

	Request for Proposal	KZNOU
-----------------------------------------------------------------------------------	-----------------------------	--------------

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

Document Identifier:

Alternative Reference Number: **N/A**

Area of Applicability: **KZNOU**

Functional Area: **Security**

Revision: **1**

Total Pages: **31**

Next Review Date: **N/A**

Disclosure Classification: **Controlled Disclosure**

Content

	Page
1. Introduction.....	4
2. Supporting Clauses	4
2.1 Scope.....	4
2.1.1 Purpose.....	4
2.1.2 Applicability	4
2.1.3 Effective date.....	4
2.2 Normative/Informative References	4
2.2.1 Normative.....	5
2.2.2 Informative.....	5
2.3 Definitions	5
2.4 Abbreviations	5
2.5 Roles and Responsibilities	6
2.6 Process for Monitoring.....	6
2.7 Related/Supporting Documents.....	6
3. Request for proposal	Error! Bookmark not defined.
3.1 Contract Duration	7
3.2 Scope of Work.....	19
3.2.1 Physical Security Services.....	19
3.2.2 Technology Integration Services (Baseline) linked to control room	20
3.2.3 Maintenance and Support.....	20
3.2.4 Technology Roadmap	21
3.2.5 Community Involvement	21
3.2.6 Handover Phase (At Contract End or Termination):.....	22
3.3 Key performance indicators (KPI'S).....	23
3.4 Site evaluations	27
3.5 Annual rates	27
3.6 Terms of payment for monthly invoices	28
4. Acceptance.....	Error! Bookmark not defined.
5. Revisions.....	Error! Bookmark not defined.
6. Development Team	Error! Bookmark not defined.
7. Acknowledgements(if applicable).....	Error! Bookmark not defined.

TABLE

Table 1: Pietermaritzburg Zone substations/Area offices/offices and network infrastructure (268 sites) 10

Table 2:Empangeni Zone substations/Area offices/offices and network infrastructure (148 sites) 13

Table 3: Newcastle Zone substations/Area offices/offices and network infrastructure (188 sites).. 16

CONTROLLED DISCLOSURE

Table 4: Primary KPIs 23

Table 5: Secondary KPIs 25

Table 6: Innovation and Improvement KPIs..... 26

1. Introduction

Eskom Holdings SOC Ltd invites qualified and experienced service providers to submit proposals for the provision of Outcome-Based Physical Guarding Services and technology solutions at Eskom facilities in the KWAZULU NATAL OPERATING UNIT ZONES. The aim is to enhance security outcomes through the integration of advanced technology, innovation, and measurable performance metrics. The contract will focus on delivering physical guarding services, technology-driven solutions, and continuous improvement to ensure the safety and protection of Eskom's assets, personnel, and operations.

This contract will include a Technology as a Service (TAAS). The successful service provider will have to maintain the installed system and train all the relevant stakeholders on the installed security system equipment.

2. Supporting Clauses

2.1 Scope

2.1.1 Purpose

To procure outcome-based physical guarding services that integrate advanced technology solutions with traditional security measures to protect Eskom facilities in the KwaZulu Natal Operating Unit Zones through measurable performance outcomes. This is a five (5) year contract with payments distributed equally over the contract period. All equipment, technology, and systems installed as part of this contract shall become the property of Eskom upon installation but transferred at the end of the contract at zero cost and must comply with Eskom technical standards as a minimum requirement, with higher specifications preferred where technically and commercially viable. The tenderer/bidder may submit proposals for multiple zones; however, successful bidders will be permitted to operate in a multiple zones.

2.1.2 Applicability

This document shall apply to KwaZulu Natal Operating Unit Zones.

2.1.3 Effective date

This document is effective from the date of signature.

2.2 Normative/Informative References

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

CONTROLLED DISCLOSURE

2.2.1 Normative

- [1] ISO 9001 Quality Management Systems
- [2] 240-102220945 Specification for Integrated Access Control System for Eskom sites
- [3] 240-91190304 Specification for CCTV Surveillance with Intruder Detection
- [4] 240-86738968 Specification for Integrated Security Alarm System for Protection of Eskom Installations and its subsidiaries
- [5] 240-170000096 Physical security integration standard
- [6] 240-170000257 Technical Evaluation Criteria for the Integrated Security System
- [7] 240-170000691 Standard for Intrusion pre-detection systems used at Eskom sites
- [8] 240-78980848 Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom installations and its subsidiaries
- [9] 240-171000171 Commissioning guideline for secondary plant physical security system
- [10] 240-180100001 Secondary Plant Security Systems Maintenance Procedure

2.2.2 Informative

- [11] N/A

2.3 Definitions

Definition	Explanation
Tender	Refers to an open or closed competitive request for quotations / prices against a clearly defined scope / specification.
Integrated Access Control System	It is an electronic system that aims to collaborate and align efforts across the logical and physical security domains to standardise access control within Eskom.
Control Centre	Where alarms and CCTV footage are monitored and needed response/s initiated from. The alarms and CCTV footage can be aggregated to a national security control centre that can initiate requisite actions from a national perspective.

