

Title: **STANDARD FOR INTRUSION  
PRE-DETECTION SYSTEMS  
USED AT ESKOM SITES**

Unique Identifier: **240-170000691**

Alternative Reference Number: **n/a**

Area of Applicability: **Engineering**

Documentation Type: **Standard**

Revision: **1**

Total Pages: **30**

Next Review Date: **April 2027**

Disclosure Classification: **Controlled  
Disclosure**

---

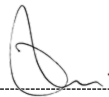
**Compiled by**



**Donald Moshoeshe**  
**Snr Engineer: PTM&C**

Date: 02/06/2022

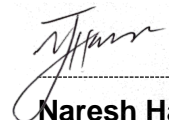
**Approved by**



**Nelson Luthuli**  
**Manager (Acting):  
PTM&C**

Date: 03 June 2022

**Authorized by**



**Naresh Hari**  
**General Manager:  
Transmission Engineering**

Date: 2022-06-06

---

**Supported by SCOT/SC**



**Nelson Luthuli**  
**Metering, DC & Security SC  
Chairperson**

Date: 03 June 2022

---

## Content

	Page
1. Introduction .....	3
2. Supporting clauses .....	3
2.1 Scope .....	3
2.1.1 Purpose .....	3
2.1.2 Applicability .....	3
2.2 Normative/informative references .....	3
2.2.1 Normative .....	3
2.2.2 Informative .....	4
2.3 Definitions .....	5
2.3.1 Disclosure classification .....	5
2.4 Abbreviations .....	5
2.5 Roles and responsibilities .....	5
2.6 Process for monitoring .....	5
2.7 Related/supporting documents .....	5
3. Requirements .....	5
3.1 General requirements .....	5
3.2 Principle of Operation .....	6
3.3 Housing and safety .....	6
3.4 System alarming and notifications .....	7
3.5 Communication .....	8
3.6 Cybersecurity .....	8
3.7 Cabling .....	9
3.8 Environmental operating Conditions .....	9
3.9 Power Supply .....	9
4. Management and Monitoring requirements .....	10
5. Support services .....	10
6. System Documentation .....	10
7. Design acceptance .....	11
8. Authorization .....	11
9. Revisions .....	11
10. Development team .....	11
11. Acknowledgements .....	11
Annex A – System Performance Calculation .....	12
Annex B – Technical Schedules A and B .....	13

## **1. Introduction**

Eskom has high value assets that are situated in different geographical areas scattered throughout the country. At most sites there is lack of perimeter pre-detection systems and hence the existing barriers can be penetrated undetected with relative ease. Some areas are high risk areas and it is necessary for Eskom to put measures to secure their assets and ensure the continuity of Electricity supply. The document is necessary to provide the specification for intrusion pre-detection systems for protection of Eskom sites.

## **2. Supporting clauses**

### **2.1 Scope**

This specification sets out the physical, technical and functional requirements for intrusion pre-detection systems for protection of Eskom sites and assets. This document stipulates requirements for intrusion pre-detection systems to detect intruders crossing a boundary of a protected site as well as to detect an intruder penetrating or moving inside a protected area.

The typical intrusion pre-detection systems covered by this specification include (but not limited to) systems such as the following:

- a) Optic Fibre with Artificial Intelligence
- b) Taut Wire System
- c) Vibration sensors
- d) Fibre optic wire sensors
- e) Strain sensitive cables
- f) Electric field sensors
- g) Active Infrared Detectors
- h) Passive Infrared Detectors
- i) Microwave / Radar / Microphone sensors

**Note:** Tenderers may propose alternative systems which conforms to the requirements outlined in this specification for Eskom's approval. Eskom's Technical evaluation Team (TET) will evaluate the suitability of the proposed system in meeting the requirements. Eskom reserves the right to choose the preferred technology.

#### **2.1.1 Purpose**

The purpose of the document is to stipulate physical, technical and functional requirements for intrusion pre-detection systems for protection of Eskom sites.

#### **2.1.2 Applicability**

This document shall apply to Eskom Transmission Division.

