Eskom	**Scope of Work**	

Title: **Scope of Work for Integrated Security Systems at Eskom**

Document Identifier:	**559 - 487902534**
Alternative Reference Number:	**363-ERE-CEEC-D00035-23**
Area of Applicability:	**Eskom Academy of Learning**
Functional Area:	**Security**
Revision:	**4**
Total Pages:	**27**
Next Review Date:	**Not Applicable**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Supported by	Functional Responsibility	Authorised by

Content

1. Introduction

The Eskom Academy of Learning (EAL) is undertaking a strategic initiative to upgrade and modernize its campus into a fully integrated smart facility. As part of this transformation, physical security has been identified as a critical discipline requiring enhancement to align with the smart campus vision.

Over time, existing security technologies have deteriorated due to technological advancements, inadequate maintenance, and an increasingly complex crime risk landscape. These factors have contributed to significant vulnerabilities, exposing the campus to potential operational and asset losses.

To address these challenges, a comprehensive review and enhancement of EAL's physical security infrastructure is essential. The objective is to mitigate current and emerging threats through the deployment of advanced, AI and IoT driven security technologies.

This document outlines the minimum requirements for the design, supply, installation, commissioning, and ongoing maintenance of an Integrated Security System at EAL. The engagement will be structured through an outcome-based contract, ensuring accountability and performance.

The appointed service provider will be responsible for:

- Delivering and maintaining the integrated security solution.
- Providing training to all relevant stakeholders on the operation and management of the installed equipment.

2. Supporting clauses

2.1 Scope

Eskom invites potential suppliers to submit proposals for a turnkey solution covering the design, supply, installation, commissioning, and maintenance of an Integrated Physical Security System (IPSS) at Eskom Academy of Learning.

The proposed IPSS must incorporate and integrate multiple subsystems, including:

- Closed-Circuit Television (CCTV),
- Access Control (including metal detectors and X-ray machines at main entrance points),
- Alarm Systems,
- Public Address (PA) Systems,
- Intrusion Pre-Detection Systems,

N.B. The systems specified represent baseline technology and do not preclude the tenderer from proposing more advanced alternative solutions.

These subsystems must interface with a Physical Security Information Management (PSIM) system, including the necessary IT infrastructure, and upgrading of the current control room.

This document will further outline the business objectives and the desired functionality of the integrated system. Bidders are required to use the accompanying technical specifications/standards when preparing their proposals. Proposals must include a technology roadmap or project plan with detailed cost breakdown with priority given to the Access Control System rollout.

Following installation and commissioning, a successful service provider should continue support and maintain the systems to ensure system sustainability, continuous improvement, and alignment with the evolving risk landscape at Eskom Academy of Learning and all equipment maintains a warranty for a period of 5 years.

2.1.1 Purpose

Eskom invites potential suppliers to submit proposals for the Integrated Physical Security Systems at Eskom Academy of Learning. This document serves as an overview of the technical scope for an Integrated Physical Security System and stipulates technical requirements and deliverables.

2.1.2 Applicability

This document shall apply to Eskom Academy of Learning.

2.1.3 Effective date

This document will be effective from the 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] 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] 240-170000086 Roles and Accountabilities for Lifecycle Management of Physical Security Systems in the Transmission Division

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

[8] 240-60725641 Specification for Standard (19-inch) Equipment Cabinets

[9] DEM2412993 & 2425114 LAD (Logical Architecture Definition) PAC (Physical Application Component) for Physical Security Information Management System (PSIM)

[10] Business Requirement Specification DEM_2412993 & 2425114 Tx and ET Security Monitoring System

[11] 240-170000691 Standard for Intrusion Pre-detection Systems used at Eskom sites.

[12] 240-170000723 Generic Technical Requirements for Physical Security Technologies Contracts

[13] 240-78980848 Specification for Non-Lethal Energised Perimeter Detection System (NLEPDS) for Protection of Eskom Installations and its Subsidiaries

[14] 240-171000171 Commissioning Guideline for Secondary Plant Physical Security System

[15] 240-180100001 Secondary Plant Security Systems Maintenance Procedure

[16] 240-55410927 Cyber security standard for Operational Technology

[17] 0.54-393 Earthing Standards

[18] 240-161708025 Generic Public Address Systems Standard

2.2.2 Informative

N/A

2.3 Definitions

2.3.1 General

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 Academy of Learning.
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.
Contractor	The term will be used interchangeably with tenderer, service provider, supplier or bidder.

2.4 Abbreviations

Abbreviation	Explanation
EAL	Eskom Academy of Learning
AC	Alternating Current
CCTV	Closed Circuit Television
DC	Direct Current
DVR/NVR	Digital Video Recorder/Network Video Recorder
GUI	Graphical User Interface

Abbreviation	Explanation
PA system	Public Address system
IPSS	Integrated Physical Security System
IACS	Integrated Access Control System
LAN	Local Area Network
PSIM	Physical Security Information Management
UPS	Uninterrupted Power Supply
PTZ	Pan Tilt Zoom
PSIRA	Private Security Industry Regulatory Authority
WAN	Wide Area Network
PIR sensor	Passive Infra-Red sensor
SSP	Security Solutions Physical
AI	Artificial Intelligent
SAHPRA	South African Health Products Regulatory Authority

2.5 Roles and responsibilities

The contractor should specify the roles and responsibilities of each of their team members. Roles shall be as outlined in 240-170000086.