2.4 Abbreviations

Abbreviation	Explanation
OBC	Outcome-Based Contract
CCTV	Closed Circuit Television

CONTROLLED DISCLOSURE

Abbreviation	Explanation
KPI	Key Performance Indicator
RFP	Request for Proposal
SSP	Security Solutions Physical

2.5 Roles and Responsibilities

- a) The team shall utilise the latest revision of this document.
- b) Control room establishment is open to any bidder to set up a centralised control room where all sites' video feeds and alarms are going to be linked and ensure that all alarms and video feeds are linked.
- c) The successful bidders for Pietermaritzburg, Empangeni and New Castle zones will be responsible to link video feeds and alarms to the centralised control room.
- d) Eskom security team to coordinate the project and ensure alignment with the roll out plan.

2.6 Process for Monitoring

N/A

2.7 Related/Supporting Documents

559-348635181 OBC Guidelines.

3. The successful bidder(s) will be required to provide comprehensive security services across three KwaZulu-Natal Operating Unit Zones, covering 604 facilities. Services must be tailored to four distinct risk tiers, each with unique threat profiles and operational challenges.

Tier 1: National Key Points / High-Risk Critical Infrastructure

- **Sites:** Power stations, key substations, national control centres, Regional Distribution Centres (RDCs)
- **Threat Profile:** Organized crime syndicates, sophisticated external attacks, insider threats
- **Operational Challenge:**
 - Continuous 24/7 protection
 - Maximum security protocols
 - Zero tolerance for service disruption

CONTROLLED DISCLOSURE

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

- **Sites:** Distribution substations, Customer Network Centres (CNCs), regional offices, warehouses, walk-in centres, training centres
- **Threat Profile:** Copper theft syndicates, equipment vandalism, opportunistic crime
- **Operational Challenge:**
 - Effective security coverage
 - Cost optimization without compromising safety
 - Scalable response strategies

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

- **Sites:** Mini substations, customer hubs, secondary facilities
- **Threat Profile:** Opportunistic theft, minor vandalism, trespassing
- **Operational Challenge:**
 - Basic security measures
 - High cost-efficiency
 - Preventive deterrence

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

- **Sites:** Vacant properties, remote mini-substations, low-value storage units
- **Threat Profile:** Trespassing, minor vandalism, environmental hazards
- **Operational Challenge:**
 - Remote monitoring solutions
 - Minimal physical presence
 - Budget-conscious surveillance

3.1 Contract Duration

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

Technology Implementation: 90 days from contract award.

Performance review meeting: For the purposes of reviewing contract performance and operational demands, review meetings shall be conducted when requested by the service manager/end user.

CONTROLLED DISCLOSURE

Termination due to poor performance: Service manager/end user has the right to issue warning letter or to terminate contract if there is persistent poor performance resulting from three consecutive months of service failure condition being recorded. If termination is exercised under this condition, contractor shall be issued with three months' notice.

Surges and emergencies: Contractor shall be obliged to support surge and contingency operations demand as define by service manager.

Support Obligations

The Contractor shall be obliged to support surge and contingency operations as defined and directed by the Service Manager. Such obligations include, but are not limited to, the provision of additional personnel, equipment, and resources necessary to respond effectively to unplanned increases in demand or emergency circumstances.

Definition of Surges

For purposes of this RFP, a surge shall mean any sudden or temporary increase in the required level of services beyond the normal operational baseline. Surges may arise due to, inter alia:

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

Definition of Emergencies

An **emergency** shall mean any unforeseen or urgent circumstance which, in the reasonable opinion of the Service Manager, requires immediate deployment of Contractor's resources to safeguard life, property, or critical infrastructure. Emergencies may include, but are not limited to:

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

Response Times and Flexibility

The Contractor shall ensure availability of a standby team capable of rapid deployment

CONTROLLED DISCLOSURE

within a reasonable response time, not exceeding the period prescribed in the Service Level Agreement. The Contractor shall maintain operational flexibility to upscale service levels, redeploy personnel, or extend working hours as may be required.

Compensation and Cost Recovery

All surge and emergency support services shall be rendered in accordance with the agreed pricing structure for contingency operations. Where additional costs are reasonably and necessarily incurred by the Contractor, such costs shall be recoverable upon submission of verifiable supporting documentation and subject to the prior approval of the Service Manager.