## **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] 240-170000723 Generic Technical Requirements for Physical Security Technologies Contracts
- [3] 240-91190294 DC and Auxiliary Supplies Philosophy

**COPYRIGHT PROTECTED**

- [4] 240-118870219 Standby Power Systems Topology and Autonomy for Eskom Sites
- [5] 240-86738968 Specification for integrated security alarm system for protection of Eskom installations and its subsidiaries
- [6] 240-46264031 Fibre-Optic Design Standard – Part 2: Substations
- [7] 240-55410927 Cybersecurity Standard for Operational Technology
- [8] 32-273 Information Security – IT/OT and Third-Party Remote Access Standard
- [9] 240-79669677 Demilitarised Zone (DMZ) Designs for Operational Technology
- [10] SANS 60839-1-3, Alarm systems Part 1: General requirements Section Three: Environmental testing
- [11] SANS 2220-1-1, Electrical Security Systems, Part 1-1, Intruder alarm systems – General requirements
- [12] SANS 2220-1-6, Electrical Security Systems, Part 1-6, Intruder alarm systems- Passive Infra-red detectors for use in buildings
- [13] SANS 2220-1-7, Electrical Security Systems, Part 1.7: Intruder alarm systems: Power units
- [14] SANS 60839-2-3, Alarm system Part 2: Requirements for intruder alarm systems, Section Three – requirements for infrared beam interruption detectors in buildings
- [15] SANS 60839-2-4, Alarm systems Part 2: Requirements for intruder alarm systems Section 4: Ultrasonic Doppler detectors for use in buildings
- [16] SANS 60839-2-5, Alarm systems Part 2: Requirements for intruder alarm systems Section 5: Microwave Doppler detectors for use in buildings
- [17] SANS 60839-2-6, Alarm systems Part 2: Requirements for intruder alarm systems Section 6: Passive infra-red detectors for use in buildings

### **2.2.2 Informative**

- [18] 240-170000156, Anti-Theft vibration sensor and Alarm System
- [19] 240-86738968, Specification for Integrated Alarm System for protection of Eskom Installations and its subsidiaries
- [20] 240-170000096, Physical Security Integration Standard
- [21] 240-78980848, Standard for Non-lethal energized Perimeter Detection System (NLEPDS) Electrical Components
- [22] 240-102220945, Specification for Integrated Access Control System (IACS) for Eskom Sites
- [23] 240-91190304, Specification for CCTV surveillance with Intruder Detection
- [24] 240-170000098, Security Public Address Systems for Substations and Telecoms High Sites
- [25] 240-106871262 Physical Security Systems Technology Roadmap
- [26] 240-56360086 – Stationary Vented Nickel Cadmium Batteries Standard
- [27] 240-56360034 – Stationary Vented Lead Acid Batteries Standard
- [28] 240-51999453 – Standard Specification for Valve-Regulated Lead Acid Cells
- [29] 240-53114248 – Thyristor and Switch Mode Chargers, AC/DC to DC/AC Converters, and Inverter/Uninterruptible Power Supplies Standard
- [30] 240-64139144 – AC Boards and Junction Boxes for Substations
- [31] 240-76628687 – AC/DC Reticulation Equipment for Breaker-and-a-Half Substations
- [32] 240-75658628 – Distribution Group’s Specific Requirements for AC/DC Distribution Units

**COPYRIGHT PROTECTED**

## 2.3 Definitions

### 2.3.1 Disclosure classification

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

## 2.4 Abbreviations

Abbreviation	Description
AC	Alternative Current
DC	Direct Current
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PSIM	Physical Security Information Management System
SABS	South African Bureau of Standards
UPS	Uninterrupted Power Supply

## 2.5 Roles and responsibilities

- a) The Security Technologies Care Group shall ensure that the technology developed is adequate for application across Eskom sites where it will be utilized.
- b) Group security shall be responsible for auditing to ensure compliance with the requirements of this standard.
- c) The procurement team shall utilise this document for the enquiry process for intrusion pre-detection systems.

## 2.6 Process for monitoring

This document will be monitored through the SCOT process.

## 2.7 Related/supporting documents

Not applicable.

