	<b>Report</b>	<b>Group Technology</b>
---	---------------	-------------------------

Title: **Scope of Work for Integrated Physical Security System contract for Eskom Transmission Grid and Telecoms** Document Identifier: **240-170001030**

Alternative Reference Number: N/A

Area of Applicability: **Transmission**

Functional Area: **Engineering**

Revision: **3**

Total Pages: **31**

Next Review Date: **N/A**

Disclosure Classification: **Controlled Disclosure**

**Compiled by**



**Donald Moshoeshe**  
**Chief Engineer- PTM&C**

Date: 19/08/2024

**Functional Responsibility**



**Cornelius Naidoo**  
**Middle Manager - Telecoms & Physical Security T&S**

Date: 22 August 2024

**Authorized by**



**Judith Malinga**  
**Senior Manager – PTM&C**

Date: 23/08/2024

## **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.....	4
2.2.2 Informative.....	5
2.3 Definitions .....	5
2.3.1 Disclosure Classification.....	6
2.4 Abbreviations .....	6
2.5 Roles and Responsibilities .....	6
2.6 Process for Monitoring.....	6
2.7 Related/Supporting Documents.....	6
2.7.1 Reference drawings.....	6
3. Scope of work.....	6
3.1 General .....	6
3.2 Accreditation .....	7
3.3 Experience and Expertise.....	7
3.4 Supplier's obligations.....	7
3.5 Product Design and Engineering .....	7
3.5.1 Design artifacts.....	7
3.5.2 Design assurance.....	7
3.5.3 Design Engineering .....	7
3.5.4 Application.....	8
3.5.5 Equipment and Product Profile .....	8
3.6 Supply and delivery .....	8
3.7 Support Services .....	8
3.8 Equipment evaluation .....	9
3.9 Test equipment and tools .....	9
3.10 Training .....	9
3.11 Handbooks .....	9
3.12 Project Management .....	9
3.13 Installation and commissioning.....	9
4. Technical returnables and index .....	13
5. Acceptance.....	13
6. Revisions.....	13

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

7. Development Team .....	14
8. Acknowledgements .....	14
Annex A: Technical Returnables Index Guideline.....	15
Annex B: Detailed design report index for Integrated Physical Security System .....	16
Annex C: Typical installation scope for a Fully integrated Physical Security Site.....	18
Annex D: Typical site layouts .....	28
Annex E: PSIM interfaces development typical process.....	30

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

## **1. Introduction**

Eskom is obliged to comply with the provisions of the Occupational Health and Safety Act and the Critical Infrastructure Protection Act. The safety of people, the integrity of assets and information are key priorities in enabling Eskom to meet its obligations and deliver on its mandate.

Due to the constant changes in the risk profiles of Eskom assets and installations, the review of physical security measures is necessary to ensure that current threats are appropriately mitigated, through the implementation of suitable site-specific protection measures, systems and procedures.

This document provides an overview of National Transmission Company South Africa (NTCSA) scope of work for a commercial enquiry to establish national enabling agreements with physical security suppliers for the supply, design, installation, refurbishment, maintenance, support and services of an integrated physical security system in the NTCSA Grids and Telecoms. The System shall be an integration of the CCTV system, intruder detection system, Integrated Access Control System (IACS), alarm system, public address (PA) system and the Physical Security Information Management (PSIM) system.

*Note: In this document NTCSA and Eskom shall refer to the same entity.*

## **2. Supporting Clauses**

### **2.1 Scope**

#### **2.1.1 Purpose**

The document stipulates the technical scope of work for the Integrated physical security system contract for NTCSA Grids and Telecoms.

#### **2.1.2 Applicability**

This document shall apply to the integrated physical security system contract enquiry process for NTCSA Grids and Telecoms.

#### **2.1.3 Effective date**

The authorisation date.

### **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

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- [4] 240-86738968 Specification for Integrated Security Alarm System for Protection of Eskom Installations and its subsidiaries
- [5] 240-170000098 Security Public Address Systems for Substations and Telecoms high sites
- [6] 240-170000096 Physical security integration standard
- [7] 240-171000068 Technical Evaluation Criteria for the Integrated Physical Security System enquiry
- [8] 240-60725641 Specification for Standard (19 inch) Equipment Cabinets
- [9] 240-46264031 Fibre-Optic Design Standard – Part 2: Substations
- [10] DEM2412993 & 2425114 LAD (Logical Architecture Definition) PAC (Physical Application Component) for Physical Security Information Management System (PSIM)
- [11] Business Requirement Specification DEM\_2412993 & 2425114 Tx and ET Security Monitoring System
- [12] 240-170000723 Generic technical requirements for Physical Security Technologies Contracts
- [13] 240-170000691 Standard for Intrusion Pre-detection System used at Eskom sites
- [14] 240-118870219 Standby Power Systems Topology and Autonomy for Eskom sites
- [15] 240-53114248 Thyristor and Switch Mode Chargers, AC/DC to DC/AC Converters and Inverter/Uninterruptible Power Supplies Standard
- [16] 240-64139144 AC Boards and Junction Boxes for Substations
- [17] 240-55410927 Cyber Security Standard for Operational Technology
- [18] 32-373 Information Security – IT/OT and Third Party Remote Access Standard
- [19] 240-79669677 Demilitarised Zone (DMZ) designs for Operational Technology
- [20] 32-85 Information Security Policy

### **2.2.2 Informative**

- [21] 240-78980848 Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom installations and its subsidiaries
- [22] 240-139282493: Security Lighting for Eskom Applications

### **2.3 Definitions**

Definition	Description
<b>Tender</b>	A tender refers to an open or closed competitive request for quotations / prices against a clearly defined scope / specification.