2.6 Process for monitoring

Not applicable

2.7 Related/Supporting documents

Not applicable

3. Project scope - OPTION 1: NEC Outcome Based Contracting (OBC)

The project includes requirements for an Integrated Physical Security System comprising a perimeter fence, non-lethal fence on top, Access Control Systems, CCTV System, Intrusion Pre-detection System, Alarm System, public address (PA) including Fire Detection System and interfaces to the PSIM System and IT infrastructure and upgrade the current control room.

The contractor shall design, supply, develop user documentation, perform testing, and deliver, install, and commission the Integrated Physical Security System and associated equipment (hardware/software etc.) at EAL according to the associated technical specifications.

The scope of work for the contractor for the Integrated Security System will include the following:

1. Produce designs for the Integrated Security System. The designs must include details for the Access Control System, CCTV System, Intruder Detection System, Alarm System, Public Address System and PSIM System (including IT Infrastructure). The design must also cover the integration of these different systems into an Integrated Security System.
2. Present the proposed designs to the Security Team for acceptance.

3. Installation and configuration of EAL security LAN Infrastructure.
4. Installation, configuration and commissioning of the CCTV System in totality on site as per Eskom Standard (240-91190304).
5. Installation, configuration and commissioning of the Integrated Access Control System (IACS) in totality on site as per Eskom Standard (240-102220945).
6. Installation, configuration and commissioning of an Intruder Detection System in totality on site as per Eskom Standard (240-91190304,240-86738968 & 240-170000096).
7. Installation, configuration and commissioning of an alarm system on site as per Eskom Standard (240-86738968).
8. Installation, configuration and commissioning of Public Address System in totality on site as per Eskom Standard (240-170000098).
9. Installation, configuration and commissioning of intrusion pre-detection system in totality on site as per Eskom Standard (240-170000691.
10. Integration of the Access Control System (ACS), CCTV System, Intruder Detection System, Alarm System, and Public Address System into an Integrated Security System (240-170000096) to interface with the PSIM system.
11. Provide services as per 240-170000723.
12. Standard For Non-Lethal Energised Perimeter Detection System (NLEPDS) Electrical Components 240-78980848.
13. Ensure full compliance with Eskom's Cyber Security Standard for Operational Technology (OT) Standard 240-55410927 in the design, installation, configuration, and commissioning of all security-related systems, networks, and infrastructure. This shall include the implementation of cybersecurity controls, hardening of devices, secure configurations, network zoning, access management, firewall rules, system monitoring, encryption requirements, patching, and vulnerability mitigation in accordance with the standard. All systems integrated into the security environment shall be secured and validated for cyber compliance prior to commissioning.
14. Installation, configuration and commissioning of interfaces to the Physical Security Information Management (PSIM), including firewall configuration and Telecoms circuit commissioning, for data collection, incidents management, data correlation, controlling functionality (CCTVs, IACS systems, PA Systems, etc.) and provision of real-time dashboards and reports (refer to DEM2412993 & 2425114).
15. Conduct FAT and SAT tests before commissioning the complete integrated system.
16. Compile site as-built drawings with electrical and engineering details.
17. Create a graphical user interface (GUI) and behaviour models for the site.

N.B. The systems specified represent baseline technology and do not preclude the tenderer from proposing more advanced alternative solutions.

3.1 Integrated Access Control System (IACS)

1. The Integrated Access Control System will be used to manage the access rights of Eskom Academy of Learning employees, visitors and contractors in and out of different areas at all the sites.
2. The system will also be used to grant and limit access permissions in and out of secure and non-secure areas.
3. The offered system shall comply with the requirements of the Specification for Integrated Access Control System (IACS) for Eskom sites (240-102220945).
4. The system should support a tiered architecture, which will allow monitoring of the sites both locally and remotely. This architecture comprises field devices (biometric, QR codes and card readers) at the site level and system management servers at the remote security nerve centre.
5. The system should integrate with other subsystems like Visitor management system, Surveillance system, etc. The system should be modern and fit for a smart campus initiative. The supplier can propose the latest technology to be deployed in a smart campus environment.

3.1.1 Biometrics, QR codes and card reader

The main access to the premises should be the use of either a fingerprint or a card.

- Biometrics and card reader shall comply with SANS 2220-2-5 and SANS 2220-2-3, respectively.
- Card and biometric reader should be installed at every point of entry.

3.1.2 License plate recognition (LPR) cameras:

- High-resolution cameras capable of capturing license plates in various lighting and weather conditions.
- Integration with access control systems to automate vehicle entry/exit.
- Integrate with eNatis for real-time alerts for unauthorised or flagged vehicles. Maintain necessary licenses.