Incentive for Performance: Each substation that is fully equipped with systems and successfully integrated with the control room will qualify for a once-off bonus equivalent to ten percent (10%) of the substation's invoice value, calculated prior to the installation of any alarm or CCTV systems.

Scope and Risk Levels

The scope of this engagement covers all three zones within the KwaZulu-Natal Operating Unit facilities, categorized by their risk levels and corresponding minimum-security requirements as detailed below:

CONTROLLED DISCLOSURE

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

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 4	63 substations	<p>Outcome: Deter casual intrusion and enable rapid incident verification.</p> <p>Integrated Video Alarms: Motion or perimeter breach detection with immediate video verification capabilities.</p> <p>24/7 Remote Monitoring: Centralized monitoring of alarms and video feeds.</p> <p>Tiered Armed Response: Pre-arranged rapid armed response services triggered by verified alarms, with defined Service Level Agreements (SLAs). As and when required.</p>
Tier 2	<p>3 Area offices</p> <p>1 Warehouse</p> <p>2 Training Centres</p> <p>16 Customer Network Centres</p> <p>10 Walk in Centres</p>	<p>Outcome: Prevent unauthorized access, detect and deter criminal activity, and enable swift, coordinated response.</p> <p>Comprehensive CCTV Surveillance: High-definition cameras with analytical capabilities (e.g., motion, loitering) covering critical areas.</p> <p>Advanced Integrated Alarm Systems: Multi-layered sensors (e.g., perimeter, vibration, volumetric) linked to the CCTV and access control.</p> <p>Integrated Access Control: Card/biometric access for all entry/exit points, with audit trails and remote management capabilities.</p> <p>24/7 Centralized Monitoring: Dedicated control room operators for continuous oversight, alarm management, and dispatch.</p> <p>Rapid Armed Response: Priority armed response with shorter SLAs, pre-identified routes, and site familiarization.</p>

CONTROLLED DISCLOSURE

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
	119 Substation 1 Control Centre 17 Radio Site	On-site Deterrence: Visible, uniformed Security Guards (C-grade, ideally armed or with clear escalation protocols to armed response) for access control and initial visual deterrence during vulnerable periods (e.g., peak crime times, specific operational windows). Their primary role is access management and observation, relying on technology and armed response for engagement. As and when required.
Tier 3	36 Substations	Outcome: Maximize prevention of sophisticated attacks, ensure immediate detection, and enable overwhelming response to protect critical assets. AI-Powered Advanced Surveillance: High-definition cameras with AI analytics for anomaly detection, facial recognition (where permissible), object tracking, and predictive analysis, integrated with a Public Address (PA) system for audio warnings. Multi-Layered Perimeter Défense: Advanced sensors (e.g., fibre optic fence, ground radar, thermal imaging) coupled with physical hardening measures. Robust Integrated Access Control: Biometric systems, anti-pass back, and visitor management. 24/7 Dedicated Monitoring & Intelligence: Proactive monitoring by highly trained operators, leveraging security business intelligence feeds for pre-emptive actions. Immediate Armed Response: Direct armed response deployment with the shortest possible SLAs, possibly including dedicated on-call teams or co-location agreements.

CONTROLLED DISCLOSURE

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
		<p>Highly Trained On-site Security Guards (Armed Recommended): Visible, well-trained and armed security personnel (or highly trained unarmed guards supported by immediate armed response presence) to provide a robust physical barrier, rapid initial response, and coordination with external armed response. Patrols should be intelligence driven. As and when required.</p>
<p>Network Infrastructure</p> <p>Tier 3&4</p>	<p>All Feeder Lines, Pole Mounted Transformers, Reclosers, lines in operation and lines not in operation linked to substations</p>	<p>Outcome: Detect and deter widespread opportunistic theft and vandalism across distributed assets, enabling targeted intervention.</p> <p>Targeted Drone Surveillance: Regular or on-demand drone patrols with high-resolution and thermal imaging to identify suspicious activity or damage along lines and at remote assets.</p> <p>IoT/Smart Sensor Deployment: Intelligent sensors on high-value pole-mounted transformers and reclosers to detect tampering, removal, or unusual activity, providing real-time alerts.</p> <p>GPS Tracking & Asset Tagging: For portable or high-value components. Proactive Remote Monitoring: Alerts from sensors and drone feeds are centralized for analysis and dispatch.</p> <p>Mobile Armed Response: Dedicated mobile armed response teams covering specific geographic clusters, dispatched based on alerts, and utilizing intelligence-led patrols.</p> <p>Community Engagement & Whistleblower Programs: Encouraging public reporting of suspicious activity.</p> <p>As and when required</p>