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

### 2.3.1 Disclosure Classification

**Controlled disclosure:** controlled disclosure to external parties (either enforced by law, or discretionary).

## 2.4 Abbreviations

Abbreviation	Explanation
CCTV	Closed Circuit Television
IACS	Integrated Access Control System
NTCSA	National Transmission Company South Africa
PA	Public address
PSIRA	Private Security Industry Regulatory Authority
PSIM	Physical Security Information Management
Tx	Transmission

## 2.5 Roles and Responsibilities

As per PTM&C technology development standard (240-83684419)

## 2.6 Process for Monitoring

Not applicable

## 2.7 Related/Supporting Documents

### 2.7.1 Reference drawings

Not applicable

## 3. Scope of work

### 3.1 General

- The Supplier shall supply, design, install, refurbish, maintain, support and provide services for the Integrated Physical Security System in the NTCSA Grids and Telecoms “on an “as and when required” basis for the duration of the contract.
- The integrated physical security system shall comprise of the CCTV system, intrusion pre-detection system, IACS, alarm system, public address (PA) system, integration, and the Physical Security Information Management (PSIM) system.
- CCTV system shall comply to requirements of 240-91190304.
- Access control system shall comply to requirements of 240-102220945.
- Alarm system shall comply to requirements of 240-86738968.
- Intrusion pre-detection system shall comply to requirements of 240-170000691.
- Public address shall comply to requirements of 240-170000098.

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- h) The PSIM system shall comply to requirements of DEM2412993 & 2425114 (LAD and BRS).
- i) The subsystems listed above shall be integrated as per 240-170000096.

*Notes:*

*The words Supplier and Tenderer are used interchangeably in this document.*

### **3.2 Accreditation**

- a) Accreditation of Suppliers shall comply with requirements stipulated in section 3.1 of 240-170000723.

### **3.3 Experience and Expertise**

- a) Experience and expertise for Suppliers shall comply with requirements of section 3.1.2 of 240-170000723.

### **3.4 Supplier's obligations**

- a) Supplier's obligations shall be as stipulated in section 3.2 of 240-170000732.

### **3.5 Product Design and Engineering**

#### **3.5.1 Design artifacts**

- a) Suppliers shall produce design artifacts, and these shall comply to requirements of section 3.3.2 of 240-170000723.

#### **3.5.2 Design assurance**

- a) Suppliers shall provide design assurance services, and these shall comply to requirements of section 3.3.3 of 240-170000723.

#### **3.5.3 Design Engineering**

- a) Suppliers shall provide design engineering services, and this shall comply to requirements of section 3.3.4 of 240-170000723.

*Note: The maintenance standard will be developed by the appointed suppliers post contract award through Eskom processes.*

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

#### **3.5.4 Application**

- a) Suppliers shall provide application design services, and these shall comply to requirements of section 3.3.5 of 240-170000723.

#### **3.5.5 Equipment and Product Profile**

- a) Suppliers shall provide equipment and product profiles, and these shall comply to requirements of section 3.3.6 240-170000723.

#### **3.6 Supply and delivery**

- a) Suppliers shall provide supply and delivery services, and these shall comply to requirements of 3.4 of 240-170000723.

#### **3.7 Support Services**

- a) Suppliers shall provide support services for all product(s), equipment and/or solutions offered. These shall comply to requirements in section 3.6 of 240-170000723.

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.



### **3.8 Equipment evaluation**

- a) Suppliers shall provide equipment for evaluation, these shall comply to requirements of section 3.7 of 240-170000723.

### **3.9 Test equipment and tools**

- a) Test equipment and tools shall comply to requirements of section 3.8 of 240-170000723

### **3.10 Training**

- a) Suppliers shall provide training services, and these shall comply to requirements of section 3.9 of 240-170000723

### **3.11 Handbooks**

- a) Suppliers shall produce and submit handbooks as per section 3.10 of 240-170000723 post contract award.

### **3.12 Project Management**

- a) Suppliers shall provide project management services, these shall comply to requirement of section 3.11 of 240-170000723.

### **3.13 Installation and commissioning**

#### **3.13.1 General**

- a) The installation services shall be provided as per section 3.5 of 240-170000723.
- b) The Supplier shall cost for sites where a fully integrated system is required. This is for sites where all subsystems (i.e., alarm system, CCTV system, intrusion pre-detection system, PA system, IACS system & overall system integration) including interfacing to PSIM is required. The costing shall be based on typical scope for fully integrated Physical Security sites as per Annex C. Costing shall cover typical Tx substation site as per Figure D1 and as well as typical ET site as per Figure D2 in Annex D (associated drawings will be provided).
- c) The security threats at office and power network facilities are constantly evolving, while there will be standard design scenario for extremely high-risk sites, subsequent low risk sites may be subject to sporadic incursions which may require quick deployment solution to protect high risk boundaries permanently or temporally.
- d) The costing shall be on a per site basis and shall make provision for the typical project scopes outlined below. Site visits will have to be conducted by the Supplier to confirm and refine the scope of works with photographic evidence.
- e) Additional costing shall be provided for each of the installation modules under sections 3.13.2, 3.13.3, and 3.13.4 below.

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- f) All site level installations shall include the necessary networking equipment such as switches, routers, servers, software licences and interface(s) to the PSIM system at the remote security control room.

### **3.13.2 General strategic capability at the Remote Security Control Centre and Disaster Recovery (DR) site**

- a) Full deployment of centralized PSIM infrastructure shall be provided by the PSIM Supplier at the Remote Security Control Centre and the DR site.
- b) The PSIM system shall be sized to accommodate 500 substations and 500 telecoms sites including the common integration components below for Mobile Compact Surveillance sites and non-Substation sites.
- c) The PSIM shall include interface(s) to site level sub-systems with the required functionality/capability including (but not limited) to security control centre DMZ jump server(s) for running updates, PSIM local server licence(s), connection monitoring to site level, subsystems and devices. State synchronisation capability to sites after establishing connection and handling of events (fault, alarms etc.) from sites.
- d) Full deployment of a backup PSIM system at the DR site shall be provided by the PSIM Supplier. Suppliers shall propose the disaster recovery (DR) plan consisting of a procedure which outlines when and how the DR site will be activated in the form of a business continuity plan. Suppliers will be required to prove and demonstrate that their solution can be set-up and configured for a fully redundant application and infrastructure.
- e) Both the remote Security Control Centre and DR site shall have the necessary storage servers for storing security information (events and video recordings) from the monitored sites. Security recordings shall be kept for a month on the live system and stored for two years offsite (options include cloud storage, hard drives etc).
- f) All digital video recordings must be able to comply with the chain of evidence integrity in a court of law.