## 3. Requirements

### 3.1 General requirements

- a) Intrusion pre-detection systems will be used to provide pre-detection at all strategic areas at site as identified by Eskom including site perimeter, entrances, control rooms, battery rooms, HV yard , store rooms etc.
- b) The system shall provide intrusion pre-detection for the following (but not limited to):
  - 1) Unauthorised movement around/inside a protected area at site
  - 2) Tunnelling underneath the fences,
  - 3) Separation of electric fence conductors,
  - 4) Cutting and climbing over perimeter barrier fences/walls,
  - 5) Vibrations caused by Digging underneath, breaking through and climbing over the barrier fences/walls.

**COPYRIGHT PROTECTED**

- c) Where mode of operation depends on line of sight, this must be kept clear of all obscuring objects.
- d) Where mode of operation depends on vibrations, the system shall not be susceptible to nuisance alarms due to passing vehicles/trucks.
- e) The system should have a capability to log at least 1000 events in a memory using First-In-First-Out method for overwrite.
- f) The system shall have a zoning capability for alarm monitoring and fault finding.
- g) The system shall return to its normal non-alarm condition within 10s after an alarm signal is generated and acknowledged.
- h) All system components shall be synchronized with a real-time clock with minimum accuracy of 250ms.
- i) Depending on the mode of detection, the weight of the object that may trigger an alarm shall be configurable.
- j) Depending on the mode of detection, the height of the object that may trigger an alarm shall be configurable.
- k) Depending on the mode of detection, the depth from ground surface of the object that may trigger an alarm shall be configurable.
- l) Depending on the mode of detection, the linear range of the object that may trigger an alarm shall be configurable. Minimum is 300 meters.
- m) The system shall cover the entire protected area, the size/area of the protected site shall be configurable. Typical area is 120 000 m<sup>2</sup>.
- n) Depending on the mode of detection, the frequency and level of the vibration that may trigger an alarm shall be configurable.
- o) There shall be a mechanism to reduce/eliminate false alarms, the supplier shall demonstrate how false alarms are reduced/eliminated.
- p) The system life cycle of the proposed product must be a minimum of 10 years.
- q) Mode of operation shall not be limited by different light conditions (e.g., day vs night conditions).
- r) The maximum dimensions (number, size, length, etc) of the sensors/detection units shall be variable to suit site specific requirements.

### **3.2 Principle of Operation**

- a) Tenders shall include detailed technical information and principles of operation of their system offered. Failure to do so may render their tender incomplete.
- b) The overall performance (O) of each security system during operation shall be monitored on a monthly basis and kept above 88% when calculated as outlined in Annex A:
  - 1) System availability, which should be greater than 98%
  - 2) System dependability, which should be greater than 95%
  - 3) Overall performance (O) shall be greater than 88%
  - 4) If overall performance falls below 88% then remedial action must be taken and the system shall be self-healing.

### **3.3 Housing and safety**

- a) System units shall be sealed to prevent insects from interfering with their normal operation.
- b) Housing for system units to be frost and dew resistant and fitted with an anti-tamper facility.

**COPYRIGHT PROTECTED**

- c) It shall not be possible to alter the enclosure arrangements of the detector or to change its existing area of detection coverage or detection range without causing an alarm condition.
- d) It shall not be possible to disable the tamper detection device by means of normally available tools such as knives or screwdrivers.
- e) Housing for system units shall have an IP rating of IP65 or higher.
- f) Material of the housing units must be UV stable for at least 10 years.
- g) Housing shall not hinder/interrupt wireless communication signals to/from the units where applicable.
- h) Any container for batteries shall be so constructed that the battery terminals are protected against inadvertent contact with metal parts.
- i) A power unit for the system shall be so constructed that electronics and electrical circuits are protected against hazards caused by battery charging, accidental electrolyte spillage, fumes or explosive gas.
- j) The mechanical construction of any part of the system shall be such that injury caused by mechanical instability or by moving parts, protruding or sharp edges is prevented.
- k) Enclosures shall be so constructed and mounted such that electrical tests and operations are possible without the removal of the devices from their mounting.