CONTROLLED DISCLOSURE

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

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 4	32 Substations	<p>Outcome: Deter casual intrusion and enable rapid incident verification.</p> <p>Integrated Video Alarms: Motion or perimeter breach detection with immediate video verification capabilities.</p> <p>24/7 Remote Monitoring: Centralized monitoring of alarms and video feeds.</p> <p>Tiered Armed Response: Pre-arranged rapid armed response services triggered by verified alarms, with defined Service Level Agreements (SLAs).</p> <p>As and when required.</p>
Tier 2	<p>1 area Office</p> <p>1 Empangeni Warehouse</p> <p>56 Substations</p> <p>18 Network Centre</p> <p>6 Hubs</p>	<p>Outcome: Prevent unauthorized access, detect and deter criminal activity, and enable swift, coordinated response.</p> <p>Comprehensive CCTV Surveillance: High-definition cameras with analytical capabilities (e.g., motion, loitering) covering critical areas. Advanced Integrated Alarm Systems: Multi-layered sensors (e.g., perimeter, vibration, volumetric) linked to the CCTV and access control.</p> <p>Integrated Access Control: Card/biometric access for all entry/exit points, with audit trails and remote management capabilities.</p> <p>24/7 Centralized Monitoring: Dedicated control room operators for continuous oversight, alarm management, and dispatch.</p> <p>Rapid Armed Response: Priority armed response with shorter SLAs, pre-identified routes, and site familiarization.</p>

CONTROLLED DISCLOSURE

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
	6 Radio Site	<p>On-site Deterrence: Visible, uniformed Security Guards (C-grade, ideally armed or with clear escalation protocols to armed response) for access control and initial visual deterrence during vulnerable periods (e.g., peak crime times, specific operational windows). Their primary role is access management and observation, relying on technology and armed response for engagement.</p> <p>As and when required</p>
Tier 3	28 Substations	<p>Outcome: Maximize prevention of sophisticated attacks, ensure immediate detection, and enable overwhelming response to protect critical assets.</p> <p>AI-Powered Advanced Surveillance: High-definition cameras with AI analytics for anomaly detection, facial recognition (where permissible), object tracking, and predictive analysis, integrated with a Public Address (PA) system for audio warnings.</p> <p>Multi-Layered Perimeter Défense: Advanced sensors (e.g., fibre optic fence, ground radar, thermal imaging) coupled with physical hardening measures.</p> <p>Robust Integrated Access Control: Biometric systems, anti-pass back, and visitor management.</p> <p>24/7 Dedicated Monitoring & Intelligence: Proactive monitoring by highly trained operators, leveraging security business intelligence feeds for pre-emptive actions.</p> <p>Immediate Armed Response: Direct armed response deployment with the shortest possible SLAs, possibly including dedicated on-call teams or co-location agreements.</p> <p>Highly Trained On-site Security Guards (Armed Recommended): Visible, well-trained and armed security personnel (or highly trained unarmed guards supported by immediate armed response presence) to provide a robust physical barrier, rapid initial response, and coordination with external armed response. Patrols should be intelligence driven. As and when required.</p>

CONTROLLED DISCLOSURE

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

CONTROLLED DISCLOSURE

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

Risk Level	Sites (Count & Type)	Minimum Security Requirements (Outcomes-Based)
Tier 4	71 Substations	<p>Outcome: Deter casual intrusion and enable rapid incident verification.</p> <p>Integrated Video Alarms: Motion or perimeter breach detection with immediate video verification capabilities.</p> <p>24/7 Remote Monitoring: Centralized monitoring of alarms and video feeds.</p> <p>Tiered Armed Response: Pre-arranged rapid armed response services triggered by verified alarms, with defined Service Level Agreements (SLAs).</p> <p>As and when required</p>
Tier 2	<p>2 Area Offices</p> <p>1 Vryheid Warehouse</p> <p>79 Substations</p> <p>11 Control Network Centre</p> <p>7 Radio Site</p>	<p>Outcome: Prevent unauthorized access, detect and deter criminal activity, and enable swift, coordinated response.</p> <p>Comprehensive CCTV Surveillance: High-definition cameras with analytical capabilities (e.g., motion, loitering) covering critical areas. Advanced Integrated Alarm Systems: Multi-layered sensors (e.g., perimeter, vibration, volumetric) linked to the CCTV and access control.</p> <p>Integrated Access Control: Card/biometric access for all entry/exit points, with audit trails and remote management capabilities.</p> <p>24/7 Centralized Monitoring: Dedicated control room operators for continuous oversight, alarm management, and dispatch.</p> <p>Rapid Armed Response: Priority armed response with shorter SLAs, pre-identified routes, and site familiarization.</p>

CONTROLLED DISCLOSURE

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

CONTROLLED DISCLOSURE

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

CONTROLLED DISCLOSURE

3.2 Scope of Work

3.2.1 Physical Security Services

- **Guard Deployment:** Provide trained, PSIRA-registered security personnel of the required grade as per site-specific risk assessments. Ensure optimal staffing levels for continuous protection.
- **Access Control:** Implement and manage robust access control protocols and systems at all entry/exit points, including visitor management and personnel verification.
- **Patrol Services:** Conduct regular, documented site inspections, perimeter patrols, and vulnerability assessments to deter and detect unauthorized activities.
- **Incident Response:** Provide 24/7 rapid armed response to security alerts, intrusions, and other incidents within defined service level agreements.