3.1.3 Metal Detectors and X-Ray machines

The bidder is required to provide screening equipment at designated main access points to support the detection and prevention of unauthorised items entering the premises. The solution should include personnel and baggage screening technologies that are suitable for high-traffic environments and aligned with recognised safety and performance standards. The equipment must be capable of detecting a wide range of prohibited items and should support rapid processing without compromising accuracy or safety.

It is expected that the proposed systems will integrate seamlessly with existing security infrastructure, including access control and centralised security management platforms. Compliance with applicable local regulatory requirements, including radiation safety regulations enforced by the South African Health Products Regulatory Authority (SAHPRA). Equipment must include shielding to prevent radiation leakage and emergency stop features for operator safety.

3.1.4 IACS device layout

The examples of access control devices for the sites and their locations are shown in Table 1 below:

Area	Point	Device	Status Contact	Lock	Evacuation Device	Bypass
Main Access	Boom Gate	Card or Fingerprint Reader	Boom Status Contact	Electro-mechanical Lock	None	Mechanical Switch
Security Office	Entrance Door	Card or Fingerprint Reader	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Switch
Control Room	Entrance Door	Card +Face recognition Reader	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Switch
	Emergency Exit Door	Emergency Exit Button	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Switch
	Server Room Entrance	Card +Face recognition Reader	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Switch
Offices, boardrooms, residences, classrooms and Canteens	Entrances	Card or Fingerprint (In) & Card (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Switch

Table 1: IACS devices positioning

3.1.5 IACS high-level devices positioning and architecture philosophy

1. The contractor is required to submit a detailed design depicting the proposed architecture and narratives of how the IACS functional requirements will be achieved. The implemented architecture for IACS should comply with the principles outlined in the technical standards for IACS.

2. In addition to ensuring that the installed system operates as required on-site, the contractor must also ensure that the system enables remote monitoring and control through Eskom WAN.

3.2 Intruder Detection Systems

Intrusion pre-detection units shall be installed in all areas of the Working Environments, including buildings, rooms and the perimeter area which need to be protected.

The proposed solution must include hardening of the existing perimeter fence with an energised **non-lethal fence on top.** The fence lining must be integrated with the Security Management System to enhance the required detection capability. Proposed Intruder detection systems may be perimeter thermal cameras with three layered virtual fencing.

The sensors shall be placed to effectively detect intrusion into the protected (secured) areas.

The intruder detection should have protection from vibrations caused by digging underneath, breaking through and climbing over the barrier fences/walls. The contractor can propose a suitable device for this protection.

The buildings inside should be protected by a PIR sensors or cameras that are capable of this function and the scope should add the devices where they are missing.

The Intrusion Pre-detection System installed shall comply with the requirements of the Standard for Intrusion Pre-detection Systems used at Eskom sites (240-170000691).

3.2.1 Security Lighting

The perimeter shall be equipped with security lighting that activates automatically in the event of an intrusion or alarm condition. The solution must include the following:

- Intelligent perimeter lighting that automatically switches on when an intrusion, alarm, or pre-warning signal is received from any perimeter detection device, thermal camera, fence alarm, or access control alert.
- Lighting systems shall be integrated into the Security Management System (SMS) to ensure real-time activation, event correlation, and operator visibility.
- The lighting must provide sufficient illumination for CCTV verification, guard response, and deterrence without compromising safety or revealing covert systems.
- Lighting units must be placed to:
    - Eliminate dark spots along the fence line
    - Support visual tracking along patrol routes
    - Enhance facial and vehicle identification during alarm-triggered events
- Lighting infrastructure shall support low-power standby mode and switch to full output when triggered.
- The system must fail-safe to ensure minimum security illumination during power or network disruptions, with backup power integrated into the lighting circuit design.
- The contractor shall propose lighting technology suitable for the environment (e.g., LED floodlights, pole-mounted lights, integrated smart security lighting).

The perimeter lighting solution must be designed to support detection, verification, response, and deterrence, functioning as a visual extension of the intrusion detection system.

3.3 Visitor Management System

a) Complete installation and setup of the system to facilitate visitor management. Visitors can pre-register through an online portal or a mobile app before their visit. For permission, the system gathers identity documents, pictures, personal information, and the reason for the visit.
b) Set up a self-service kiosk or tablets at the appropriate location. Visitors can use the self-service kiosk or tablet at the facility entry to check in when they arrive. The visitor can look up the host by name using the system. For security reasons, guests will need to take a picture, digitally sign in, or scan their identification card.
c) The ability to give and deny access to authorised areas based on visitor data is one of the features of integration with the present access control system that ensures compatibility.
d) Identification and verification: Several identity verification techniques, including QR code scanning, ID scanning, driver's license verification, and biometric choices (such as fingerprint or face recognition).
e) Following a successful check-in, visitors are given a physical or digital badge that contains their name, photo, the locations they are permitted to enter, and the host's information.
f) Host notification: setting up to notify hosts in real-time when guests arrive (visitors can only proceed when the host collects them from reception).
g) Integration with access control systems, including key cards and biometric readers, is made possible. Depending on their authorisation, visitors can enter secure areas using their badges, and security staff can monitor them in real-time.
h) Compliance and audit trails keep a thorough record of every visitor's activity, including the precise times of check-in and check-out, the locations visited, and any incidents.

