Eskom	Scope of Work	Grootvlei Power Station

Title: **Scope of Work for Grootvlei Power Station and Vaal dam Pump Station Outcome Based Contract**

Document Identifier: **GVL/0622**

Alternative Reference Number: **N/A**

Area of Applicability: **Grootvlei Power Station Security**

Functional Area: **Security**

Revision: **1**

Total Pages: **20**

Next Review Date: **N/A**

Disclosure Classification: **Controlled Disclosure**

Compiled	Supported by	Functional Responsibility	Authorized by
Mike Shange	Tessa Sibeko	Lebo Sebetoane	Ndondo Mabanne
Officer Security Ops	Senior Advisor GX Security	Security Manager	R&A Manager
Date: 15/10/2025	Date: 15.10.2025	Date: 15/10/2025	Date: 2025/10/17

Content

1. Introduction

Grootvlei Power Station and Vaal dam Pump Station are designated as a National Key Point in terms of the NKP Act 102 of 1980. The Key Point is regulated by National Key Point Act and other Legislatives to protect the infrastructure, information, assets and employees against any security threats. Grootvlei and Vaal dam requires security services to maintain a safe working environment. Grootvlei and Vaal dam in-house security is supplemented by a Security service provider for the protection of both NKP and Non NKP areas. These services should be rendered by trained security officers and accredited service provider in alignment with NKP act 102 of 1980, PSIRA Act 56 of 2001, Firearm and Ammunition Act of 2000 and SASSETA Act.

Vaal dam Pump Station supply water to Grootvlei Power Station to generate electricity since the commencement of Grootvlei. The Pump Station consists of a steel cement structure, where water pipelines are installed, and the pump house should be guarded 24/7.

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. 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. The technology that will be deployed on site will be Technology as a Service (TAS). The service provider will be required to roll out the technology as a service to Eskom Grootvlei Power Station and Vaal dam Pump station, and charge Eskom a monthly fee. The service fee should be reflected on the cost breakdown.

2. Supporting Clauses

2.1 Scope

This scope of work outlines the services needed to protect Eskom Grootvlei Power Station and Vaal dam Pump Station assets. The service provider will be required to conduct an assessment to identify physical risks and vulnerabilities and provide us with a comprehensive proposal for guarding and technology services.

2.1.1 Purpose

The purpose of this document is to procure outcome-based security contract that integrates advanced technology solutions with traditional security measures to protect Eskom Grootvlei Power Station and Vaal dam Pump Station through measurable performance outcomes. This will be a 60-months outcome-based contract. All equipment, technology, licenses and systems installed as part of this contract shall become the property of Eskom upon installation and must comply with Eskom technical standards as a minimum requirement, with higher specifications preferred where technically and commercially viable.

2.1.2 Applicability

This document is applicable to Security Department at Grootvlei Power Station.

2.1.3 Effective date

This document is effective as of the date of authorisation.

2.2 Normative/Informative References

2.2.1 Normative

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

2.2.2 Informative

[1] ISO 9001 Quality Management Systems

[2] ISO 18788: 2015 Management System for Private Security Operations

[3] Control of Access to Public Premises and Vehicles Act, No. 53, 1985

[4] Protection of Constitutional Democracy against Terrorists and Relative Activities, Act 33 of 2004

[5] Constitution of the Republic of South Africa, 1996

[6] Public Finance Management Act 1 of 1999

[7] Protection of Information Act 84 of 1982

[8] Prevention and Combating of Corrupt Activities Act 12 of 2004

[9] Labour Relations Act 66 of 1995

[10] Basic Conditions of Employment Act 75 of 1997

[11] Basic Conditions of Employment Act 75 of 1997: Sectoral Determination 6: Private Security Sector

[12] Occupational Health and Safety Act 85 of 1993

[13] Prevention of Organised Crime Act 121 of 1998

[14] Protected Disclosures Act 26 of 2000

[15] The Promotion of Access to Information Act 2 of 2000

[16] Critical Infrastructure Protection Act 8 of 2019

[17] National Key Points Act and Regulations, Act 102 of 1980

[18] National Key Points Directive, CS/OPS/NSP/P/329/1/B

[19] The Criminal Procedure Act 51 of 1977

[20] Firearms Control Act 60 of 2000

[21] National Strategic Intelligence Act 39 of 1994

[22] Eskom's Procurement and Supply Chain Management Policy 32-1033

[23] Private Security Industry Regulation Act and Regulations, Act 56 of 2001

[24] Private Security Industry Levies Act 23 of 2000

[25] Eskom's Procurement and Supply Chain Management Procedure 32-1034

[26] Integrated Risk Management Policy 32-86

[27] Safety, Health, Environment and Quality (SHEQ) Policy 32-727

[28] Eskom Incident Management Procedure 32-95

[29] Eskom Delegation of Authority Policy 240-62072907

[30] Employment Equity Act 55 of 1998

[31] The Eskom Code of Ethics 32-527

[32] Security Service Provider Code of Conduct (PSIRA)