### **3.13.3 Wireless Vibration Perimeter Intrusion Detection (PID) system sites**

#### **3.13.3.1 General**

- a) Suppliers shall make provision for a Wireless Vibration Perimeter Intrusion Detection (PID) system for sites where a quick deployment detection system is required.
- b) The system must cover a perimeter of at least 2000m of high security mesh fence (It should be possible to deploy the system on concrete wall as well as diamond mesh fences).
- c) All sensor aggregation base station 3-meter poles must be hot dipped galvanized.
- d) The system configuration must ensure redundant communication routes to the guard house (or any building/structure serving a similar purpose).
- e) System components outside of the guard house (or any building/structure serving similar purpose) must be wireless, self-powered with appropriately sized solar panels.
- f) All non-battery components to have operating life of at least 10 years post manufacture discontinuation.

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

### **3.13.3.2 Substation Wireless Vibration Perimeter Intrusion Detection (PID) system Module**

- a) This Wireless Vibration Perimeter Intrusion Detection (PID) solution will be for substation sites where a quick deployment detection system is required.
- b) The base station shall be located approximately 20 m from the outer fence to be protected and a maximum of 1 km from the Guard house.
- c) Provision must be made for an HMI at the entrance of the guard house with a siren and strobe light.
- g) The system must integrate with the PSIM at the remote physical security control room via the Eskom's Telecommunications WAN.
- h) Suppliers shall make provision for a site network firewall, controller, and 12 hours battery standby at the guard house (or any building/structure serving similar purpose).

### **3.13.3.3 Non-Substation, Non-Eskom communication Vibration Perimeter Intrusion Detection (PID) system module.**

- a) This Wireless Vibration Perimeter Intrusion Detection (PID) solution will be for non-substation sites and/or for sites that do not use Eskom's Telecommunications WAN for offsite communication, where a quick deployment detection system is required.
- b) The solution must integrate with the PSIM at the remote physical security control room via a Non-Eskom WAN communication channel (alternatives may include Cellular, Sigfox, Narrowband-IOT).
- c) The costing for this solution must include a 12 month off site communication and cloud service, with the option of a month-to-month service plan thereafter for the duration of the framework agreement.
- d) Month-to-month extension for communication and cloud service to be costed separately.

### **3.13.4 Compact Surveillance system sites**

- a) Suppliers shall make provision for a Compact Surveillance system for sites where a quick deployment surveillance system is required.
- b) Fixed Compact Surveillance solution shall be self-powered (solar) standalone unit with east west fixed camera with day/night vision and intrusion analytics, PTZ, PA and fence vibration sensors for at least 100m perimeter section.
- c) All sensor aggregation base station 3-meter poles must be hot dipped galvanized.
- d) All non-battery components to have operating life of at least 10 years post manufacture discontinuation.

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

#### **3.13.4.1 Substation Fixed Compact Surveillance system module**

- a) This Compact Surveillance system is for Substation sites where a quick deployment surveillance system is required.
- b) The base station shall be located 20 m from the outer fence to be protected and a maximum of 1 km from the Guard house.
- c) The Supplier shall make provision must for an HMI at the entrance guard house with a siren and strobe light.
- d) For this system, assume that there will be line-of-sight between compact node and the Guard house.
- i) The solution must integrate with the PSIM at the remote physical security control room via the Eskom's Telecommunications WAN.
- j) Suppliers shall make provision for a site network firewall, controller, and 12 hours battery standby at the guard house (or any building/structure serving similar purpose).

#### **3.13.4.2 Non-Substation Fixed Compact Surveillance system module**

- a) This Compact Surveillance system is for will be for non-substation sites and/or for sites that do not use Eskom's Telecommunications WAN for offsite communication, where a quick deployment detection system is required.
- b) The solution must integrate with the PSIM at the remote physical security control room via a Non-Eskom WAN communication channel (alternatives may include Cellular, Sigfox, Narrowband-IOT).
- c) The costing for this solution must include a 12 month off site communication and cloud service, with the option of a month-to-month service plan thereafter for the duration of the framework agreement.
- d) Month-to-month extension for communication and cloud service to be costed separately.

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

### **3.13.4.3 Mobile Compact Surveillance module**

- a) This Surveillance system is for sites where a quick deployment compact mobile surveillance system is required.
- b) Suppliers shall make provision for a temporary HMI at the guard house/security equipment building with a siren and strobe light when this module is deployed at a substation.
- c) The components outside of the guard house/security equipment building must be wireless, self-powered with appropriately sized solar panels.
- d) For this solution, assume there will be line-of-sight between compact Surveillance node and the Guard house/security equipment building.
- e) This solution must integrate with the PSIM at remote physical security control room via the non-Eskom WAN communication (alternatives may include Cellular, Sigfox, Narrowband-IOT).
- f) The compact mast and all electronics must be installed on a legally compliant trailer not exceeding the requirements for an EB License code holder.
- g) The combo must include a 12 month off site communication and cloud service, with the option of a month-to-month service plan thereafter.
- h) Month-to-month extension for communication and cloud service to be costed separately.

## **4. Technical returnables and index**

- a) The index in Annex A of this document provides a guideline of how the technical returnables for this enquiry should be indexed by the Tenderers.
- b) The tenderer shall produce and submit a detailed design report for the Integrated physical security system as per the index in Annex B of this document.