3.4 CCTV Systems

A CCTV System shall be installed and the proposed system for the Working Environments is intended to provide the guards/control room operators with a single point from where they can view and verify alarm events from the Intrusion Detection System and energised fence triggers without having to physically respond to the alarm event in the case of a false/nuisance alarm and correctly assess and verify positive alarm events in the event of an attempted or successful intrusion attempt.

Implement AI video analytics software that integrates with the existing CCTV cameras. Use AI-driven intrusion detection systems that can analyse patterns and detect unusual activities.
Integrate AI with the existing access control systems to add features like biometric authentication and predictive analytics for identifying potential security breaches.

The offered system shall comply with the requirements of the Eskom Standard for CCTV System (240-91190304).

The CCTV System shall be integrated with video analytics and automatically record any alarm event using the 30-second pre-event buffer, the actual event (for however long motion is detected by the camera) and at least a 30-second post-event period. The system shall utilise a Video Analytics System as pre-detection to automatically generate alarms and perform event recording.

It is proposed that static thermal cameras with video motion detection be installed along the perimeter of the Working Environments to provide both surveillance and detection functionality. In addition, it is proposed that PTZ cameras be installed strategically for zooming and recognition functionality.

The CCTV System shall be connected to the security LAN to enable event-driven video streaming to the local security control room and a nerve centre.

A video intercom system must be installed at the main gate entrance, and the audio feed and camera feed from the unit must be integrated into the local NVR to ensure both visual and audio recording of events. This unit enables the Security Control Room to interact with unannounced visitors and non-EAL staff.

The contractor shall determine the required camera lens types to ensure that the positioning of the cameras results in the most optimised and economical installation of the cameras on the Working Environments. This includes ensuring that continuous visibility is created along the perimeter by eliminating blind spots with one camera having the next camera within its field of view for effective monitoring.

All steel poles and structures shall be hot-dipped galvanised.

3.4.1 CCTV positioning

All CCTV (cameras) may be positioned as below, and the tenderer can propose the best solution:

Area	Location	Device	Type
Perimeter	Perimeter fence	Static thermal camera Associated PTZ	Detection and Identification
Access gates	Main access gate	Static optical camera Video intercom	Identification
Buildings and offices	Main building entrances	Interior and exterior static cameras	Monitoring and Identification
	Office and canteens entrance	Interior static dome camera	Monitoring and identification
Inside buildings	Building corridors, classrooms and common areas	Static dome cameras	Detection and Identification
Outside Working Environments	Working Environments and driveways	Motion detection cameras PTZ	Detection and Identification
Entrance and Exit of Parking lot	Parking Lots	Camera capable of vehicle counting	Counting

Table 2: Camera positioning layout

3.5 Alarm System

The Alarm System shall be installed and will form an integral part of the other security systems installed at EAL to provide proactive coverage and monitoring of all protected areas i.e. site perimeter, entrances, buildings, server rooms and other strategic places within the campus. The following inputs shall trigger the Alarm System:

- Camera video analytics alarm detection on the zone(s).
- Alarm inputs from the electric fence.
- Alarm inputs from intrusion pre-detection devices.
- Alarm inputs from access control points.

The installed Alarm System shall comply with the requirements of the Specification for Integrated Security Alarm System for Protection of Eskom Installations and its Subsidiaries (Identifier: 240-86738968) and alarming requirements of other integrating technologies mentioned above, forming part of the Integrated Security System at the site.

3.6 Public Announcement System

- The installation of a PA System is required to engage potential intruders and issue warnings.
- The PA System shall be able to be remotely and locally operated when necessary.
- The system must be operable from the guard house and remotely from the responsible control rooms to warn intruders of the restriction of access to the site.
- Voice recordings shall be synchronised with the cameras and recorder on the local NVR via suitable audio input to ensure synchronisation of events.
- Linking the PA to the Fire Detection System and the closest CCTV camera. This will assist with deploying emergency response to the exact location.
- The installed PA System shall comply with the requirements of Technical Specification for Public Address Systems (240-170000098).

All speakers shall be positioned strategically along the perimeter fence and across the campus.

3.7 Site monitoring and control

The contractor will be responsible for the relocation of the current control room at Eskom Academy of Learning. The new control room must be a state of the art and must be designed and equipped to meet modern operational and security standards, enabling effective command, control, and monitoring capabilities.