[33] PFMA Reporting Procedure rev 2 32-92

[34] Protection of Personal Information Act 4 of 2013 (POPIA

[35] Performing Animal Protection Amendment Act (Act 4 of 2016).

[36] Eskom Framework for physical security guarding services.

[37] Implementation of Eskom Outcome Based Contracts Security Tender

[38] Security Vetting Policy 32-0122M

[39] Contractor Access Control Standard 32-0126M

[40] 559- 620181114 Eskom Body-worn camera standard

2.3 Definitions

Definition	Explanation
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.

Definition	Explanation
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.
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.
Private Security service provider	An entity or organisation which conducts or contracts security operations and whose business activity includes the provision of security services, either on its own behalf or on behalf of another such entity or organisation.
OBC	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
Guarding Service	The deployment of trained security personnel to protect people, assets, infrastructure and operations from security threats, unauthorised access, theft, vandalism, and other risk.

2.4 Abbreviations

Abbreviation	Explanation
BU	Business Unit
SSP	Security Service Provider
NKP	National Key Point
GX	Generation
OHS	Occupational Health and Safety
FCA	Firearms Control Act
SAPS	South African Police Services
PPE	Personal Protective Equipment
PSIRA	Private Security Industry Regulation Authority
SOW	Scope of Work
SASSETA	Safety and Security Sector Education Training Authority
SHEQ	Safety, Hygiene, Environmental and Quality
OBC	Outcome-Based Contract

CCTV	Closed Circuit Television
KPI	Key Performance Indicator
RFP	Request for Proposal
SSP	Security Solutions Physical
SACAA	South African Civil Aviation Authority
COIDA	Compensation for Occupational Injuries and Disease Act
PSIRA	Private Security Industry Regulation Act
ROI	Return On Investment
PAPAA	Professional Association of Proprietary Agencies and Authorities

2.5 Roles and Responsibilities

- Security Department shall compile the scope of work for the provision of security services for Special Operations (Tactical Response team and drone Surveillance) for a period of **60** months at Grootvlei Power and Vaal dam Pump Station.

2.6 Process for Monitoring

- Security department will ensure compliance to this document.

2.7 Related/Supporting Documents

N/A

3. Request for proposal

The successful bidder(s) will be required to provide the services considering the following **Risk levels** within Grootvlei and Vaal dam pump Station.

The scope covers three categories at Grootvlei Power Station.

Risk Level	**Tier Level**	**Sites**	**Minimum Security Requirements**

Level 1 (Low to medium risk)	**1**	**5 Buildings (Main building, medical centre, Stores, Visitor parking, old ash plant, coal stock yard, AWR, Reservoir dam**	Physical guarding, Panic buttons, body cameras Drone Technology monitoring and armed response
Level 2 (Medium to High risk)	**2**	**2** **AWR, Reservoir dam**	Drone Technology monitoring and armed response
Level 3 (High risk)	**3**	**17** **Plant areas**	Physical guarding, Panic buttons, body cameras

Table 1: Risk Level Classifications

3.1 Legislative and Regulatory Framework

3.1.1 National Key Points Act Compliance

As a designated National Key Point under the National Key Points Act 102 of 1980, Grootvlei Power Station is subject to stringent regulatory requirements that mandate comprehensive protection of strategic infrastructure. The Act empowers the Minister of Police to declare and protect sites of national strategic importance against sabotage, espionage, and other threats that could compromise national security or economic stability. This designation places a specific obligation on Eskom as the facility owner, including the implementation of approved security measures, maintenance of occurrence books for incident recording, and immediate notification of security breaches to relevant protecting authorities.

