utilised as per this contract.

b) The contractor must ensure provision of equipment / facilities for making firearms safe. A procedure to that effect, should also be in place. Such facility must be secured, to meet the requirements of Firearm Control Act 60 of 2000 relating to safe keeping and storage of firearms, such as CCTV, alarm systems, dual locking mechanisms- two-man rule

c) Each Officer and Supervisor officer must be provided with two full loaded (ammunition) magazines.

d) The service provider must ensure that Security officer's private firearms are not utilised for their business purposes, in terms of this contract. No personnel are allowed to bring personal firearms on site.

e) Firearms must comply with the firearm Control Act Requirements as indicated below:

- Company's Firearm licence valid for 5 years (Mandatory)
- Appointment of the responsible person / Armoury manager/Supervisor (Mandatory).
- Firearm competency certificates of owner or appointed responsible person (Mandatory) o Training records of owner or appointed responsible person for handle and use of firearms for business purposes all prescribed firearms and Knowledge of Firearm Control Act (FCA) from a SASSETA accredited institution. (Mandatory).
- The company must have a firearm safe handling procedure. (Info required before contract commencement).
- Security guards to carry firearms must be trained on use and handle of firearms for business purpose (Information required before contract commencement)
- Security guards to carry firearms must have SAPS competency certificate (Information required before contract commencement).

[4] Safe handling of firearms during shift changes must be always adhered to. The contractor must ensure that a procedure is put in place to that effect.

18. ADDITIONAL REQUIREMENTS

[1] All security personnel issued with firearms must possess firearm competency certificates (issued by SAPS) and always carry it.

[2] All security personnel, will be expected to sign a declaration of Secrecy before commencements of their duties in terms of this contract.

[3] All security personnel may be subjected to a screening / vetting process and polygraphy testing-

[4] All security personnel should be able to read, write and express themselves well in English.

[5] All security personnel may be required to undergo a polygraph test as and when required at the supplier's own cost

[6] All security personnel must be trained on the Standard Operating Procedures (SOPs) relevant for their site of deployment and/or be made available for training by Eskom at no additional costs on any process or procedure necessary for them to do their duties. Proof of training must be kept on file and availed to Eskom on request.

[7] No security personnel are to be deployed in terms of this contract, before undergoing necessary Eskom induction, training, and assessments. Eskom reserves the right to remove such Officers that have not complied with this requirement from their sites or duties as per this contract at the cost to the contractor.

[8] Shift supervisors to conduct SMAT (Behavioural Safety Observation) and submit via the Eskom App

[9] Contractor to attend Monthly SHEQ Meeting, and conduct plant safety walk by Safety Officers and SHE Representative

[10] Security Personnel should observe the provisions of the Criminal procedure Act and all relevant legislation regarding the use of minimum force. Security personnel shall at all-time use minimum force sufficient to bring the situation under control and such force shall cease as soon as the situation is brought under control. No deliberate assault on suspects will be condoned.

[11] The Security Officers/personnel will be expected to do a pre-job/ daily risk assessment and safety talks before commencement of every shift. The risk assessment must be updated as new risks are identified or emerge.

[12] Before posting security, members and review the risk assessment when new risk arises.

[13]. Security officers will be subjected to alcohol and drug testing at sites and shall have their person and possessions searched, without exception. Refusal to co-operate will necessitate immediate removal of the officer /personnel from site at the cost of the Contractor. Defaulting security officers are not to be deployed at any other Eskom site, under any circumstances

19. PATROLS, ESCORTING AND RESPONSE SERVICES

[1] Execution of crime patrols and response at Duvha Power station – NKP and Non NKP areas

[2] Patrolling of NKP and Non NKP areas at irregular intervals and not in a specific sequence, to detect the presence of unauthorised people, suspicious activities or occurrence that may endanger the property and employees /contractors and visitors.

[3] Prevention of unauthorised removal of Eskom assets from site

[4] Perform response services to all Duvha Power Station sites.