### **3.4 System alarming and notifications**

- a) System alarming shall comply with requirements of 240-86738968, specification for integrated security alarm system for protection of Eskom installations and its subsidiaries.
- b) The Intrusion pre-detection system shall allow for the signalling of the following alarm conditions to a central monitoring point locally and remotely from the site:
  - 1) Intrusion pre-detection alarms
  - 2) Equipment fail alarm (health check, mains supply fail, battery low)
  - 3) Tamper detection
  - 4) Signal processing interference failure
- c) For each alarm notification, the following information shall be disseminated to the monitoring/viewing stations:
  - 1) Type of event (System, Incident, or Administrative).
  - 2) Date and time of the event in format CCYY/MM/DD; hh:mm:ss.
  - 3) Name/identification of the reporting device.
  - 4) Location of the reporting device in the form of GPS coordinates. Accuracy of the location shall be within 10-meter radius from the device.
- d) The alarms shall be viewable both onsite and remotely.
- e) The system shall be interoperable with existing alarming system(s) at site.
- f) The system shall resume its normal non-alarm condition within 10s after restoration from an alarm state.
- g) The system shall be immune to nuisance alarms due to small targets such as birds.
- h) The detection range and sensitivity of the detectors shall be configurable.
- i) The system shall sustain the alarm state until the controller has acknowledged a receipt of the intrusion alert on the Data Monitoring System.
- j) There shall be a graphical user interface (GUI) with site zones and aggregation of the system data.

**COPYRIGHT PROTECTED**

- k) Alert notifications/alarms shall be colour coded (e.g. yellow, green, orange, red, etc.) on the GUI to indicate the status and criticality of the alert/alarm.
- l) The system shall have intelligence to eliminate nuisance alarms due to vibrations, shadows and noise caused by passing cars, airplanes etc.

### **3.5 Communication**

- a) Single-mode optical fibre shall be the preferred physical transport medium due to the high EMC environment at substations. The fibre requirements shall comply with the standard 240-46264031 ("Fibre-Optic Design Standard – Part 2: Substations").
- b) Eskom Telecommunications shall be a default means of communication for off-site communication, where Eskom Telecoms has no presence, the supplier shall provide alternative communication.
- c) The system shall allow for wireless sensor connection to an onsite central hub or cellular connectivity to onsite hub or Security Operations Centre.
- d) The system shall be ICASA approved.
- e) Supplier to ensure communication in areas where cellular coverage is known to be minimal and/or not available. The supplier to provide ICASA telecoms service provider license details.
- f) The system shall be configurable remotely
- g) The system shall conform to Eskom cybersecurity standards for operational technology with AES-256 and IPsec as a minimum.
- h) When the system detects that the alarm event cannot be sent, it should store the alert information in its memory and try every 5min to resend the event from the device memory until successful alert has been sent.
- i) The system shall support SMS and email notifications.
- j) The system shall support a stand-alone mode as well as a hierarchical architecture with client/server mode with a centralised management system.
- k) The application software shall be compatible and upgradable to support the latest Microsoft Windows operating system.
- l) The system shall support industry open communication protocols to integrate seamlessly to a centralised Physical Security Information Management (PSIM) system without requiring extensive reengineering. The supplier to list communication protocols supported.
- m) The system shall be able to automatically poll each unit/sensor at least once every 24 hours to confirm both its health status and GPS coordinates and send alert information to the control station.
- n) The system shall allow a system administrator with the appropriate user-level authorization and two-way factor authentication to remotely configure it including arming/on, disarming/off and setting changes.
- o) The status of the field units/sensors shall be periodically and automatically checked and reported to the control monitoring/viewing stations. The frequency of these reporting shall be configurable.

### **3.6 Cybersecurity**

- a) The system shall comply with 240-55410927 ("Cybersecurity Standard for Operational Technology"), which serves to guide the implementation of cybersecurity principles in the OT environment.
- b) All connections to the Eskom OT networks shall be firewalled as per 240-79669677 ("Demilitarised Zone (DMZ) Designs for Operational Technology").
- c) All connections to the Eskom corporate network shall be firewalled and approved by Eskom Group IT.

**COPYRIGHT PROTECTED**



- d) Remote access to the Eskom network shall adhere to 32-273 ("Information Security – IT/OT and Third-Party Remote Access Standard").