The National Key Points framework requires that all security measures implemented at Grootvlei and Vaal dam Pump Station must align with prescribed standards for perimeter protection, access control, surveillance systems, and personnel vetting procedures. Non-compliance with these requirements can result in severe legal consequences, including prosecution under national security

legislation. Furthermore, the Act mandates that security upgrades and modifications must receive prior approval from designated authorities, ensuring that proposed solutions meet national security standards while maintaining operational effectiveness

3.1.2 PSIRA Regulatory Compliance

All security service providers contracted to operate at Grootvlei and Vaal dam Pump Station must demonstrate full compliance with the Private Security Industry Regulation Act 56 of 2001. This legislation establishes the Private Security Industry Regulatory Authority (PSIRA) as the governing body responsible for regulating all aspects of private security operations in South Africa. Compliance requirements include company registration, individual licensing of security personnel, adherence to prescribed training standards, and maintenance of operational records that meet regulatory specifications.

PSIRA compliance extends beyond basic registration to encompass ongoing obligations for skills development, equipment certification, and operational auditing. Security technology providers must demonstrate that their personnel possess appropriate qualifications for handling sophisticated security systems, including biometric technologies, integrated surveillance platforms, and access control networks. Additionally, any firearms or specialised security equipment deployed at the facility must be properly licensed and registered in accordance with PSIRA regulations and related firearms legislation.

The regulatory framework also mandates that security service providers maintain comprehensive insurance coverage, establish formal complaints procedures, and participate in industry oversight mechanisms. These requirements ensure that service providers operate within legal parameters while maintaining professional standards that align with the critical nature of National Key Point protection

Data Protection and Privacy

All system components must comply with the Protection of Personal Information Act (POPIA), incorporating appropriate data encryption, access controls, and retention policies, Biometric data.

3.2 GENERAL PROVISIONS

3.2.1 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.

3.3 CORE SERVICE REQUIREMENTS

3.3.1 Personnel Deployment Structure

Primary Security Teams:

- 22 security personnel per shift (including Grade B supervisor).
- Total deployment: 44 personnel covering day/night shifts.
- Additional provision for NDO (Normal Day Off) coverage ensuring continuous 24/7 operations.

Ad-hoc security-related services required which may be requested for a specific task and any period at any given time which includes:

- Tactical/Armed Response X 20 Grade C and 1 x supervisor Grade "B"
- Static guarding (Outages) x 20 Grade "C"
- Mobile Cameras X 05

The service will be required on a, as and when required basis, as per the identified security threat condition. A 12-to-48- hour notice to the Security service provider will be given, to ensure the availability of sufficient armed Response team. Requests be made by the duly appointed Service Manager.

A plant orientation will be conducted once the induction and access authorization processes have been completed.

3.3.2 Tactical Armed Response Officer Minimum Requirements (as and when required service):

- A Shift Supervisor Grade B minimum with Armed Response Training
- Armed Tactical security officers Grade C with Armed response Training.

- Grade C armed Tactical security officers shall be physically and mentally fit to perform the nature of duties as detailed in site specific scope of work, determined by changing risks and/or business requirements.

- Armed Tactical security officers shall have training and expertise in the use of specialized tactical equipment for crowd control.
- Armed Tactical Officer must respond with urgency to security breaches, perimeter /crowd control, containment and command of other serious incidents that threaten the safety and security of the NKP and Non NKP areas.
- Armed Tactical Security officers must have completed SASSETA business purpose training on the specific firearms, they are expected to use (handgun/Shotgun) 12 Br shotguns with rubber bullets for crowd control.
- Armed tactical security officers must possess valid firearm competency certificates for business purposes issued by SAPS, TRT and should have undergone Regulation 21 training for the contracting period for the starting year & annually thereafter. Proof of training will be required before commencement of the duties.

  The Service provider must ensure that all the employees or work force have the relevant tactical Response and Special Operation uniform or gear (i.e. protective shields, bottom sticks, etc.

Specialised Personnel:

- 1x Security Site Manager (Grade A, NKP qualified, valid driver's license).
- 1x Full-time Safety Officer (safety file management, audit participation, compliance oversight).
- 4x Drone Pilot Operators (2 per shift). Additional provision for NDO (Normal Day Off) coverage ensuring continuous 24/7 operations. Total deployment: 4x personnel covering day/night shifts.
- Two 2 X double cab vehicles (with 8 reaction officers 4 x day and 4 x night, this will be in addition to drone pilots per shift) conforming to Eskom vehicle specifications.

3.4 Operational Duties and Responsibilities

Core Security Functions:

- Continuous monitoring and protection of critical infrastructure.
- Proactive patrolling of vulnerable assets and plant critical areas.
- Detection, deterrence, and response to criminal activities including:
    - Prevent Plant tampering and vandalism.
    - Unauthorized access attempts to restricted buildings/ areas.
    - Prevent Copper cable theft and asset removal.
    - Prevent Security breaches and industrial action threats.