[5] Provide escort duties to Eskom employees and contractors working in remote areas and hotspot.

[6] Provide escort to Fuel Oil trucks from point of entry, during offloading until exit.

[7] Eskom Security manager or his/her delegated official reserves the right to redirect crime prevention activities in his/her area of responsibility.

[8] No deviation from the operational plan without authorisation of the Eskom security manager or his/her delegated official will be permitted.

NB: **The Contractor's duties are not limited to the above but shall include any other legal security activities that Eskom may introduce to enhance security operations, and such activities shall be communicated to the service provider either verbally or on writing.**

20. TRAINING

All Supervisor, Security Officers deployed must have been trained in terms of the various legislative requirements. (Private Security Industry Regulatory Authority (PSIRA), National Key Point (NKP), Aviation training, Firearm Control Act (FCA) and Critical infrastructure Act. All Security personnel to comply with the continuation and refresher training in terms of the NKP and FCA.

21. Reporting and Communication

a) The Contractor must ensure suitable continuous communication between the operational control room and their deployed staff. Either one or more of the following mediums of communications shall be provided as per user requirements:

- hand-held radios,
- satellite radio, *NB: radios must be monitored in the site control room*
- contracted cell phones,
- base radios (compulsory in all vehicles)
- push to talk (PTT).

b) Deployed security personnel shall remain in constant reach and communication with the Eskom security control room, Supervisors, Security manager.

c) Situational reports and a complete operational report – Daily briefings and debriefings on location (issuing of tasks).

d) A communication platform will be established by the Security Service provider with the Supervisor / Operations managers and Eskom designated security personnel (to be stipulated).

e) Supervisors to provide weekly status report which will reflect the following:

- Daily postings
- Vehicle information and kilometres driven per day
- Equipment checklist
- Site firearm / ammunition register
- Incident register (arrests, recoveries)
- Occurrence register entries of note.

22. SEGREGATION OF ROLES

The Eskom In-house and contract security teams will be responsible for the day-to-day security functions and operations at the Power stations.

The Private security team will be deployed as per par.2 and shall remain under the control of the appointed Manager / Supervisor during the tour of duty.

• The responsible Eskom Security Manager shall exercise overall command of the Security resources on site.

23. CONTINGENCY PLAN

The service provider must have contingency plans in place and share with the employer for the following:

a) Own Strike / Labour unrest amongst own staff.

b) Shortage of Manpower due to e.g., absenteeism, sick leave, or annual leave.

c) Equipment Failure Vehicle breakdown and Communication system.

d) Mobile cameras for remote areas monitoring as and when required

e) Additional members for outages and emergency posting

f) Additional technicians and technical resources

24. WORKING TIMES/SHIFTS

[1] Working times determined by PSIRA Act – 48 hours per week Shift workers and 45 hours per weekdays.

[2] The security service is required as per the agreed shift roster.

[3] A name list of Security officers deployed in terms of this contract must be provided on monthly basis, within 5 days prior to the commencement of the new month.

[4] The contractor is responsible to ensure that every shift complement is satisfied before commencement of the shift.

[5] Safe handling of firearms during shift changes must be adhered to at all times. The contractor must ensure that a procedure is put in place to that effect.

[6] Firearm Safes and Facilities must be provided by the contractor for the safekeeping of firearms not in use.

[7] The Supervisor team will be expected to do a pre-job / daily risk assessment and safety talks before commencement of every shift.

25. DOCUMENTATION

25.1 Security Operations

The following documentation is to be supplied by the security service provider within two weeks before a commencement of the contract:

[1] List of all potential security officers intended to be deployed on Eskom sites in terms of this contract.

[2] Certified ID copies, PSIRA certificates and security clearance certificates of all security officers.

[3] Certified copies of firearm competency certificates of the security officers.

[4] List of all firearms to be used and certified copies of the licenses.