### **3.7 Cabling**

- a) All cabling as circumstances dictate to be placed in trenching at least 300mm deep or as Eskom regulations dictate and encased in conduit or armoured cabling shall be used. This will be clarified by Eskom on a site to site basis.
- b) Data and low voltage (0-48V DC/AC) cable installations shall be separated from mains power installations by a minimum of 500mm.
- c) Where data and low voltage cabling has to cross power cabling, this shall always be at 90° angles.
- d) Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.
- e) Cabling in manholes shall be kept above the manhole floor level to avoid water contact.
- f) Where any power reticulation work has been undertaken, contractors shall make provision to submit an approved reticulation certificate issued by an authorised electrical Contractor.

### **3.8 Environmental operating Conditions**

- a) The system shall function normally under the following environmental conditions:
  - 1) System frequency: 50Hz
  - 2) Altitude: 0m to 2500m above sea level
  - 3) Ambient temperature: -20°C to 50°C
  - 4) Maximum relative humidity: 100%
- b) The system shall not be susceptible to environmental factors such as wind, rain, heat, etc.
- c) The sensors shall be inconspicuous to reduce likelihood of vandalism and other physical hazards.
- d) The system will be installed where it will be subject to voltage surges due to lightning, a variety of line faults, power interruptions and high voltage switching conditions. The system shall be able to operate without failure under all of the above-mentioned conditions.
- e) Protection against high voltage transients shall be provided on both the signal and power circuitry, without impairing the system's electrical parameters, sensitivity, or performance.
- f) The system shall comply with the relevant EMC standards regulated by ICASA. The system ECM shall ensure correct operation in the a substation environment and EMI performance shall not interfere with any power system or its operations, including any onsite communication infrastructure.
- g) Alarm module of the system shall comply to environmental testing requirements outlined in [10], SANS 60839-1-3 (Alarm systems Part 1: General requirements Section Three: Environmental testing).

### **3.9 Power Supply**

- a) The system shall be supplied with 240V mains AC 50Hz available at site.
- b) The system shall have a capability to be powered by a DC source.
- c) The existing standby power systems on site shall be used as the primary standby power source, provided that the standby time (autonomy) requirements of the site are not adversely affected.
- d) Where the existing standby power systems on site cannot be used, the alternative standby power systems proposed shall comply with the requirements of [3], 240-91190294 (DC and Auxiliary Supplies Philosophy).

**COPYRIGHT PROTECTED**

- e) The standby time of the system shall be in line with the overall required standby time for the site. The requirements of [4], 240-118870219 (Standby Power Systems Topology and Autonomy for Eskom Sites) shall be adhered to.
- f) Power units for alarm module shall comply to requirements of [13] , SANS 2220-1-7 (Electrical Security Systems, Part 1.7: Intruder alarm systems: Power units).
- g) The system shall have an additional power failure alarm indication that shall be sent through to the Eskom control room should the power supply be interrupted.
- h) All electrical components shall be protected against excess current and short-circuit by adequately rated overload protective devices.

#### **4. Management and Monitoring requirements**

- a) On-site (local) management of the system shall be via human interface through a computerised system.
- b) The system shall enable monitoring of alarms both locally and remotely.
- c) Hardware: Management platform shall comprise of a desktop computer and minimum 17" Flat Screen monitor to support rapid execution of maintenance and reporting routines.
- d) Software: Management/administrative software and licensing shall execute maintenance routines of the entire system, monitor the operational status of all components of the system and changing the configuration parameters of the system both on site and remotely.
- e) Access to an on-site management system service terminal must be password protected.
- f) The remote management must not require any specialised remote management platform to access the installed location/s remotely.
- g) The supplier to state previous PSIMs which they have integrated to and provide API/SDK information flow details (not the code, just the information and object descriptions.)
- h) List all the functionalities provided over remote access configuration.
- i) The system software shall maintain a real-time sequential record (on the hard disk) of sensor events, alarm events and all operator programming events. If so required, these events shall be stored in such a format that it is possible for other operators to sort and analyse them.
- j) Transactions shall be recorded in a database with different level of administrative rights ( write, read only etc).
- k) Database reports shall be capable of being exported and transmitted electronically in different formats (e.g., MS excel, PDF, etc).
- l) The supplier shall provide details of the backup strategy and off-site storage procedures.