## **5. Acceptance**

This document has been seen and accepted by:

<b>Name</b>	<b>Designation</b>
Cornelius Naidoo	Middle Manager – Telecoms & Physical Security T&S
Judith Malinga	Senior Manager – PTM&C

## **6. Revisions**

<b>Date</b>	<b>Rev.</b>	<b>Compiler</b>	<b>Remarks</b>
August 2024	3	R Moshoeshoe	Included Supplier Equipment Tendered Declaration form as part of technical returnables index guideline in Annex A
April 2024	2	R Moshoeshoe	Excluded information that is covered by the contract strategy
May 2023	1	R Moshoeshoe	First Issue

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

## **7. Development Team**

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

- Victor Lehobo
- Chris Van Reenen
- Phelokazi Ndlovu

## **8. Acknowledgements**

Not applicable

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

## **Annex A: Technical Returnables Index Guideline**

The index below is a guideline of how the technical returnables and supporting information should be indexed for this enquiry.

1. Valid PSIRA registration certificate.
2. Completed Supplier Tendered Equipment Declaration form as per Annex K of 240-171000068 including supporting information/evidence.
3. Completed Technical Schedules A/B related to 240-86738968 as per Annex A of 240-171000068 including supporting information/evidence.
4. Completed Technical Schedules A/B related to technical specification 240-91190304 as per Annex B of 240-171000068 including supporting information/evidence.
5. Completed Technical Schedules A/B related to technical specification 240-102220945 as per Annex C of 240-171000068 including supporting information/evidence.
6. Completed Technical Schedules A/B related to technical specification 240-170000098 as per Annex D of 240-171000068 including supporting information/evidence.
7. Completed Technical Schedules A/B related to technical specification 240-170000691 as per Annex E of 240-171000068 including supporting information/evidence.
8. Completed Technical Schedules A/B related to technical specifications DEM2412993 & 2425114 as per Annex F of 240-171000068 including supporting information/evidence.
9. Completed Technical Schedules A/B related to technical specification 240-170000096 as per Annex G of 240-171000068 including supporting information/evidence.
10. Completed Technical Schedule A/B related to specification 240-17000723 as per Annex H of 240-171000068 including supporting information/evidence.
11. Completed Technical Schedule A/B related to section 3.1 of specification 240-17000723 as per Annex I of 240-171000068 including supporting information/evidence.
12. Detailed design report as per index in Annex B of this document (240- 170001030)

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

## **Annex B: Detailed design report index for Integrated Physical Security System**

- a) Overview of functional specification
- b) Scope of work
- c) High Level Integration
  - 1) Local vs remote monitoring and control capabilities
  - 2) Software and network config files.
  - 3) Cause and effect matrices (e.g. if alarm on fence, lights and image sent to control)
- d) System Architecture (to include Logical and physical design, networking and bandwidth requirements, Information flow, Physical security information management, User access profile management and enrolment process, cyber security controls e.g. firewalls, DMZ, System support remote access authentication etc.)
- e) Lifespan of System and product software versions
- f) Recommended Maintenance (Procedures, Spares and FMECA- Failure mode effects and criticality analysis, tools and test equipment, training requirements-engineering and field operations)
- g) System commission and acceptance testing procedure (commissioning results to be provided prior to system handover (minimum tests as per 240-171000171).
- h) Annex A – Drawings
  - Site layout
  - Typical system Field of detection/view
  - Typical Site Security Zoning
  - System Configuration
  - Typical Security LAN and Fibre Reticulation
  - Typical Cable and trench layout
  - Power reticulation
  - Control Panels
- i) Annex B – Equipment Specification
  - Access Control system
  - Intrusion pre-detection system
  - CCTV system
  - Alarm system
  - Lighting Control System (if it is a separate controller)
  - PA system
  - Wireless Vibration Perimeter Intrusion Detection (PID) system
  - Compact Surveillance system

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.



- Physical security information management (PSIM) system
- Data storage equipment

j) Annex C – Datasheets

- Access Controllers
- Card Readers
- Biometric Readers
- Maglocks
- Break Glass Units
- Door Contacts
- Intrusion pre-detection Sensors
- Power Supplies (including UPS sizing)
- Intercoms
- Cameras
- Video Recorders
- Client Workstations
- Network Switches
- Fibre Converters
- Enclosures & Racks
- PA systems
- Security LAN and firewalls
- Wireless Vibration Perimeter Intrusion Detection (PID) system readers and controllers
- Compact Surveillance system readers and controllers

k) Annex D - Bill of Materials

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

## **Annex C: Typical installation scope for a Fully integrated Physical Security Site**

### **1. General Installation scope**

The scope includes requirements for an Integrated physical security system comprising of an Access Control System, CCTV system, Intrusion pre-detection system, alarm system, public address (PA) system and interfacing to the PSIM system (includes IT Infrastructure) for a fully integrated Physical Security Site. The Contractors shall provide the following installation services:

- a) Produce basic and detailed designs for the Integrated physical security system . The detailed design must include detailed designs for the Access Control System, CCTV system, Intruder detection system, alarm system, the public address system and the interfaces to PSIM system (includes IT Infrastructure). The design must also cover integration of these different systems and the NLEPDS (existing) into an Integrated physical security system .
- b) Installation and configuration of substation security LAN Infrastructure.
- c) Installation, configuration and commissioning of the CCTV system in totality on site as per Eskom standard (240-91190304).
- d) Installation, configuration and commissioning of the IACS in totality on site as per Eskom standard (240-102220945).
- e) Installation, configuration and commissioning of intruder detection system in totality on site as per Eskom standard (240-91190304, 240-86738968 & 240-170000096).
- f) Installation, configuration and commissioning of alarm system in totality on site as per Eskom standard (240-86738968).
- g) Installation, configuration and commissioning of public address system in totality on site as per Eskom standard (240-170000098).
- h) Installation, configuration and commissioning of intrusion pre-detection system in totality on site as per Eskom standard (240-170000691).
- i) Integration of IACS, CCTV system, Intruder detection system, alarm system, public address system into an Integrated physical security system (240-170000096) to interface with the PSIM system.
- j) Installation, configuration and commissioning of interfaces from subsystems to the Physical Security Information Management (PSIM) for data collection, incidents management, data correlation, controlling functionality (CCTVs, IACS systems, PA systems, etc.) and provision of real-time dash-board and reports.
- k) Conduct SAT tests before commissioning the complete integrated system.
- l) Compile site as built drawings with electrical and engineering detail.
- m) Create a Graphical User Interface (GUI) and behaviour models for the site.