[5] Certified copies of NKP certificates

[6] Certified copies of the company and Directors PSIRA registrations certificates.

[7] All site standard operating procedures

[8] A list of all vehicles and maintenance records for vehicles to be used as per this contract.

[9] Driver risk profiles must be submitted for every driver as per this contractor.

[10] A compressive risk assessment and a site risk assessment report for all sites.

[11] Emergency Preparedness procedure with relevant contact details.

[12] Equipment list per site.

[13] Standard operating procedures per site to include the following but not limited to and should be approved by Eskom representative before application:

a) Wearing of uniform standard.

b) Communication procedure.

c) Firearm handling procedure.

d) Shift changes.

e) Response process.

NB: The proof of communication relevant to the procedure must be made available to Eskom delegated official as and when required.

a) Security Register

[1] The Security Service provider will be required to provide the Occurrence Books for all their site of operations.

[2] Occurrence book to be correctly completed by Supervisor listing all occurrences / incidents.

[3] Contractor must ensure that quality registers are provided. Occurrence Book must remain bonded, with no loose pages.

[4] Accurate records of all occurrences are to be kept for a minimum of 12 months post the occurrence and should be made readily available to Eskom at any time.

[5] All the security personnel shall have the issued pocketbooks at all times

b) Occurrence Book

[1] Service provider shall record duty on and off in the Occurrence Book.

[2] Check for any reports of security interests from the person handing over and record this in the occurrence book for future reference.

[3] All patrols must be logged in the OB and cross reference the feedback as follows:

[4] Record all incidents reported to Protective Services.

[5] After shift completion, the supplier shall record a proper shift hand over to the next reliever and ensure that he/she notes all irregularities.

[6] The Supplier's Security Responsible (Supervisor) person shall record all visits to the premises in the occurrence book and place his/her signature next to entry.

[7] Book out and back from patrol.

[8] Record all irregularities found during the patrol.

[9] Record and specify times and places patrolled.

c) Technical

On completion of the installation the contractor shall provide Eskom with the following documentation:

[1] Detailed as-built drawings of the installation including the following:

a) A site layout diagram indicating the position of all equipment and devices installed. A complete cable block and wiring diagram with cable & wire numbers

b) A site layout diagram indicating the position of all equipment and devices installed

c) Coverage plots of the areas covered by intruder detectors and a list and description of each zone.

d) Coverage plots of the areas covered by cameras' fields of view

e) Alarm system zones

[2] Manufacturer's technical and maintenance specifications for each item of equipment installed.

[3] All documents shall be provided in soft and hard copy. Drawings softcopies shall be provided in Micro Station (DGN) format. Other soft copy documents shall be provided as pdfs.

[4] Software license certificates where needed.

[5] Recommended spares list.

[6] The Contractor shall provide all necessary additional or amended pages to ensure that every copy of manuals and drawing sets is complete and accurately reflects all modifications made to the Works up to the date of termination of this Agreement. These updates shall be incorporated in a manner that maintains consistency, clarity, and traceability within the documentation. The Contractor shall ensure that all revisions are properly indexed and integrated into the existing documentation sets.

26. SAFETY REQUIREMENTS

[1] All vehicles utilized to transport staff, must be fitted with SABS approved seatbelts.

[2] The Service provider is responsible to ensure that the security officers deployed at Ad-hoc sites have access to a shelter, water, and sanitation.

[3] All contractor personnel must receive a safety induction before they can be deployed on Eskom sites.

[4] Safety recommendations following an incident shall be implemented by all Security Service providers to prevent further reoccurrences at any of the Eskom site, as per allocated timeframes.

[5] Open fires, the use of bar heaters and hotplates as heaters at Eskom sites, is **totally prohibited.**

[6] Safety officer shall submit monthly man-hours to Eskom Security and safety department on the 1st day of every month.