#### **5. Support services**

- a) Supplier shall offer support and maintenance for all product(s), equipment and/or solutions offered. The detailed description of the services required will be stipulated in the enquiry documentation.

#### **6. System Documentation**

- a) The system shall be supplied together with the following documentation:
  - 1) Technical description of the proposed system including the following:
    - i. Types of sensors used and method of pre-detection;
    - ii. Method of communication between field units/sensors and central master station;
    - iii. Method of false alarms elimination;

**COPYRIGHT PROTECTED**

- iv. Expected failure rate as a percentage of Units installed;
- v. Cost of the System operation;
- 2) Instructions for the installation. Any component that may be damaged by the reversal of the input polarity shall have this fact clearly stated in the instructions.
- 3) List of all field replaceable spare parts
- 4) Electrical and mechanical specifications and parameters for the equipment
- 5) Wiring diagrams of the equipment
- 6) Installation, commissioning and maintenance procedures
- 7) All modules and circuit diagrams
- 8) Schematic diagrams
- 9) Installation drawings
- 10) Power supply requirements
- 11) Performance characteristics, including the MTBF
- 12) Wiring and mounting instructions
- 13) Output ratings
- 14) Instructions for adjustment, including specification of any special tools required
- 15) Programme for maintenance, testing and servicing

## **7. Design acceptance**

- a) The successful supplier will be required to obtain design review governance approval for both the basic design as well as the detailed design.
- b) All design documents to be provided in Eskom approved formats.

## **8. Authorization**

This document has been seen and accepted by:

Joint Security Care Group

## **9. Revisions**

<b>Date</b>	<b>Rev</b>	<b>Compiler</b>	<b>Remarks</b>
May 2022	Rev 1	R Moshoeshoe	First issue

## **10. Development team**

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

- Donald Moshoeshoe

## **11. Acknowledgements**

Not applicable.

## Annex A – System Performance Calculation

The overall System performance shall be calculated as follows and shall conform to the performance levels outlined below:

$$\text{System availability} = \frac{(\text{amount of hours per month}) - (\text{amount of non-operational hours})}{\text{Amount of hours per month}} \times 100$$

$$= \frac{(720 \text{ hours}) - (\text{amount of non-operational hours})}{\text{Amount of hours per month}} \times 100$$

$$= \text{Better than 98\%}$$

$$\text{System Dependability} = \frac{\text{number of successful Detections}}{\text{Number of alarms}} \times 100$$

$$= \text{Better than 95\%}$$

- 1) The number of alarms will be the number of alarms recorded by the system during the course of the month.

$$\text{System Reliability} = \frac{100 - (\text{number of faults})}{100} \times 100$$

$$= \text{Better than 95\%}$$

- 1) Where the number of faults will be the number of physical faults on the system that had to be repaired.

### The overall performance (O)

$$= \text{System availability} \times \text{System Dependability} \times \text{System Reliability}$$

$$> 88\%$$

**Annex B – Technical Schedules A and B**

TECHINAL SCHEDULE A AND B FOR INTRUSION PRE-DETECTION SYSTEMS USED AT ESKOM SITES 240-170000691

Schedule A: Purchaser’s specifications

Schedule B: Guarantees, compliance, and technical particulars of equipment offered

- The clauses and numbering in this table are not necessarily the verbatim clauses as per 240-170000691. Therefore, it is OBLIGATORY on the TENDERER to review the applicable clauses in 240-170000691 in order to provide an informed response.
- When completing the Schedule B and the References section, The Tenderer is required to state clearly, for each clause that requires a statement of compliance, with one of the following options:
  - a) Comply – Confirmation of FULL Compliance to all clauses of the applicable section of the Technical Standard. No deviations
  - b) Partially Comply – Confirmation of PARTIAL Compliance and that FULL Compliance is not possible. Deviations taken.
  - c) Do Not Comply - Confirmation of Non-Compliance to ALL requirements in the applicable section
    - Reference to evidence in the form of datasheets, equipment manuals, drawings, hyperlinks shall be included in the References section
    - Where there are any deviations taken from the clauses in the applicable section, these should be indicated under the References and Deviations section