- Armed escort services for personnel in high-risk situations.
- Immediate tactical response to security incidents.
- Comprehensive incident documentation and reporting.

3.5 Incident Management

- All incidents and response to incidents must be handled according to the relevant Grootvlei and Vaal dam Pump Station Security SOP and/or work instructions.
- All incidents and response must be immediately reported to the Chief Security Officer and Eskom operating control room.
- The SAPS must be contacted immediately only for criminal or suspected ongoing criminal activities.
- Weekly status reports are to be supplied by the contractor.
- The Contractor 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.

All SHEQ incidents should be reported within 24 hours (Flash report). Preliminary Investigation must be conducted within 07 days and the final incident investigation report must be provided within 14 days from the date of occurrence.

3.5.1 Advanced Security Operations:

- High-risk tactical response deployment within 5 minutes.
- Life-threatening situation intervention capabilities.
- Team mobilisation for emergency situations.
- Video recording / and digital documentation of all tactical responses.
- Asset protection until threat neutralisation.

3.6 Electronic Security Registers

The service provider to propose a suitable electronic register to transition from traditional paper-based to digitalized register at Grootvlei and Vaal dam Pump Station. The system must ensure that records are retained for a minimum of 12 months, readily retrievable for inspection, and readily available to Eskom at any given time.

Register / Document	Traditional Paper Requirement	Electronic Register Equivalent	Key Features / Controls
Posting Sheets	Printed duty rosters for guard posting	Digital duty roster (accessible on mobile or PC)	Real-time updates, role assignments, shift reminders, exportable reports
Patrol Reports	Handwritten patrol notes	Mobile patrol logging app (QR, NFC, GPS checkpoints)	Auto timestamp, proof of presence, exception alerts
Firearm Handover / Takeover Register	Signed handover logbook	Digital firearm management system	Weapon ID scan, officer ID, supervisor e-signature, audit trail
Firearm Permits	Paper permits issued & filed	Electronic firearm permit system	Digital storage of permits, searchable by officer/serial number
Firearm Incident Register	Manual log after discharge	Incident reporting module	Incident capture with notes, photo/video evidence, automatic report submission
Weekly / Monthly Inspection Registers	Signed inspection sheets	Digital inspection checklists	Auto reminders, photo evidence upload, compliance tracking
Monthly Safety Inspection Register	Manual monthly entries	Safety audit form in system	Checklist-driven, digital signatures, dashboard compliance %
Pocket Book	Guard's personal notebook	Guard app digital pocketbook	Notes, incidents, photos, all timestamped & stored centrally
Inspection Reports (Weekly & Monthly)	Written reports filed	Auto-generated digital reports	Exportable to PDF/Excel, trend analytics
Safe Key Report	Manual safe key issue/return	Digital key management log	Records issue/return times, user PIN/biometric, alerts for overdue returns

Firearm Daily Permit Issuing Register	Daily paper permits	Daily digital permits	Easy tracking by officer, date, firearm ID
Occurrence Book (OB)	Bonded OB with shift logs, patrols, incidents	Electronic Occurrence Book	Shift sign-in/out, patrol logging, incident recording, supervisor visits (e-signed), tamper-proof audit trail

Table 2: Electronic Register requirements

3.7 AERIAL SURVEILLANCE OPERATIONS

3.7.1 Legal and Regulatory Compliance

All drone operations must comply with:

- South African Civil Aviation Authority (SACAA) regulations.
- Remote Pilot License (RPL) requirements for all operators.
- Aircraft registration and operational certificates.
- Third-party liability insurance (minimum R2 million coverage).
- Visual Line of Sight (VLOS) operational parameters.
- Restricted airspace compliance (military installations, schools, public areas).
- Flight altitude restrictions (maximum as per SACAA guidelines).

3.7.2 Drone Specifications and Requirements

- Maximum weight: 7kg (unless special permits obtained).
- Night vision capabilities (thermal and infrared technology).
- High-definition recording capabilities.
- GPS tracking and flight logging systems.
- Weather-resistant operational capability.
- Minimum 2-hour continuous flight time.
- Real-time video transmission to control room.

3.7.3 Operational Parameters

Non NKP Coverage Areas (5km radius from Grootvlei Power Station):

- Complete power station infrastructure.

- Ash Dam
- Reservoir dam
- Coal Rail Terminal and AWR substation.
- Cable infrastructure
- Perimeter fencing and access points.
- All dam facilities and reclamation areas.
- Ash pipelines and monitoring systems.