The control room must include the necessary infrastructure (like Video wall, consoles, server room, modern furniture, etc), systems, and user interfaces to support the centralised management of on-

site systems as well as remote sites. The design should facilitate the integration of multiple security subsystems and allow for real-time decision-making across the broader security environment.

a) There shall be a security manager workstation at the site in the security building for local allocation and revoking of access rights and control of security workflows.
b) There shall be a maintenance manager workstation in the security building for controlling maintenance workflows.
c) Some or all of the functions listed in Items (a) and (b) above may be combined into a single physical workstation. The workstation software GUI shall be based on the operator log-on credentials to be able to perform functions listed in Items (a) and (b) above.
d) The security alarms and CCTV visuals should be routed to the remote nerve centre through the Eskom WAN or alternative network.
e) The system shall allow the remote Security Control Centre to remotely control PTZ cameras at the site.
f) The system shall allow the remote Security Control Centre to communicate audio (via PA system) and data with the Working Environments, including the ability to give audio warnings over the PA System to the security zone that detected an intrusion.
g) Security Control shall be able to retrieve any of the stored event data or video streams in real-time, either locally or remotely.

3.8 E-Guarding or virtual guarding

The e-guarding or virtual guarding system serves as a technology-enabled extension of physical security, leveraging surveillance infrastructure to provide remote monitoring, verification, and proactive detection of risks. Its primary role is to supplement physical patrols**,** enhance awareness, and ensure continuous coverage of critical areas.

a) The tenderer to propose a system that can be utilised in conjunction with the cameras to conduct virtual guarding.
b) The system should be integrated into the management system software.
c) The system should allow guards/operators to virtually patrol the sites and tag to detect the areas where the guards have missed.
d) The system must be fully integrated into the centralized Security Management System (PSIM platform) to ensure seamless monitoring, event logging, and reporting.
e) All patrol activities, alarms, and operator actions must be recorded within the management platform for audit and compliance purposes.
f) The system must support real-time incident escalation to the control room and trigger automated responses (e.g., PTZ camera zoom, alarms, or notifications to on-site teams).

3.9 Video Walls

The Video Walls shall be a key tool in the Control Centres, providing a clear and shared view of security operations. The video wall shall support real-time monitoring, quick decision-making, and coordinated response across all security systems. The video walls must be modern, seamless (Ultra narrow bezel), smart, and flexible, allowing for easy integration, configuration, and display of data from multiple security platforms.

a) Live Video Monitoring and Visualisation

- Display live video feeds from all local CCTV cameras, including critical infrastructure, perimeter zones, access points, and high-risk areas.
- Support simultaneous display of multiple camera streams with configurable layouts, prioritisation of critical feeds, and rapid switching during incidents.
- Enable automatic camera call-up based on alarms, access control events, or intrusion detection triggers.

b) Integrated Operational Dashboards and Alerts

- Display consolidated operational data and dashboards sourced from PSIM, VMS, access control, intrusion detection, and other integrated systems.
- Provide real-time visualisation of emergency alerts, alarms, system health status, and incident escalation levels.
- Support visual and audible alerting on the video wall to draw operator attention to high-priority or critical incidents.

c) Access Control, Intrusion, and Sensor Event Visualisation

- Display access control logs, including real-time and historical entry/exit events for personnel.
- Visualise intrusion detection events, motion sensor activations, thermal alerts, and perimeter breaches in real time.
- Present building layouts, floor plans, site maps, and GIS overlays with event pinpointing to enable rapid navigation and incident localisation.

d) Command, Control, and Coordination Enablement

- Support shared situational awareness among operators, supervisors, and incident commanders through a common operational picture.
- Facilitate coordination between security personnel, emergency responders, and management by displaying incident timelines, response actions, and communication status.
- Allow role-based access to content displayed on the video wall to ensure operational and information security.

e) Operational Resilience and Continuity

- Operate continuously on a 24/7/365 basis with redundancy at display, controller, power, and network levels.

- Provide automated failover, system health monitoring, and proactive fault alerts to minimise downtime.
- Ensure seamless operation during power interruptions through integration with UPS and backup power systems.

f) Scalability and Future Readiness

- Be modular and scalable to support future expansion in screen size, resolution, number of sources, and integrated systems without major redesign.
- Support evolving technologies, including AI-driven analytics, advanced dashboards, and additional remote site integration.

3.10 Power supply

a) All system servers shall be housed in 19-inch equipment cabinets as specified in the Eskom Standard 240-60725641. This specification covers the earthing requirements in the cabinet as well.

b) Power shall be distributed through the panel to isolate the supply of the subsystems using appropriately sized MCBs. At a minimum, the following will be on separate supply circuits:

- Perimeter cameras
- Indoor cameras
- PA system devices
- Site controllers and server-based equipment.

c) Other security-related equipment such as gate motors and electric fence energisers.

d) The system shall have a power failure indication that shall be sent through to the remote Security Control Room should the supply be interrupted.

e) The existing power systems at the site shall be used as the primary power sources, provided that the site's standby time (autonomy) requirements are not adversely affected.

f) Tenderers are required to propose a suitable standby power system and UPS sized appropriately to handle the expected system load. Eskom Academy of Learning may, however, decide to utilise the existing standby batteries at the site.