	Description	Schedule A	Schedule B	References/Statement supporting evidence/ Deviations	Comments
3	Requirements	<del>X</del>	<del>X</del>		
3.1	General requirements	<del>X</del>	<del>X</del>		
a)	Intrusion pre-detection systems will be used to provide detection at all strategic areas at site as identified by Eskom including site perimeter, entrances, control rooms, battery rooms, HV yard, storerooms etc.	comply			
b)	The system shall provide intrusion detection for the following (but not limited to):	<del>X</del>	<del>X</del>		

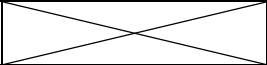

**COPYRIGHT PROTECTED**

	1) Unauthorised movement around/inside a protected area at site	comply			
	2) Tunnelling underneath the fences	comply			
	3) Separation of electric fence conductors	comply			
	4) Cutting and climbing over perimeter barrier fences/walls	comply			
	5) Vibrations caused by Digging underneath, breaking through and climbing over the barrier fences/walls.	comply			
c)	Where mode of operation depends on line of sight", this must be kept clear of all obscuring objects.	comply			
d)	Where mode of operation depends on vibrations, the system shall not be susceptible to nuisance alarms due to passing vehicles/trucks.	comply			
e)	The system should have a capability to log at least 100 events in a memory using First-In-First-Out method for overwrite.	comply			
f)	The system shall have a zoning capability for alarm monitoring and fault finding.	comply			
g)	The system shall return to its normal non-alarm condition within 10s after an alarm signal is generated.	comply			

**COPYRIGHT PROTECTED**

h)	All system components shall be synchronized with a real-time clock with minimum accuracy of 250ms	comply			
l)	Depending on the mode of detection, the weight of the object that may trigger an alarm shall be configurable	comply			
j)	Depending on the mode of detection, the height of the object that may trigger an alarm shall be configurable.	comply			
k)	Depending on the mode of detection, the depth of the object that may trigger an alarm shall be configurable.	comply			
l)	Depending on the mode of detection, the range of the object that may trigger an alarm shall be configurable. Minimum is 300 meters.	comply			
m)	The system shall cover the entire protected area, the size/area of the protected site shall be configurable. Typical area is 120 000 m <sup>2</sup> .	comply			
n)	Depending on the mode of detection, the frequency and level of the vibration that may trigger an alarm shall be configurable.	comply			
o)	There shall be a mechanism to reduce/eliminate false alarms, the supplier shall demonstrate how false alarms are reduced/eliminated.	comply			
p)	The system life cycle of the proposed product must be a minimum of 10 years.	comply			

**COPYRIGHT PROTECTED**

q)	Mode of operation shall not be limited by different light conditions (e.g., day vs night conditions).	comply			
r)	The maximum dimensions (number, size, length, etc) of the sensors/detection units shall be variable to suit site specific requirements.	comply			
<b>3.2</b>	<b>Principle of Operation</b>				
a)	Tenders shall include detailed technical information and principles of operation of their system offered with their quote or tender. Failure to do so may render their tender incomplete.	comply			
b)	The overall performance (O) of each security system during operation shall be monitored on a monthly basis and kept above 88% when calculated as outlined in Annex A:	comply			
	1) System availability, which should be greater than 98%	comply			
	2) System dependability, which should be greater than 95%	comply			
	3) Overall performance (O) shall be greater than 88%	comply			

**COPYRIGHT PROTECTED**



	4) If overall performance falls below 88% then remedial action must be taken and the system shall be self-healing.	comply			
<b>3.3</b>	<b>Housing and safety</b>				
a)	System Units shall be sealed to prevent insects from interfering with their normal operation.	comply			
b)	Housing for system units to be frost and dew resistant and fitted with an anti-tamper facility.	comply			
c)	It shall not be possible to alter the enclosure arrangements of the detector or to change its existing area of detection coverage or detection range without causing an alarm condition.	comply			
d)	It shall not be possible to disable the tamper detection device by means of normally available tools such as knives or screwdrivers.	comply			
e)	Housing for system units shall have an IP rating of IP65 or higher.	comply			
f)	Material of the housing units must be UV stable for at least 10 years.	comply			
g)	Housing shall not hinder/interrupt wireless communication signals to/from the units	comply			