Operational Schedule:

- Night operations: 8-10 hours maximum flight time.
- Day operations: 1-8 hours as required.
- Emergency callout services available 24/7.
- Mandatory rest periods for equipment and operators.

3.7.4 Pilot Qualifications and Requirements

- Valid SACAA Remote Operator Certificate.
- Clean criminal record with disclosure requirements.
- English language proficiency.
- Secrecy declaration agreement.
- Security screening clearance.
- Site-specific SOP training.
- Eskom safety induction completion.

3.8 Panic buttons

Panic Button shall be provided on each site where security officers are deployed to enable a quick response to any emergency.

3.9 Body cameras

Body cameras (HD Video Recording, water resistance and dust resistance body cameras with docking system) supplied by contractor to be issued to each security officer on duty which should be 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.

3.10 Guard patrol monitoring system

Service provider to provide guard monitoring system to monitor guards patrolling routine and frequency. The system must be installed as per par. 2 scoped areas & monitored in the Eskom security control room. The system must be 100% functional & available at all times & capable to generate a report to be submitted to the Security Manager on a weekly basis.

3.11 FIREARMS AND ARMAMENT

They security should be equipped with the following:

- Rifles
- Shotguns (12 Bore)
- 9MM
- **All firearms must be company-licensed (revolvers specifically excluded).**

3.11.1 Firearm Control Act Compliance

- Company firearm licenses (5-year validity).
- Designated responsible person/armoury manager appointment.
- Competency certificates for all armed personnel.
- SASSETA accredited training completion.
- Regulation 79 annual compliance training.
- Safe handling procedures and equipment.
- SABS approved firearm storage facilities.
- Daily permit systems for deployed firearms.

3.12 VEHICLE AND TRANSPORTATION REQUIREMENTS

3.12.1 Vehicle Specifications

- 2x 4x4 LDV Double Cab patrol vehicles.
- SABS approved seatbelt installation.

- Searchlight equipment on each vehicle.
- GPS tracking/vehicle monitoring systems.
- Monthly mileage limit: 6,000km per vehicle (including fuel runs).

3.12.2 Driver Requirements

- Valid driver's licenses for all operators.
- Accredited defensive driving course completion.
- Driver risk profile assessments.
- Regular vehicle maintenance and safety inspections.

3.13 COMMUNICATION SYSTEMS

3.13.1 Communication Infrastructure

Service provider must establish continuous communication through:

- Handheld radio systems.
- Satellite communication backup.
- Contracted cellular devices.
- Base radio stations.
- Push-to-talk (PTT) systems.
- Integration with Eskom control room communications.

3.14 Three Phase Response Plan Integration

The security framework incorporates a comprehensive Three Phase Response Plan that ensures coordinated human-technology integration across all security tiers:

3.14.1 Primary Response Action Plan (Plan and Prepare)

- Competent personnel deployment with tier-appropriate training and security clearance levels.
- Continuous threat assessment and vulnerability analysis specific to each zone's risk profile.
- Equipment readiness and communication system verification across all integrated platforms.

- Community engagement and intelligence gathering protocols for external threat assessment.

3.14.2 Secondary Response Action Plan (Respond)

- Coordinated response using technology-human integration aligned with tier-specific escalation procedures.
- Real-time communication and backup deployment coordinated through the central PSIM platform.
- Evidence preservation and incident documentation with automated chain of custody protocols.
- Tactical response protocols matched to threat levels and zone criticality classifications.

3.14.3 Tertiary Response Action Plan (Recovery)

- Post-incident investigation and forensic analysis with tier-appropriate investigation depth.
- System performance evaluation and improvement identification across all security zones.
- Personnel support and trauma management for security officers involved in incident response.
- Lessons learned integration and procedure updates to enhance future response effectiveness.

3.15 ADDITIONAL SCOPE ELEMENTS

3.15.1 Emergency Preparedness and Business Continuity

- Comprehensive emergency response procedures.
- Alternative communication protocols during system failures.
- Backup equipment and personnel deployment strategies.
- Natural disaster and extreme weather response plans.
- Cyber security incident response protocols.
- Medical emergency response capabilities.

3.15.2 Environmental and Sustainability Considerations

- Environmental impact assessment for all operations.

- Waste management protocols for operational materials.
- Fuel efficiency monitoring and reporting.
- Carbon footprint reduction initiatives.
- Sustainable equipment replacement programs.