[7] All the supervisor shall have all the relevant qualifications related to safety such as legal liability training, first aid, firefighting, - **Safety department shall provide additional requirements during the safety file evaluation**

27. SALARIES AND PAYMENTS

Security companies shall pay security guard at least the minimum wage specified on the Sectorial Determination, of the Private Security Sector, South Africa. Register all security guards with the Department of Labour: UIF, COID and provident fund.

28. UNIFORMS AND DRESS CODES

[1] The contractor must comply with legislative requirement (PSIRA Regulation 13). Uniform items must be kept in clean, neat, and good condition always.

[2] Uniform must be always in good condition in terms of the environment where security staff are deployed.

[3] Bullet proof vests shall be worn as part of uniform by all security officers. Only Eskom shall indicate the level of protection and provide Standard.

[4] The supply must ensure that all the employees or work force have the relevant uniform or gear (i.e., protective shields, bottom sticks, etc

[5] All Suppliers' Security guards shall dress in full uniform when on duty and no private clothes will be permitted to be worn with their uniforms.

[6] The supplier shall ensure that security guards uniforms are always neat and clean when on duty. Security officer with torn or damaged uniform/ PPE shall not be permitted to be posted at any Eskom posts.

[7] Reflective vests (bibs) will be worn with the uniform at all times

[8] The supplier shall ensure that all armed security officers and supervisors are always provided with and wearing body armour vest with uniform and comply with Eskom standard- *Wearing of Ballistic Resistance Body Armour by Security personnel Document Identifier: 240- 91252214*

[9] The supplier shall provide correct PPE to the security guards (firearms prescribed by Eskom, torches, panic buttons (handheld radios, bullet vest, rain suits, safety boots and hardhats prescribed by Eskom).

29. GENERAL PROVISIONS

29.1 All-Inclusive Service Delivery

- All security equipment, vehicles, firearms, ammunition, uniforms, communication devices **(BodyCams)**, protective equipment (Bullet-proof vests), and operational tools shall be included in the contract price.
- No startup costs, equipment deposits, or additional charges will be permitted.
- Service provider assumes full responsibility for all operational expenses including fuel, maintenance, insurance, and consumables.
- PSIRA regulations mandate that security equipment costs be incorporated into service fees, not charged separately.

29.2 Technology and Data Ownership.

a. **Ownership of Installed Technology**: All technology (e.g., surveillance cameras, access control systems, alarms, 2D vehicle scanners, GPS tracking devices, etc.) installed by the contractor during the period will remain the property of Eskom upon contract expiry or early termination.

b. **Data Ownership and Access**: All data collected (e.g., surveillance footage, access logs, incident reports) during the contract period will be the sole property of Eskom. The contractor must provide Eskom with unrestricted access to this data. The Security Manager or Risk & Assurance Manager will be the only people who can decide who will receive the information from Security Systems.

c. **Data Storage and Security**: The contractor must store all data securely in compliance with the Protection of Personal Information Act (POPIA) and other relevant legislation. Data must be encrypted and stored on servers located within South Africa unless otherwise approved by Eskom.

d. Data Handover: Upon contract expiry or termination, the contractor must provide Eskom with all data in a usable format (e.g., digital files, cloud access) and ensure no data is retained or deleted without Eskom's written consent.

e. **Monitoring Access**: Eskom must be provided with a secure link to monitor all surveillance and access control systems in real-time. The contractor must ensure the link is operational 24/7 and accessible to authorised Eskom personnel.

f. **Third-Party Control Centre Access**: Eskom must have the right to visit the contractor's or third-party control centre at any time, without prior notice, to inspect operations, verify compliance, and ensure data integrity.

g. **Licences and Data fees**: The contractor shall be responsible for ensuring that all license and Data fees for installed systems, equipment, and technologies are paid and maintained throughout the contract period, with ownership and responsibility transferring to Eskom upon contract expiry or termination.