### **2. Integrated Access Control System (IACS)**

- a) The Integrated access control system will be used to manage access rights of Eskom employees, visitors and contractors in and out of different areas at site.
- b) The system will also be used to grant and limit access permissions in and out of areas such as secure and non-secure areas.

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- c) The offered system shall comply with requirements of Specification for Integrated Access Control System (IACS) for Eskom sites (240-102220945).
- d) The system should support a tiered architecture which will allow monitoring of the site both locally and remotely comprising of field devices (biometric & card readers) at site level and system management servers at the remote security control room (zero control).

## 2.1 IACS devices layout

The envisaged integrated Access Control devices for the site and their locations are shown in Table 1 below:

**Table 1: IACS readers positioning**

Area	Point	Device	Status Contact	Lock	Evacuation Device	Bypass
Main Gate (Inbound traffic)	Exterior Perimeter Fence (Gooseneck Mount)	Card Reader	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
	Energized Fence Gate	Integrated with exterior gate automation	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
	Inner Perimeter Fence (Gooseneck Mount)	Card + Biometric Reader	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
Outbound Traffic	Exterior Perimeter Fence (Gooseneck Mount)	Card + Biometric Reader	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
	Energized Fence Gate	Integrated with interior gate automation	Gate Status Contact	Electro Mechanical Lock	None	Mechanical Bypass
	Inner Perimeter Fence (Gooseneck Mount)	Card Reader	Gate Status Contact	Electro Mechanical Lock	Emergency Exit Button	Mechanical Bypass
Guard House	Entrance Door	Card + Biometric Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Equipment Room Door (Inside)	Card + Biometric Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
Control Room Buildings	Office Door	Card Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

Area	Point	Device	Status Contact	Lock	Evacuation Device	Bypass
(	Control Room Entrance Door	Card + Biometric Reader	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Control Room Back Door (Emergency Exit)	Emergency exit break-bar	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Control Room Double Door	Card Reader (Inside only)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Battery Room	Card + Biometric (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Carrier Room	Card + Biometric (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
Office buildings & store rooms	Main entrances	Card + Biometric (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass

## 2.2 IACS high level devices positioning and architecture philosophy

- The contractor will be 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 principles outlined in the technical standards for IACS
- In addition to ensuring that the installed system operates as required on site, the contractor will also be required to ensure that the system enables remote monitoring and control through the Eskom's WAN.

## 3. CCTV system

- A CCTV system shall be installed and the proposed system for the site 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 energized 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.
- The offered system shall comply with requirements of Eskom standard for CCTV system (240-91190304).
- It is proposed that static thermal cameras with video motion detection be installed along the perimeter of the Substation to provide both surveillance and detection functionality. In addition it is proposed that PTZ cameras be installed for zooming and recognition functionality.

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- d) The CCTV system shall be connected to the site security LAN and Eskom WAN to enable event driven video streaming to the local and remote security control rooms.
- e) 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. The purpose of this unit is to enable the security control room to interact with unannounced visitors and non-Eskom staff. The communication will be point-to-point between the gate and the security control room and will not be integrated with the gate control system.
- f) The contractor shall determine the required camera lens types that will ensure that the positioning of the cameras results in the most optimised and economical installation of the cameras at site. This includes ensuring that a 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.

### **3.1 CCTV System devices layout and positioning**

The areas identified where CCTV devices (cameras) are to be installed are listed in Table 2 below. The cameras are to be positioned as per the site layout.

**Table 2: CCTV cameras positioning**

Area	Site location	Device(s)
Perimeter and Main Access Gate	Perimeter fence	Static thermal Cameras
		PTZ Cameras
	Access Gate	Static Cameras
		Video Intercom
Control Room Building	Guard House	Interior Static Cameras
	Outside Battery Room entrance	Exterior static Cameras
	Control Room Door	Interior Static Cameras
	Control Room Emergency Exit	Interior Static Cameras
	Control Room Double Door	Exterior Static Cameras
Office buildings & store rooms	Carrier Room	Interior Static Cameras
	Main entrances	Exterior Static Cameras

### **4. Intruder Pre-detection system**

- a) Intrusion pre-detection units shall be installed in all areas of the substation including buildings, rooms and substation perimeter area which need to be protected.
- b) The sensors shall be placed so as to effectively detect intrusion into the protected (secured) areas for the following:
  - i. Unauthorised movement around/inside a protected area at site
  - ii. Tunnelling underneath the fences,

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- iii. Separation of electric fence conductors,
  - iv. Cutting and climbing over perimeter barrier fences/walls,
  - v. Vibrations caused by Digging underneath, breaking through and climbing over the barrier fences/walls.
- c) 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).