3.15.3 Quality Assurance and Continuous Improvement

- Monthly performance review meetings.
- Quarterly security assessments and gap analyses.
- Annual contract review and optimization sessions.
- Continuous training program development.
- Best practice implementation from industry standards.
- Regular benchmarking against security industry standards.

3.15.4 Stakeholder Engagement and Communication

- Regular briefings with Eskom management.
- Community liaison and engagement protocols.
- Coordination with local law enforcement agencies.
- Integration with emergency services (fire, medical, police).
- Regulatory body communication and compliance reporting.

3.16 CONTRACTUAL AND ADMINISTRATIVE REQUIREMENTS

3.16.1 Documentation Package (Pre-Contract)

All documentation must be submitted 14 days before task order issuance:

- Complete personnel database with certifications.
- Equipment inventory and maintenance records.
- Insurance certificates and coverage verification.
- Legal compliance documentation.
- Risk assessments and mitigation strategies.
- Standard Operating Procedures (SOPs)
- Emergency contact directories

3.16.2 Ongoing Administrative Obligations

- Monthly personnel deployment schedules.
- Weekly status and performance reports.
- Quarterly compliance audits.
- Annual contract performance reviews.
- Continuous legal and regulatory compliance monitoring.

3.16.3 Payment and Compensation Structure

- Fixed monthly payments covering all services and equipment.
- Performance-based adjustments according to KPI achievements.
- No additional charges for equipment, fuel, maintenance, or operational costs.
- Sectorial Determination minimum wage compliance.
- Employee benefit provision (UIF, COID, provident fund).

3.17 PENALTIES AND REMEDIES

3.17.1 Performance Penalties

- KPI-based financial penalties as specified above.
- Equipment failure penalties: 5% monthly reduction for each critical system failure.
- Compliance violations: 10% monthly reduction for regulatory breaches.
- Personnel shortfalls: 3% daily reduction for each unfilled position.

3.17.2 Remedial Actions

- Corrective action plans for performance deficiencies.
- Personnel replacement requirements for non-compliance.
- Training enhancement programs for skill gaps.

3.18 CONTRACT TERMINATION AND TRANSITION

3.18.1 Termination Conditions

- Material breach of contract terms.
- Failure to meet critical KPI thresholds for consecutive months.

- Loss of essential licenses or certifications.
- Serious safety or security incidents due to negligence including accidental discharges.

3.18.2 Transition Requirements

- 60-day notice period for contract termination.
- Comprehensive handover documentation.
- Personnel and equipment transition protocols.
- Knowledge transfer and training for replacement services.
- Asset return and condition assessments.

3.19 KEY PERFORMANCE INDICATORS (KPIs)

KPI 1: Response Time Performance

- Target: 95% of security incidents responded to within 5 minutes.
- Measurement: Time from incident report to security team arrival.
- Penalty: 2% monthly fee reduction for each percentage point below target.

KPI 2: Equipment Availability and Readiness

- Target: 98% operational availability of all security equipment (vehicles, drones, communications, firearms).
- Measurement: Monthly equipment audit and availability reports.
- Penalty: 1% monthly fee reduction for each percentage point below target.

KPI 3: Training and Compliance Standards

- Target: 100% compliance with mandatory training, certifications, and legal requirements.
- Measurement: Monthly compliance audits and documentation reviews.
- Penalty: 3% monthly fee reduction for non-compliance incidents.

KPI 4: Incident Detection and Prevention

- Target: 90% reduction in security incidents within patrolled areas compared to baseline.
- Measurement: Monthly incident reports and trend analysis.
- Penalty: 3% monthly fee reduction for non-compliance to detecting and preventing incidents.

KPI 5: Documentation and Reporting Accuracy

- Target: 100% accurate and timely submission of all required reports and documentation.
- Measurement: Weekly report quality assessments and timeliness tracking.
- Penalty: 1.5% monthly fee reduction for reporting deficiencies.

KPI 6: Personnel Reliability and Attendance

- Target: 99% shift coverage with qualified personnel (no gaps in security coverage).
- Measurement: Daily shift reports and attendance monitoring.
- Penalty: 2.5% monthly fee reduction for coverage gaps.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Ndondo Mabanne	Risk & Assurance Manager

5. Revisions

Date	Rev.	Compiler	Reason for change
October 2030	1	Mike Shange	N/A

6. Development Team

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

- Matsobane Phosa
- Tessa Sibeko
- Mike Shange
- Lebo Sebetoane

7. Acknowledgements

- None

8. Appendix

None