30. KEY PERFORMANCE INDICATORS (KPIs)

KPI 1: Administration - Documentation and Reporting Accuracy

- Target 100% effective access control and timely submission of all required reports and documentation
- Measurement: Reported incident and administrative delays- invoice submission and weekly report-quality assessments and timeliness tracking.
- Penalty: 1% of the monthly task order for reporting deficiencies.

KPI 2: Visible Leadership

- Target: 4 X afterhours management site visit monthly and response to emergencies and incidents
- Measurement: Achieved targets, and response to incidents
- Penalty: 1% monthly task order for each percentage point below target.

KPI 3: Crime reduction, prevention and response

- Target: 100% Incident detection, prevention and response- response time 5 minutes. Non involvement of staff in criminal activities
- Measurement: Monthly incident report and trend analysis- Response times to incident, involvement of Staff in criminal activities. Detection and prevention of Crime
- Penalty: Total value of the loss recovery.
- 5% of monthly task order reduction for non-compliance to detecting and preventing incidents.
-

KPI 4: Resource Availability and Readiness

- Target: 100% availability of all security equipment and operational resources (vehicles, personnel communications, access control systems, CCTV systems, alarms systems 2D scanners, body cams, vehicle GPS,). Short posting limited to 10 per month
- Measurement: Monthly equipment audit and availability reports.
- Penalty: 2.5% of the monthly task order for each percentage point below target

KPI 5: Training and Legal compliance Requirements

- Target: 100% compliance with mandatory training, certifications, and legal requirements
- Measurement: Monthly, quarterly and annual compliance audits and documentation reviews
- Penalty: 3% monthly task order reduction for non-compliance
-

KPI 6: Safety Management

- Target: 100% compliance to all site SHERQ requirements, procedures and lifesaving rules
- Measurement: Monthly, SHERQ reports, audits
- Penalty: 3% monthly task order reduction for non-compliance

30.1 Measurement table: Annexure D

Eskom

KEY PERFOMANCE INDICATOR

S/N	STANDARD PERFORMANCE	TARGET	RATINGS	COMMENTS
1	ADMINISTRATION- DOCUMENTATION AND REPORTING ACCURACY	6		
	Effective Access Control	Zero Deviations	3	
	Invoices submitted on time in line with contract	Zero Deviations	3	
2	VISIBILITY- LEADERSHIP	9		
	Coaching		3	
	Site Visit- Monthly	4x Afterhours Visit	3	
	Management Response to emergency and incident	One hour	3	
3	CRIME REDUCTION, PREVENTION AND REDUCTION	9		
	Incident detection and Prevention	Zero Deviations	3	
	Response to emergency and Incident	5 Minutes	3	
	Involvement of staff in Crime	Zero Deviations	3	
4	RESOURCE AVAILABILITY AND READINESS	9		
	Availability of operational resources	Zero Deviations	3	
	100% System availability	Zero Deviations	3	
	Short posting- limited to 10 per month	Zero Deviations	3	
5	TRAINING AND LEGAL COMPLIANCE REQUIREMENTS	18		
	Psira, FCA Compliance,NKP compliance and SHERQ	Zero Deviations	3	
	Legal Contraventions	Zero Deviations	3	
	Firearm Control Act	Zero Deviations	3	
	Regulation 21- Annualy	Zero Deviations	3	
	NKP Annual continuation	Zero Deviations	3	
	Registration of all officers with PSIRA, and NKP	Zero Deviations	3	
6	SAFETY MANAGEMENT	12		
	Violation of Life saving rules	Zero Deviations	3	
	Provision of PPE	Zero Deviations	3	
	Monthly Man hours submission- safety stats	Zero Deviations	3	
	SHERQ audit	Zero Deviations	3	
		TOTAL IN PERCENTAGE	100.00	
	1. Unsatisfactory	2.Need Improvements	3.Meet Requirements	
	79% and Below	80%-89%	90% and Above	

31. ACCEPTANCE

This document has been seen and accepted by:

Name	Designation
Octavia Mohale	Risk and Assurance Manager
Robert Hlahu	Manager Security
Jeffrey Sibiya	Officer Security Investigation
Timothy Hlatshwayo	Officer Security Operation
Tessa Sibeko	GX Senior Advisor Security Operations

32. REVISIONS

Date	Rev.	Compiler	Remarks
January 2026	1	Thabo Ndlovu	Original.