3.11 Earthing and Bonding

As part of the perimeter security upgrade, the contractor shall conduct a comprehensive inspection of the earthing and bonding system along the entire perimeter fence line, including all energised fence components, perimeter lighting poles, electronic devices, and security infrastructure.

The following requirements apply:

- The contractor shall inspect, test, and verify the earthing system for compliance with Eskom standards and applicable SANS electrical safety requirements.

- All fence posts, energised fence lines, electronic devices, perimeter lighting poles, and associated metal structures must be correctly earthed to ensure:
    - Personnel safety.
    - Protection of electronic equipment.
    - Compliance with electrical standards.
    - Proper operation of energised non-lethal fence systems.
- Any faulty, damaged, high-resistance, corroded, or non-compliant earthing points shall be corrected, replaced, or reinstalled to meet specification.
- Measurements of earth resistance must be performed using calibrated instruments, and all results must be recorded and submitted.
- Earthing must be coordinated with the requirements of the energised fence, perimeter detection devices, and lighting circuits to prevent electromagnetic interference, false alarms, or equipment malfunction.
- The contractor shall submit a detailed Earthing Compliance Report, including:
    - Test results
    - Corrective actions taken
    - Location maps of earth spikes and bonding points
    - Certification of compliance
- Any additional earthing points required to stabilise the perimeter system shall be supplied and installed as part of this scope.

The earthing system must support the reliable performance of the energised fence, perimeter lighting, and all intruder detection devices as part of an integrated security solution.

3.12 Site tests and commissioning

The testing of the system shall be done in the presence and to the satisfaction of an authorised representative of Eskom Academy of Learning.

Tests shall include simulating fire conditions, testing network cabling, testing and switching audio and video signals, testing access control events, etc., to prove the efficiency of all aspects of the system to the satisfaction of Eskom Academy of Learning security team.

All equipment, material, etc., that may be necessary for these tests shall be supplied by the contractor, including a suitable smoke and heat generator.

The contractor shall do his complete commissioning tests before the actual first take-over tests are done. This is to satisfy himself that everything is working and is in accordance with the specification. Three system faults will result in Eskom Academy of Learning aborting the test, subsequent commission costs incurred by Eskom Academy of Learning shall be for the contractor’s account.

After submission of the test results, the contractor shall notify that the installation is complete, tested and in working order. Eskom Academy of Learning will witness the re-testing of the installation.

3.13 As-Built drawings and documentations

The contractor shall prepare as-built drawings of his completed installation – including conduit, cables and fibre routes.

The Operator's Manuals must be compiled and contain enough detailed information to enable a suitably qualified Eskom Academy of Learning technician to control and operate the full installation without any training from the contractor. The Operator's Manuals must be a separate set of documents from the Maintenance Manuals.

Irrespective of the abovementioned, the Operator's Manuals must also contain short-form instructions to enable trained operators (trained by the contractor) to operate the full installation.

The contractor shall also prepare a comprehensive set of Operations Maintenance Manuals for approval by Eskom Academy of Learning.
The following shall be included as a minimum:

- Cover page
- Index
- Contractor contact details
- Call-out procedure
- Manuals and specifications of all the installed equipment
- Installed equipment warranty details, including supplier contact information.
- Commissioning data
- Photo report of installation
- Snapshots of all camera’s day and night
- Handover Certificates
- Operator Guides and Procedures.
- Maintenance schedules (weekly, monthly, quarterly, and yearly)
- As-built drawings
- Bill of quantities
- Construction monitoring
- Quality assurance about specifications
- As-built drawings and close-out
- Supply and delivery of material
- Construction, commissioning and handover of the works based on the designs.

3.14 Training

All training aids and course notes necessary to conduct effective operational and maintenance training shall be supplied by the contractor. The training venue will be made available on-site by Eskom Academy of Learning.

The training documentation must be accredited and submitted to Eskom Academy of Learning for evaluation and approval.

Each group of trainees should receive a minimum of four hours of training. Allow to fully train three groups, each of up to four personnel. (The amount of personnel sent for training is at the full discretion of Eskom Academy of Learning).

Training shall be adequate to ensure that the groups trained are competent in the operation of systems, adequately trained to carry out ongoing training, and fully aware of the location of all equipment installed as part of this contract within their area of responsibility.

The contract shall adhere to Eskom Academy of Learning-defined security procedures for access to and during site attendance over the defect liability period.

3.15 Cyber Security Requirements

3.15.1 Access Control: Access control, unique user IDs and passwords shall be used to access the system.

3.15.2 Information Security Management System (ISMS): The Supplier or Service Provider shall have a valid Information Security Standard (ISO) 27001 certificate.

3.15.3 Encryption Standard: Data at rest to be encrypted using at minimum Advanced Encryption Standard (AES)-256 and in transit (or in motion) using at minimum Transport Layer Security (TLS) 1.3 or later version.