#### **4.1 Intrusion Pre-detection system devices layout and positioning**

**Table 3: Intrusion Pre-detection System devices positioning**

Area	Point	Device(s)
Guard House	Server Room	Interior PIRs
Control Room Buildings	Outside Office Door	Door Contact
	Office Interior	Interior PIRs
	Battery Room Door	Door Contact
	Battery Room	Interior PIRs
	Control Room Door	Door Contact
	Control Room Emergency Exit	Door Contact
	Control Room	Interior PIRs
	Building interior	Interior PIR
Office buildings & store rooms	Main entrances	Door Contact
Substation Perimeter	On each perimeter camera	Intrusion detection analytics
Substation Perimeter	Outer wall/barrier fences	Exterior intruder pre-detection system (Contractor to propose a system)

#### **5. Public Address System**

- a) The installation of a PA system is required in order to engage potential intruders and issue warnings.
- b) The PA system shall be able to be remotely and locally operated when necessary.
- c) The system must be operable via the guard house and remotely via the responsible control rooms to warn would be attackers of the restriction of access to the site.
- d) Voice recordings shall be synchronized with the cameras and recorder on the local NVR via a suitable audio input to ensure synchronization of events.
- e) The installed PA system shall comply with the requirements of technical specification for Public Address Systems (240-170000098).

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

## 5.1 PA system devices layout and positioning

- a) The speakers shall be mounted on the existing perimeter light masts around the site perimeter where feasible.

## 6. Alarm system

- a) The alarm system shall be installed and will form an integral part of the other security systems installed at site to provide proactive coverage and monitoring of all protected areas i.e. Site perimeter, entrances, buildings, HV yard and other strategic places within the substation. The alarm system shall be triggered by the following inputs:
- i. Due to Camera video analytics alarm detection on the zone(s).
  - ii. Alarm inputs from electric fence.
  - iii. Alarm inputs from Intrusion pre-detection devices.
  - iv. Alarm inputs from access control points.
- b) The installed alarm system shall comply with the requirements of 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 physical security system at site.

## 7. System integration

- a) The subsystems outlined above are required to be integrated into an onsite unified integrated physical security system in line with Eskom's technical specification for security systems integration (240-170000096).
- b) The integrated system shall achieve the cause the effect matrix requirements in the table below:

**Table 4: Integrated Physical Security System Cause and Effect matrix**

	Unauthorised Access					Authoris ed Access
	Breach physical perimeter fence or virtual perimeter fence by smart cameras/ beams/etc.	Outdoor Sensor Triggers	Camera Outdoor Protected Area Triggers	Indoor Sensor Triggers	Camera Indoor Protecte d Area Trigger	
Perimeter flood lights activated at night only	✓					

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

	Unauthorised Access					Authoris ed Access
	Breach physical perimeter fence or virtual perimeter fence by smart cameras/ beams/etc.	Outdoor Sensor Triggers	Camera Outdoor Protected Area Triggers	Indoor Sensor Triggers	Camera Indoor Protecte d Area Trigger	
Substation flood lights activated at night only	✓	✓	✓	✓		
Security floodlights activated at night only	✓	✓	✓	✓		
Control Room lights 24hr				✓	✓	
Switch Room lights 24hr				✓	✓	
Any other indoor room				✓	✓	
DVR/NVR record footage	✓	✓	✓	✓	✓	✓
Alarm signals(text and video) sent to Security Control Centre	✓	✓	✓	✓	✓	
PTZ tracking sent to Security Control	✓	✓	✓			
PA System recorded message activated	✓			✓	✓	
PA System Security Control operated if positive alarm verified	✓	✓		✓	✓	
Alarm System Zones triggered	✓	✓	✓	✓	✓	
Alarm Zone events sent to Security Control	✓	✓	✓	✓	✓	
Indoor Siren automatically activated				✓		
Strobe light automatically activated	✓	✓	✓	✓	✓	

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.



## **8. Site monitoring**

- a) There shall be a security manager workstation at site in the security building for local allocation and revoking of access rights and controlling of security workflows.
- b) There shall be a maintenance manager workstation in the security building for controlling of maintenance workflows.
- c) Some or all of the functions listed in item (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 item (a) and (b) above.
- d) The security alarms and CCTV visuals should be routed to remote Security Control Centre through the Eskom WAN.
- e) The system shall allow the remote Security Control Centre to be able to remotely control PTZ cameras at site.
- f) The system shall allow the remote Security Control Centre to have audio (via PA system) and data communication with the site. Including the ability to give audio warnings over the PA system to the security zone that detected an intrusion.
- g) It shall be possible for the Security Control Centre to remotely retrieve any of the stored event data or video streams in real time.

## **9. Communication**

- a) The network shall provide redundancy in the event of path failure.
- b) Single mode optical fibre is preferred as the physical transport medium of choice for on-site communication. The installation shall conform to Eskom standard, 240-46264031.
- c) For indoor connections and outdoor connection distances below 5m, CAT5e/CAT6 UTP copper cable may be used.
- d) The detailed design shall include the security LAN design used to facilitate communications between security system elements.
- e) The IT Infrastructure (LAN, cabling, servers, etc.) design shall be detailed in the IT documentation.

## **10. PSIM requirements**

- a) The Suppliers for subsystems shall install, configure and commission integration point(s) for subsystems at site as per Physical security integration standard (240-170000096) to interface to the PSIM.
- b) The PSIM Supplier shall install, configure, and commission interfaces and accompanying infrastructure to integrate the subsystems installed at site and the PSIM system at the remote Security Control Centre.
- c) Suppliers shall include a once-off cost for development of PSIM interfaces that will follow a typical process outlined in Annex E of this document.
- d) The interfaces shall comply to requirements of the LAD and BRS (DEM\_2412993 & 2425114) and shall enable the following functionality (at minimum):

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- i. Local integration server/capability located at the substation which integrates to all security systems using industry protocols.
- ii. A database server/capability which manages all incoming events and incidents and other configuration data where required.
- iii. A storage device which is used as a back-up, primarily used to record video surveillance from cameras.
- iv. The system shall allow users to remotely access the Substation physical security information system based on a role-based access control method. It shall also allow remote operators to access functional capabilities of the solution upon demand and execute on a response strategy which may be automated or based on human intervention.