33. DEVELOPMENT TEAM

N/A

34. ACKNOWLEDGEMENTS

N/A.

APPENDIX E: LOW SERVICE DAMAGE- SCHEDULE OF DEFICIENCY AND PENALTIES

Number	Low Service Damage Description	Value Of Low Service Damages	Value Of Low Service Damages	Limit of the low service damage
a	Delay in submission of documents as detailed in this agreement	1% of fixed monthly service or Task order value for an ad-hoc service	5% of monthly task order service value / task order value for ad-hoc service	Limited to 10% of monthly task order service value / task order value for ad-hoc service
b	No response of NCR/Early Warning/Letter within 2 days	1% of fixed monthly service or Task order value for an ad-hoc service	5% of monthly task order service value / task order value for ad-hoc service	Limited to 15% of monthly task order service value / task order value for ad-hoc service
c	More than 10 short posting per month	2.5% of fixed monthly service or Task order value for an ad-hoc service	Limited to 5% of monthly task order service value / task order value for ad-hoc service	Notification of default
d	Violation of Eskom Lifesaving Rule / policies and procedures	Permanent removal of Security officer from Eskom contract duties and one shift cost deduction	Issue Early Waring and NCR	Issue Early Waring and NCR
e	Refusal by Security officer to comply with lawful instruction	Permanent removal of Security officer from Eskom contract duties and one shift cost deduction	Unlimited	
f	Sleeping on duty	One shift cost deduction	Limited to two incidents per month	Issue Early Waring and NCR
g	Desertion of post	Permanent removal of Security officer from	Limited to one incident per month	Issue Early Waring and NCR

Number	Low Service Damage Description	Value Of Low Service Damages	Value Of Low Service Damages	Limit of the low service damage
		Eskom contract duties and one shift cost deduction		
h	Negligence by Security Officer in performance of duties	Permanent removal of Security officer from Eskom contract duties and one shift cost deduction	Unlimited	
I	Security officer without correct PPE/functional two-way radio/torch/body camera and not armed	1% of fixed monthly service or Task order value for an ad-hoc service	Limited to 5% of monthly task order service value / task order value for ad-hoc service	Issue Early Waring and NCR
j	Legal /Legislative contravention	100% of fixed monthly service or Task order value for an ad-hoc service & Issue Early Waring and NCR	Notification of default	Failure to rectify, the contract must be terminated
k	Loss suffered by the employer due to incidents emanating from contractor negligence/ wilful misconduct	100% deduction of the total cost of the loss value and NCR	Notification of default and NCR/Early Warning	Failure to rectify, the contract must be terminated
l	Non-payment of employee/s salaries	50% of fixed monthly service or Task order value for an ad-hoc service- Issue Notification of Default	Contract termination plus referral to Supplier review committee	
m	Failure to report / record incident	5% of fixed monthly service or Task order	Limited to 20% of monthly task order	Issue Early Warning and NCR

Number	Low Service Damage Description	Value Of Low Service Damages	Value Of Low Service Damages	Limit of the low service damage
		value for an ad-hoc service	service value / task order value for ad-hoc service	
n	Posting of untrained or registered Security Officers	Immediate removal plus 5% of fixed monthly service or Task order value for an ad-hoc service	Limited to 20% of monthly task order service value / task order value for ad-hoc service	Issue Early Warning and NCR
0	Security Officer's involvement in criminal activities	Immediate removal plus NCR/Early Warning with corrective plan- Report the officer to Psira and GX blacklisting database	Immediate removal plus NCR/Early Warning with corrective plan- Report the officer to Psira and GX blacklisting database	Unlimited