Emergency Management: Provide 24/7 rapid armed response to security alerts, intrusions, and other incidents within defined service level agreements.

Control Room Operations: Establish and operate a 24/7 state-of-the-art security control room for continuous monitoring, alarm verification, dispatch services. real-time monitoring, incident response, and data analytics.

- Installation of a state-of-the-art video wall for live surveillance feeds, analytics, and reporting.
- Integration of secure, high-speed communication networks for seamless data flow between the control room and field operations.
- Automated reporting systems for proactive threat detection and decision-making.
- Compliance with the Protection of Personal Information Act (POPIA) to ensure all data is securely stored and managed.
- All licence/accreditation fees for the duration of the contract period must be included.
- Control room establishment is open to any bidder to set up a centralised control room where all sites' video feeds and alarms are going to be linked and ensure that all alarms and video feeds are linked.
- The successful bidders for zones will be responsible to link video feeds and alarms to the centralised control room.
- Eskom security team to coordinate the project and ensure alignment with the roll out plan.

CONTROLLED DISCLOSURE

3.2.2 Technology Integration Services (Baseline) linked to control room

- **CCTV Surveillance:** Install, configure, and maintain compliant, high-definition camera systems across all designated facilities, ensuring optimal coverage and image clarity.
- **Intrusion Detection:** Deploy and maintain effective perimeter and internal intrusion detection systems (e.g., fence sensors, motion detectors, thermal cameras) tailored to site-specific vulnerabilities.
- **Access Control Systems:** Implement and maintain integrated electronic access management systems, including biometric, card-based, or other specified technologies.
- **Drone Operations:** Utilize advanced drone technology for aerial surveillance, reconnaissance, and rapid assessment of network infrastructure (feeder lines, pole-mounted transformers, reclosers) to detect suspicious activity or damage. Provide detailed flight plans and operational procedures.
- **AI Analytics:** Integrate Artificial Intelligence (AI) analytics capabilities with CCTV and other sensor systems for intelligent threat detection, behavioural analysis, anomaly detection, and predictive security insights.
- **Integration and Commissioning:** The contractor will be fully responsible for the seamless integration and commissioning of all newly installed security system technology into the current Eskom control room located in Mkondeni. This includes all necessary software, hardware, network configurations, and data feeds.
- **Existing/Inactive Systems:** The contractor shall upgrade, integrate, and commission any existing or inactive security systems (CCTV, access control, alarms) at the specified sites into Eskom control room at Mkondeni. This includes an initial audit of existing infrastructure to determine compatibility and required upgrades

3.2.3 Maintenance and Support

- **Preventive Maintenance:** Implement a robust preventive maintenance schedule for all installed security technologies and systems, including regular testing, calibration, and cleaning to ensure optimal performance.
- **Corrective Maintenance:** Guarantee prompt fault resolution within specified timeframes, minimizing system downtime and security vulnerabilities. Provide clear escalation procedures.
- **System Upgrades:** Proactively manage and propose necessary technology updates, patches, and system improvements to maintain optimal security posture and leverage new advancements.

CONTROLLED DISCLOSURE

- **Training Services:** Provide ongoing training and development programs for all deployed personnel to ensure continuous skill enhancement, certification compliance (PSIRA, FCA, SACAA), and proficiency in operating advanced security technologies.

3.2.4 Technology Roadmap

- **Implementation Plan:** Provide a comprehensive, phased timeline for deploying proposed technologies, including pilot testing phases, full-scale implementation across various sites, and a clear strategy for scaling solutions to meet future needs.
- **Scalability:** Clearly explain how the proposed security solutions and operational models can be scaled efficiently to accommodate Eskom's growing infrastructure, changing risk profiles, or expanding geographical scope.
- **Innovation Strategy:** Detail the bidder's approach to staying ahead of emerging security threats and evolving criminal methodologies. This should include a commitment to adopting modern, advanced technologies, research and development initiatives, and a proactive posture towards security innovation.