3.15.4 Audit trails, logs, user activity logs: Audit trails, logs, user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators.

3.15.5 Patch Management: Patch Management Process shall be defined. The software updates and patches shall be tested in a non-production environment before being deployed into the production environment.

3.15.6 Role-Based Access Control (RBAC): The software shall employ Role-based access control (RBAC) mechanism.

3.15.7 Input and File Handling Security: All user inputs and imported or exported files shall be validated, sanitized, and properly encoded to prevent injection attacks, block malicious content, and ensure integrity across all data and file operations.

3.15.8 Data Integrity: Data shall be secured at minimum using a secure hash algorithm (SHA)-256 for data integrity, securing transactions, and messages.

3.15.9 Privileged Access Management (PAM): The system shall be able to onboard privileged accounts onto PAM tools, such as CyberArk but not limited to onboard privileged accounts to securely manage, rotate passwords, monitor, record sessions, control, enforce access to privileged accounts, auditing and reporting capabilities.

3.15.10 Data Masking: Sensitive information such as personal identifiable information (PII) data in non-production environments shall be masked.

3.15.11 Data Back-up: A back up Restore Plan and Procedure shall be defined, annually tested, and such test results shall be shared with Eskom's Cyber Security team.

3.15.12 Daily Incremental Back Ups: Incremental daily back-ups shall be done, encrypted, and securely kept offsite only for all critical systems.

3.15.13 Security Information and Event Management (SIEM) Integration: The on-premises System and Cloud Service shall be able to integrate with SIEM standard technologies such as Syslog, Windows event logging, Simple Network Management Protocol (SNMP) and Application Programming Interface (API) but not limited to these technologies listed.

3.15.14 Database Security Management: Database Security Management tools shall be employed to provide regulatory compliance, encryption, key management, granular access controls, flexible data masking, comprehensive activity monitoring, and sophisticated auditing capabilities.

3.16 Warranty and Support

The contractor shall provide a five-year (**60**-**month**) warranty for all installed systems from the date of final acceptance, covering defects in materials, workmanship, installation, and system configuration.

During the warranty period, the contractor shall, at no additional cost, rectify all failures attributable to such defects within agreed response times, including repair or replacement of faulty components and limited preventive inspections solely for defect detection. Where required to maintain system operability, the contractor shall implement manufacturer-issued patches, firmware updates, or compatibility adjustments directly related to warranty compliance.

The contractor shall also provide limited refresher training and knowledge transfer to nominated stakeholders to ensure correct system operation and a smooth transition upon expiry of the warranty period, excluding damage arising from misuse, unauthorised modifications, third-party interference, or conditions outside specified operating parameters.

3.17 Maintenance and Support

The contractor will be fully responsible for the maintenance and support of the installed systems throughout the **60-month** contract period. This includes preventive maintenance, which entails scheduled inspections, system testing, and servicing to ensure optimal performance and reduce the likelihood of failures.

The contractor is also expected to provide corrective maintenance by addressing system faults and restoring functionality within agreed timeframes. In addition, the contractor must implement system upgrades as needed, incorporating relevant technology updates and improvements to maintain the system's effectiveness.

As part of the support scope, the contractor will also be required to provide ongoing training services, ensuring that relevant stakeholders are adequately equipped and certified to operate and manage the system by the end of the contract period, facilitating a seamless handover.

3.18 Technology Roadmap

- **Implementation Plan:** Provide a phased timeline for deploying technologies, including pilot testing, full-scale implementation, and scaling across sites. The tenderer to prioritise Integrated Access Control on the rollout plan.
- **Scalability:** The contractor to demonstrate how the proposed solutions can be scaled to meet Eskom’s growing or changing needs.

- **Innovation Strategy:** The contractor must detail the approach for staying ahead of emerging security threats through the adoption of modern and advanced technologies.

Phase	Plan	Description	Expected Outcomes
1	Foundational Upgrades	• Relocate and modernize the Control Room, with new video wall and upgraded Security Management System (SMS/PSIM). • Deploy Visitor Management System (VMS) at all main entrances. • Install License Plate Recognition (LPR) cameras at gates, fully integrated with eNatis for vehicle verification and automated gate control.	• Centralized, modern command centre. • Enhanced visitor accountability and compliance. • Automated, fast, and secure vehicle access.
2	Perimeter Intrusion Detection (Geo-fencing)	• Install thermal imaging cameras for 24/7 detection along the perimeter. • Configure geo-fencing zones for real-time alerts when breaches occur. • Link to associated PTZ cameras for auto-tracking, zooming, and incident verification. • Integrate with SMS for alarm escalation.	• Reliable perimeter intrusion detection (day/night, all weather). • Reduced false alarms. • Faster incident response via auto-tracking.
3	Access Control System (ACS)	• Implement/upgrade integrated access control using smart cards/biometrics at all sensitive areas. • Integrate with VMS and SMS for unified identity management. • Enable role-based access with full audit trails.	• Improved control over staff, contractors, and visitors. • Reduced risks of unauthorized entry. • Regulatory compliance on identity management.
4	Campus, workshops & Classroom Surveillance	• Deploy/upgrade IP cameras in classrooms, offices, and critical infrastructure buildings. • Enable video analytics (loitering, occupancy counting, motion detection, etc.). • Integrate with control room monitoring platform.	• Safer environment for employees and learners. • Evidence for disciplinary or criminal investigations. • Analytics-driven monitoring of critical indoor spaces.