## **11. Power supply requirements**

- 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, so as to isolate the supply of the subsystems by means of appropriately sized MCBs. At a minimum, the following will be on separate supply circuits:
  - i. Perimeter Cameras
  - ii. Indoor cameras
  - iii. PA system devices
  - iv. Alarm panel
  - v. Intruder pre-detection devices
  - vi. Access Control system devices
  - vii. Site controllers and server-based equipment
  - viii. Other security related equipment such as gate motors and electric fence energizers.
- c) The system shall have a power failure indication that shall be sent through to the remote security control room should the supply be interrupted.
- d) The existing power systems at site shall be used as the primary power sources, provided that the standby time (autonomy) requirements of the site are not adversely affected.
- e) Security systems are required to ensure that the site is protected at all times, hence the standby time of these systems shall be in line with the overall required standby time for the site. The requirements of Eskom's DC systems and Standby Power Systems standards shall be adhered to.

## **12. Cabling and trenching**

- a) The contractor shall provide detailed as built drawings indicating cable routes, installation locations of all equipment as part of the detailed design submission.

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- b) The contractor will be responsible for laying and terminating the cable from the peripheral devices to the control room.
- c) Data and low voltage cable installations shall be separated from the mains power installations by a minimum of 500mm.
- d) Where data and low voltage cabling has to cross power cabling, this shall always be at 90°
- e) All wiring shall be concealed inside trunking or conduit. No exposed wiring will be accepted.
- f) Cable runs next to devices that may cause electro-magnetic interference shall be avoided or suitable shielding provided.
- g) Tension when pulling cables shall not exceed recommended safe values as specified by the cable manufacturers.
- h) Supply and installation of all trunking, conduit, glands etc. form part of the contractor's scope of work.
- i) Cable joints shall be avoided as far as practically possible.
- j) An industry acceptable Source, destination cable marking system shall be used to mark all cables.

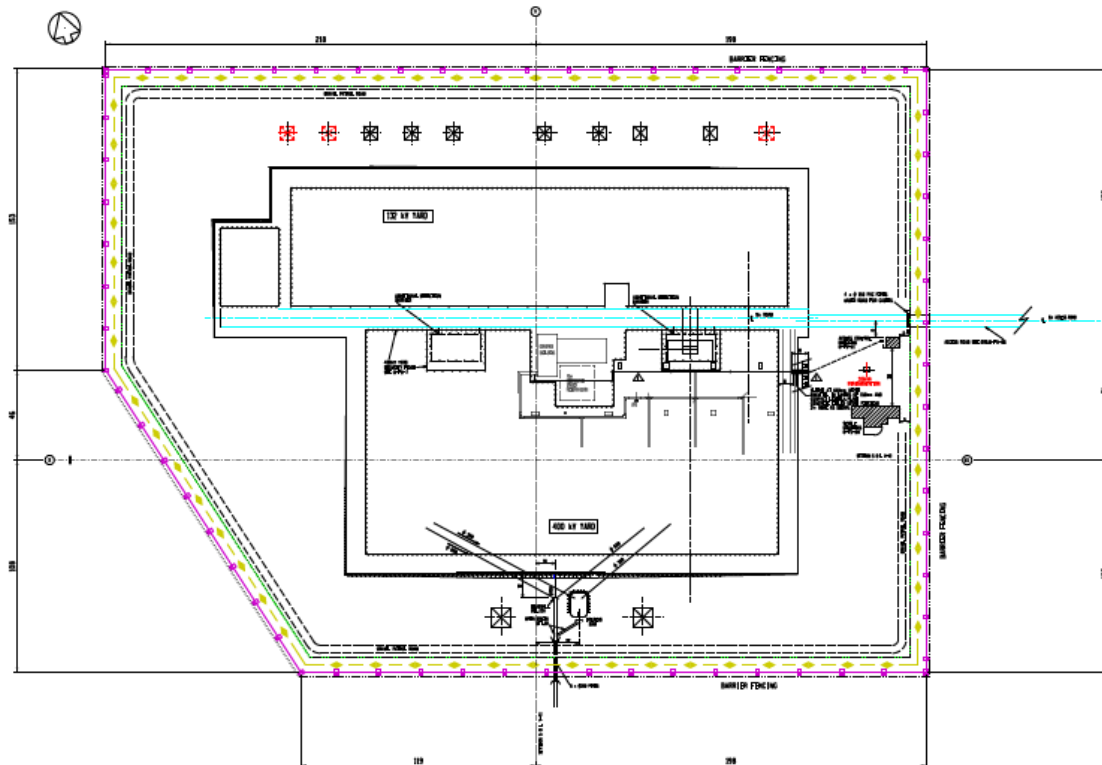
**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

## Annex D: Typical site layouts

The typical site layouts below should be used for costing and site zoning purposes:

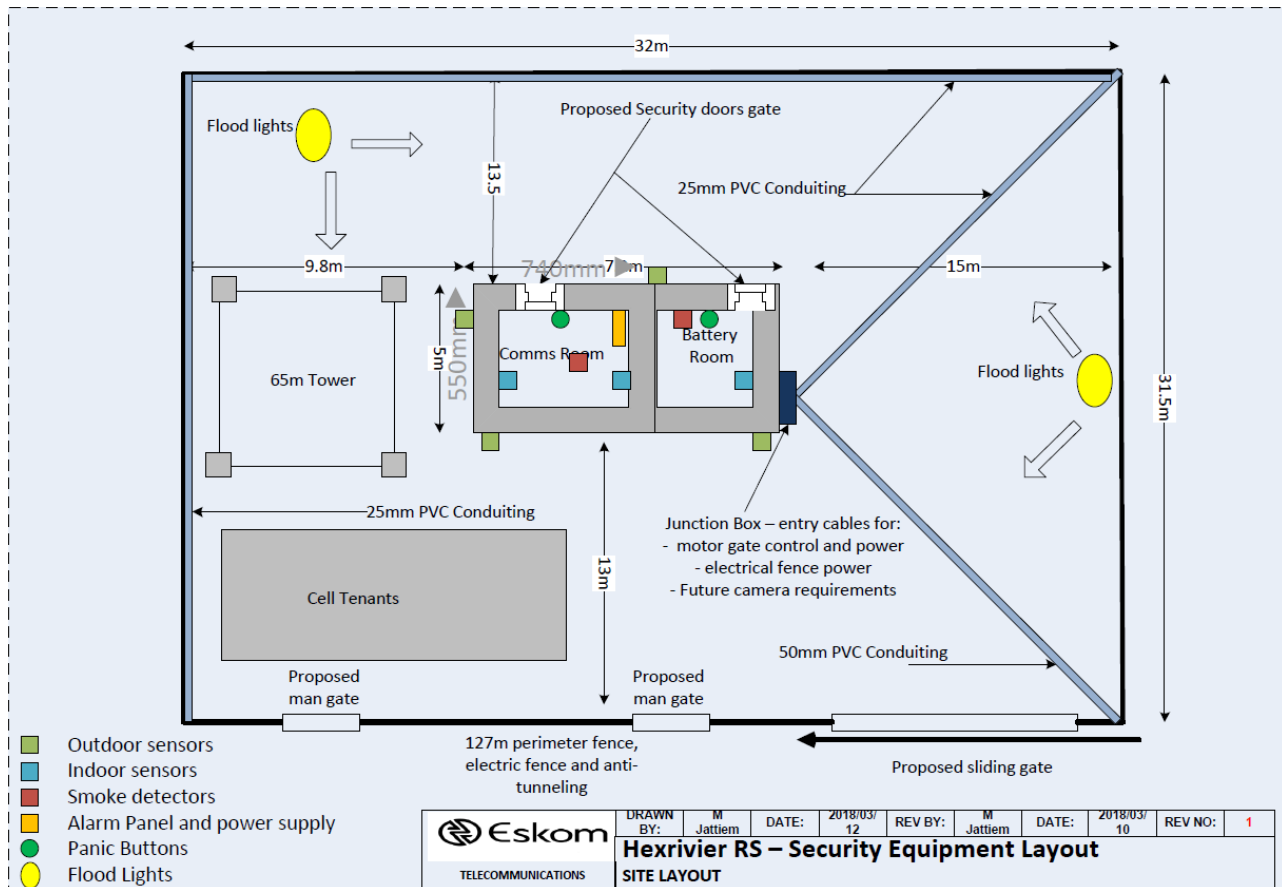


**Figure D1: Typical Tx Substation site layout (refer to drawing THE22P02-SE-42)**

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.



**Figure D2: Typical ET site layout**

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

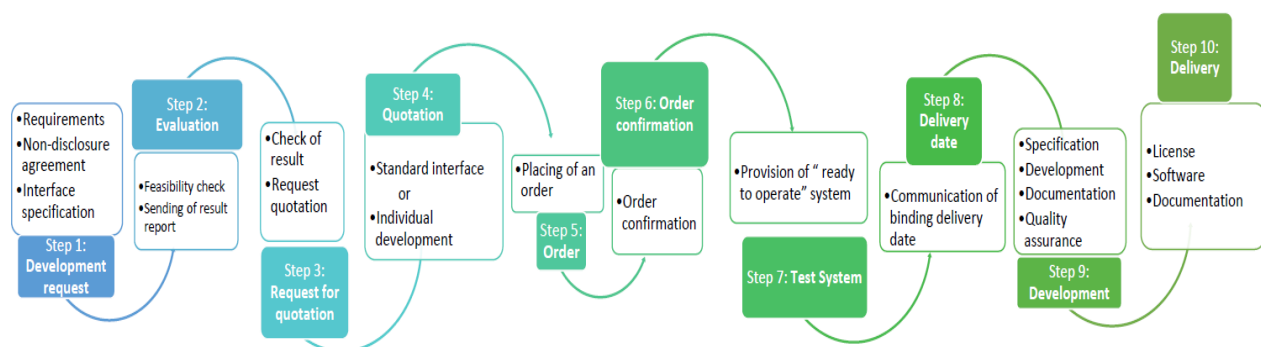
## Annex E: PSIM interfaces development typical process

### 1. Introduction

The Physical Security Information Management (PSIM) system and its centralised infrastructure will be installed at the Security Control Centre and backup (disaster recovery) site. This guideline is a typical process that will be followed by the Supplier(s) of the subsystems (CCTV, IACS, PIDS, PA, alarm system), PSIM Supplier and PSIM OEM to develop interfaces between the subsystems systems to the PSIM system to standardise and streamline the monitoring infrastructure optimally.

### 2. PSIM interfaces develop process

- a) The figure below shows the typical once off process that will be followed by the Suppliers of the subsystems (CCTV, IACS, PIDS, PA, alarm system), the PSIM Supplier and the PSIM OEM for provision/development of interfaces to link site level subsystems to the PSIM system at the remote Security Control Centre. Tenderers shall include a once-off associated cost of all the works included in this process in their costing. The appointed Supplier for the PSIM shall project manage this process and communication between the appointed Suppliers/Contractors of the subsystems and the PSIM OEM.



#### RACI

Responsible party	Steps
Contractor	1, 3, 5, 7,
PSIM OEM	2, 4, 6, 8, 9, 10

**Figure 1: Typical process for PSIM interfaces development**

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- b) The table below shall be populated to provide details for the subsystems and associated devices to start the evaluation process depicted above.

Subsystem	Vendor	Model	Panel/Device Qty.
CCTV system			
Alarm system			
Intrusion pre-detection system			
Access Control system			
Public address system			
Site Integration system (where applicable)			
Wireless Vibration Perimeter Intrusion Detection (PID) system			
Compact Surveillance system			
Other			

*Note: The use of the terms 'Suppliers of the subsystems' and 'the PSIM Supplier' are used in general terms and could refer to the same supplier.*

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.