3.2.5 Community Involvement

a) Liaison with the Community:

- **Community Liaison:** Develop and implement a strategy for effective and positive engagement with local communities surrounding the protected sites. This should include regular communication channels, awareness campaigns about the importance of electricity infrastructure, and mechanisms for receiving community intelligence regarding suspicious activities.
- **Job Creation/Local Procurement:** Where feasible and in line with Eskom's procurement policies, outline strategies for local job creation, skills transfer, and procurement from local businesses within the KZN-OU, contributing to community upliftment and fostering positive relationships.
- **Collaborative Safety Initiatives:** Propose and participate in joint safety awareness initiatives with local community structures, emphasizing the dangers of illegal connections and infrastructure tampering.

b) Liaison with Law Enforcement Agencies

- **Formal Communication Protocols:** Establish and maintain formal, documented communication protocols with the South African Police Service (SAPS) units operating in the zones, including relevant specialized units (e.g., Non-Ferrous Metals Combating Unit, Public Order Policing).

CONTROLLED DISCLOSURE

- **Intelligence Sharing:** Develop mechanisms for secure and timely sharing of intelligence regarding criminal activities, modus operandi, and identified hotspots with SAPS and other relevant law enforcement agencies (e.g., Transnet, PRASA security).
- **Joint Operations and Response:** Demonstrate a proven capability and willingness to participate in planned joint operations with SAPS and other security forces (e.g., roadblocks, scrap dealer inspections, illegal connection raids).
- **Evidence Collection and Preservation:** Ensure all security personnel are trained in proper scene preservation and evidence collection techniques to support SAPS investigations and improve the chances of successful arrests and prosecutions. Provide detailed incident reports that meet legal evidentiary standards.
- **Reporting and Compliance:** Adhere strictly to all legal requirements for reporting criminal incidents and cooperates fully with law enforcement in their investigations.

3.2.6 Handover Phase (At Contract End or Termination):

Documentation: Provide comprehensive as-built documentation for the entire control room infrastructure, including:

- Detailed architectural, electrical, and network diagrams.
- Equipment manuals, warranties, and licensing agreements.
- Software configurations, user manuals, and administrative guides.
- All Standard Operating Procedures (SOP), training materials, and emergency protocols.
- Full historical data archives.
- **Training:** Provide comprehensive training to nominated Eskom personnel (or incoming Service Provider's team) on the full operation, administration, and basic maintenance of all control room systems.
- **Knowledge Transfer:** Facilitate complete knowledge transfer regarding operational procedures, threat landscape, key contacts, and any ongoing projects.
- **Licensing Transfer:** Assist with the transfer of all relevant software licenses, warranties, and service agreements to ownership or to a successor Service Provider.
- **Physical Handover:** Securely hand over all physical assets, keys, and access credentials related to the control room.
- **Decommissioning (if applicable):** If the control room is to be decommissioned rather than handed over, provide a detailed plan for secure and environmentally responsible decommissioning and data sanitization.

CONTROLLED DISCLOSURE

3.3 Key performance indicators (KPI'S)

The successful bidder's performance will be rigorously evaluated against the following KPIs:

a) Primary Indicators

This framework outlines our commitment to measurable security outcomes, ensuring the protection of Eskom Distribution's assets and the safety of our operations.

Table 4: Primary KPIs

KPI	Target	Measurement Method	Reporting Frequency
1. Property Loss & Damage Reduction	<ul style="list-style-type: none">▪ To reduce significant theft/vandalism incidents causing material asset loss or operational disruption to:<ul style="list-style-type: none">- ≤ 4 incidents/year for High-Risk Sites (all Level 3 facilities).▪ - ≤ 2 incident/year for Medium-to-High Risk Sites (all Level 2 facilities).▪ - ≤ 0 incidents for Low-to-Medium Risk Sites (all Level 1 facilities).▪ ≤ 6 incidents/year for Network infrastructure incidents. Targeting a (zero) 0 crime incidents in the next years from current baseline.	<p>Definition: A "significant incident" is defined as confirmed theft or vandalism resulting in asset replacement cost exceeding R50,000 or causing an unplanned outage greater than 2 hours.</p> <p>Data Sources: Daily incident reports, forensic damage assessments, monthly asset audits, operational disruption logs, and reconciled financial loss reports.</p> <p>Verification: Regular third-party verification of incident classifications and financial impact.</p>	<ul style="list-style-type: none">▪ Daily (for incident reporting)▪ Monthly (for KPI tracking & reporting)▪ Quarterly (for aggregated trend analysis)
2. Incident Detection & Response Time	<p>To ensure timely and effective intervention for all security breaches:</p> <ul style="list-style-type: none">- 98% of security incidents detected within 2 minutes of occurrence.- 95% of verified security incidents receiving on-site armed response within 15 minutes (urban) / 30 minutes (rural) of dispatch.- 99% of detected incidents accurately recorded with full details and appropriate follow-up actions initiated.	<p>Detection Measurement: Automated system alerts (video analytics, alarm systems) timestamped against initial breach detection. Response Time Measurement: GPS tracking of armed response vehicles, timestamps from central monitoring dispatch to on-site arrival confirmation. Recording & Action Measurement: Review of incident logs, response reports, and documented follow-up actions (e.g., law enforcement notification, repair orders). Internal Eskom stakeholder feedback on response effectiveness.</p>	<p>Real-time (for individual incidents)</p> <p>Daily (for performance review)</p> <p>Monthly (for aggregated reporting)</p>