Phase	Plan	Description	Expected Outcomes
5	System Optimization & Advanced Analytics	• Introduce AI-driven analytics (facial recognition, abnormal behaviour detection, crowd analysis). • Upgrade storage and networking for high-volume video retention. • Deploy predictive maintenance on thermal/PTZ and access devices to reduce downtime.	• Proactive threat identification. • Enhanced operational efficiency. • Sustainable, future-proofed security ecosystem.

Table 3: Five Phase Technology Roadmap

3.19 Deliverables

- Detailed Security System architecture and designs.
- Procurement and installation of security components.
- Security integration with Smart Working Environments infrastructure.
- Training and documentation for security personnel and relevant stakeholders.
- Final performance testing and optimisation reports.

3.20 Implementation timelines

Task	Duration	Milestones
System Design and Approval		Blueprint Finalisation
Equipment Procurement		Vendor Selection
Installation and Configuration		Deployment and Testing
AI & IoT Integration		Data Synchronisation
Training and Handover		Project Completion

Table 4: Implementation Timelines

3.21 Risk management

Risk Factor	Mitigation Strategy
AI algorithm accuracy	Regular AI model training and updates

System downtime	Redundant serves and backup power systems
Compliance threats	Aligning with industry standards, Eskom Academy of Learning Standards and Security Policies
Operational disruptions	Phased implementation and testing

Table 5: Risk managements

3.22 Systems Performance Matrices

3.22.1 Alarm Systems Specification:

- Integration with motion detection systems for early threat detection.
- Must include tamper-proof mechanisms and backup power supply (e.g., UPS or solar).
- Real-time alerts to a centralised monitoring system.

Targets:

- False alarm rate: ≤ 5%.
- Uptime: 98% over 60 months.

3.22.2 Motion Sensors Specification:

- Strategically placed to cover all critical areas, including perimeters, entry points, and high-value assets.
- Must include advanced features such as thermal imaging and pet immunity to reduce false alarms.
- Integration with alarm systems and CCTV for real-time intrusion detection.

Targets:

- Detection accuracy: ≥ 95%.
- Response time: ≤ 5 seconds from detection to alert.

3.22.3 CCTV Cameras Specification:

- High-resolution cameras (minimum 4mp) with night vision and wide dynamic range (WDR) for low-light conditions.
- AI-based analytics for real-time threat detection (e.g., loitering, perimeter breaches).
- Active monitoring 24/7 with footage stored for a minimum of 90 days.
- Integration with alarm systems and motion sensors.

Targets:

- Coverage of critical areas: 100%.

- Uptime: 98% over 60 months.

3.22.4 License Plate Recognition (LPR) Cameras Specification:

- High-resolution cameras capable of capturing license plates in various lighting and weather conditions.
- Integration with access control systems to automate vehicle entry/exit.
- Real-time alerts for unauthorised or flagged vehicles.

Targets:

- Recognition accuracy: ≥ 95%.
- Response time: ≤ 10 seconds from detection to alert.

3.22.5 Access Control Systems Specification:

- Biometric scanners (fingerprint or facial recognition) for personnel access.
- Integration with LPR cameras for vehicle access.
- Real-time monitoring and logging of all access events.

Targets:

- System uptime: 98% over 60 months.
- False acceptance rate: ≤ 0.1%.

3.22.6 Public Address Systems Specification:

- Clear and audible announcements for emergency notifications.
- Integration with alarm systems for automated alerts.

Targets:

- Coverage of critical areas: 100%.
- Uptime: 98% over 60 months.

3.22.7 Intrusion Detection Systems Specification:

- Combination of motion sensors, thermal imaging, and perimeter detection systems.
- Real-time alerts to a centralised monitoring system.

Targets:

- Detection accuracy: ≥ 95%.
- Response time: ≤ five seconds from detection to alert.

4. Acceptance

This document has been seen and accepted by:

Full Name and Surname	Designation

5. Revisions

Date	Rev.	Compiler	Remarks
March 2026	4	Andre van den Berg	• Removed Section 4 and added PA System Standard
February 2026	3	Matsobane Phosa	• Added security lighting, earthing, video wall requirements. • Amended signatories.
August 2025	2	Matsobane Phosa	• Aligned the SOW to OBC model. • Added the Technology Road map. • Expanded on the E-Guarding service.
February 2025	1	Matsobane Phosa	Scope of Work for EAL

6. Development Team

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

- Sama Mabona, Middle Manager ERE Security
- Matsobane Phosa, Senior Advisor SSP

7. Acknowledgements

N/A