CONTROLLED DISCLOSURE

3. Regulatory & Policy Compliance	Achieve 100% compliance with all applicable security regulations and internal Eskom security policies (including PSIRA, FCA, SACAA, and Eskom's internal security standards).	Methodology: Monthly internal and annual external compliance audits against a comprehensive checklist of regulatory requirements and internal policies. Review of training records, license validity, and operational procedures. Documentation of all non-conformances and corrective actions taken.	Monthly (internal audits) Annually (external audits & overall compliance review)
4. Security Technology Operational Availability	Maintain 99.5% operational uptime for all critical security technology components (CCTV, access control, alarm systems, communication networks, AI analytics platforms).	Methodology: Automated system monitoring reports tracking component uptime and functionality. Detailed maintenance logs, including fault reports, resolution times, and preventative maintenance schedules. Daily system health checks by control room operators. Definition: "Operational uptime" means the system is fully functional and capable of performing its intended security detection and recording tasks.	Daily (automated reports) Weekly (detailed review) Monthly (performance summary)
5. Security Fault Resolution Time	To minimize security system downtime: - 90% of critical security system faults resolved within 8 hours. - 95% of major security system faults resolved within 24 hours. - 98% of minor security system faults resolved within 48 hours.	Methodology: Centralized fault logging system with precise timestamps for fault identification, technician dispatch, and resolution. Escalation records and root cause analysis for persistent or critical faults. Vendor performance tracking against agreed SLAs for technical support.	Real-time (for individual faults) Weekly (for trend analysis) Monthly (for overall performance review)
6. Stakeholder Satisfaction with Security Services	Achieve a ≥90% satisfaction rating from key internal Eskom stakeholders (e.g., Operations, Asset Management, regional management) regarding the effectiveness, responsiveness, and communication of security services.	Methodology: Monthly structured online surveys distributed to a defined group of key internal stakeholders, assessing satisfaction across key service dimensions (e.g., responsiveness, professionalism of guards, clarity of reports, impact on operations). Face-to-face feedback sessions and documented client feedback.	Monthly (survey deployment & report generation)

CONTROLLED DISCLOSURE

b) Secondary Indicators

These KPIs are designed to provide clear, measurable targets for key aspects of our security service delivery, ensuring operational excellence and continuous improvement.

Table 5: Secondary KPIs

KPI	Target	Measurement Method	Reporting Frequency
1. Security Personnel Deployment Rate	Achieve ≥99.5% coverage of all scheduled security guard shifts (day and night, for all assigned risk levels) across all sites, with any exceptions (e.g., unforeseen emergency leave) being immediately filled by a qualified replacement within 2 hours of notice.	Methodology: Daily automated shift management reports comparing scheduled vs. actual guard deployments, including timestamps for replacement assignments. Review of attendance logs and payroll records. Formal tracking of all unfulfilled shifts or shifts covered outside the 2-hour replacement window, with documented reasons.	Daily (for operational review & exceptions) Weekly (for aggregated percentage) Monthly (for formal reporting)
2. Verified Armed Response Time	Ensure 95% of all verified security incidents at Urban Sites (Risk Levels 2 & 3) receive armed response on-site within ≤15 minutes of dispatch. Ensure 90% of all verified security incidents at Remote Sites (Risk Levels 2 & 3) receive armed response on-site within ≤30 minutes of dispatch. This applies to all incidents requiring armed response per protocol.	Definition: "Verified incident" is an alarm or alert confirmed by monitoring as a genuine security breach requiring armed intervention. Response time is measured from the moment of dispatch (recorded in the control room log) to the confirmed arrival of the armed response unit on site (via GPS tracking data and armed response operational reports). Data Sources: Contractor GPS tracking reports, central monitoring incident timestamps, dispatch logs, and post-incident review forms.	Real-time (for incident tracking) Daily (for performance review of previous 24 hours) Monthly (for aggregated compliance percentages)
3. Security Personnel Training Compliance	Maintain 100% compliance for all active security personnel (guards, control room operators) with mandatory Eskom-specific security protocols and all relevant regulatory certifications (e.g., PSIRA grades, firearm competency, first aid), with certification validity maintained continuously. New personnel must complete mandatory	Methodology: Regular (quarterly) review of a centralized training database. Verification of individual training records, certification validity dates, and documented completion of refresher courses or new module training. Spot checks on site for valid guard licenses. Audits of training provider certifications.	Quarterly (comprehensive review) Monthly (for new hires & upcoming expiry tracking)

CONTROLLED DISCLOSURE

	Eskom induction training within 30 days of employment.		
4. Security Equipment Operational Functionality	Maintain ≥99.0% operational functionality across all deployed security technology (CCTV cameras, access control readers, alarm sensors, recording devices, communication links, drone systems) at all times, with any critical non-functional equipment restored within 24 hours.	Definition: "Operational functionality" means the equipment is performing its primary security function as designed (e.g., camera recording clear images, sensor detecting breaches, access control granting/denying access). Methodology: Automated system health monitoring reports, daily operator functional checks, maintenance logs tracking fault reports, resolution times, and preventative maintenance. Data Sources: Equipment status dashboards, maintenance management system records.	Daily (automated alerts & operational checks) Weekly (for trend analysis) Monthly (for aggregated performance reporting)

c) Innovation and Improvement KPIs

These KPIs are designed to measure our strategic progress in optimizing security operations through technology integration, achieving cost efficiencies, and fostering continuous innovation.

Table 6: Innovation and Improvement KPIs

KPI	Target	Measurement Method	Reporting Frequency
Guard Force FTE Reduction & Efficiency Gain	Achieve a 30% reduction in current full-time equivalent (FTE) guard positions by the end of Year 2 (From contract award date), specifically through the successful deployment of integrated security technologies, leading to a demonstrable improvement in operational efficiency. This will then extend to a 40% reduction by the end of Year 3 (From contract award date).	Baseline staffing reports vs. current FTE, technology deployment completion reports (verified operational status), and efficiency metrics (e.g., response times, incident resolution rates where technology is applied).	Quarterly
Critical Security Technology	Ensure 100% of all critical and high priority planned technology deployments are completed on or before their scheduled milestone	Verified project milestone completion dates, formal implementation sign-off reports, and post-deployment system functionality tests. Deviations from	Monthly

CONTROLLED DISCLOSURE

Deployment Adherence	dates, adhering to identified risk levels (as per Table 1, if available). This specifically refers to technologies enhancing site security and operational control.	schedule will require documented explanations and revised timelines.	
Technology-Driven Operational Cost Reduction	Achieve a 20% reduction in total operational security costs by the end of Year 1 (From contract award date), directly attributable to the implementation and optimization of new security technologies (e.g., reduced personnel costs, lower maintenance for older systems, energy savings from new equipment).	Comprehensive cost analysis reports comparing baseline operational security expenditure to post-technology deployment costs, detailed savings breakdown per technology, and efficiency metrics directly linked to cost reduction.	Quarterly
Strategic Security Technology Adoption & Value Realization	Successfully implement at least 1 new, approved strategic security technology into operational use annually (On contract anniversary date), each demonstrably contributing to enhanced security posture, improved operational efficiency, or significant cost savings as validated by pre-defined performance metrics and user acceptance.	Documentation of technology approval and procurement, signed implementation completion reports, post-implementation impact assessments (e.g., efficiency gains, incident reduction rates, cost savings reports with specific ROI, and structured user feedback/satisfaction surveys).	Semi-annually

3.4 Site evaluations

Site visits will be conducted for the successful bidders to verify that they have a functional Control room, legal firearms, Company owned vehicles as well as technologies that were proposed by the bidder.

3.5 Annual rates

Annual rates (as publicised in the Government Gazette) would not increase automatically but be first approved by Eskom and accepted by the Contractor in writing. There will be only one increase per year.

CONTROLLED DISCLOSURE

3.6 Terms of payment for monthly invoices

All invoices must follow the KZN OU Invoice process. The invoice period is from the 15th – 14th of each month. The monthly statements, invoices and all supporting documentation must be received before payment can be effected. All invoices must be processed in KZN office.

Should the service provider's documentation be incomplete or incorrect and cannot be resolved before the invoice period, payment will only be made once the correct documentation is provided.

ESKOM reserves the right to set-off amounts owed by the Service Provider from any amount due. The Service Provider must ensure that they furnish ESKOM with the correct banking information to affect a bank transfer and prevent delays in payment. Only original invoices will be processed for payment.

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

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

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

b) Task order instruction

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

Any specific requirements related to the quality standards for the services required will be included in the Task Order. Any constraints relevant to the services.

Contractor must prepare a quote after they received the task instruction (with full details of the scope of work) as per agreed price structure.

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

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

CONTROLLED DISCLOSURE

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

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

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

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

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

Task Order template will be provided to the Contractor after the signing and acceptance of this contract.

CONTROLLED DISCLOSURE