**COPYRIGHT PROTECTED**

h)	Any container for batteries shall be so constructed that the battery terminals are protected against inadvertent contact with metal parts.	comply			
i)	A power unit for the system shall be so constructed that electronics and electrical circuits are protected against hazards caused by battery charging, accidental electrolyte spillage, fumes or explosive gas.	comply			
j)	The mechanical construction of any part of the system shall be such that injury caused by mechanical instability or by moving parts, protruding or sharp edges is prevented.	comply			
k)	Enclosures shall be so constructed and mounted such that electrical tests and operations are possible without the removal of the devices from their mounting.				
<b>3.4</b>	<b>System alarming and notifications</b>				
a)	System alarming shall comply with requirements of 240-86738968, specification for integrated security alarm system for protection of Eskom installations and its subsidiaries.	comply			
b)	The Intrusion pre-detection system shall allow for the signalling of the following alarm conditions to a central monitoring point locally and/or remotely from the site:				
	1) Intrusion pre-detection alarms	comply			
	2) Equipment fail alarm (health check, mains supply fail, battery low)	comply			

**COPYRIGHT PROTECTED**

**STANDARD FOR INTRUSION PRE-DETECTION SYSTEMS USED AT ESKOM SITES**

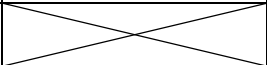
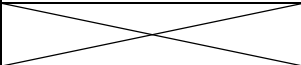
Unique Identifier: **240-170000691**

Revision: **1**

Page: **19 of 30**

	3) Tamper detection	comply			
	4) Signal processing interference failure	comply			
c)	For each alarm notification, the following information shall be disseminated to the monitoring/viewing stations:	X	X		
	5) Type of event (System, Incident, or Administrative).	comply			
	6) Date and time of the event in format CCYY/MM/DD; hh:mm:ss.	comply			
	7) Name/identification of the reporting device.	comply			
	8) Location of the reporting device in the form of GPS coordinates. Accuracy of the location shall be within 10-meter radius from the device.	comply			
d)	The alarms shall be viewable both onsite and remotely.	comply			
e)	The system shall be interoperable with existing alarming system(s) at site.	comply			
f)	The system shall resume its normal non-alarm condition within 10s after restoration from an alarm state.	comply			
g)	The system shall be immune to nuisance alarms due to small targets such as birds.	comply			

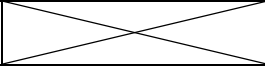
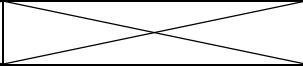
**COPYRIGHT PROTECTED**

h)	The detection range and sensitivity of the detectors shall be configurable.	comply			
i)	The system shall sustain the alarm state until the controller has acknowledged a receipt of the intrusion alert on the Data Monitoring System.	comply			
j)	There shall be a graphical user interface (GUI) with site zones and aggregation of the system data.	comply			
k)	Alert notifications/alarms shall be colour coded (e.g. yellow, green, orange, red, etc.) on the GUI to indicate the status and criticality of the alert/alarm.	comply			
l)	The system shall have intelligence to eliminate nuisance alarms due to vibrations, shadows and noise caused by passing cars, airplanes etc.	comply			
<b>3.5</b>	<b>Communication</b>				
a)	Single-mode optical fibre shall be the preferred physical transport medium due to the high EMC environment at substations. The fibre requirements shall comply with the standard 240-46264031 ("Fibre-Optic Design Standard – Part 2: Substations").	comply			
b)	Eskom Telecommunications shall be a default means of communication for off-site communication, where Eskom Telecoms has no presence, the supplier shall provide alternative communication.	comply			

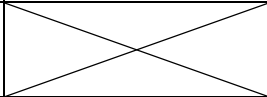
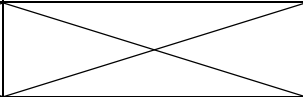
**COPYRIGHT PROTECTED**

c)	The system shall allow for wireless sensor connection to an onsite central hub or cellular connectivity to onsite hub or Security Operations Centre.	comply			
d)	The system shall be ICASA approved.	comply			
e)	Supplier to ensure communication in areas where cellular coverage is known to be minimal and/or not available. The supplier to provide ICASA telecoms service provider license details.	comply			
f)	The system shall be configurable remotely	comply			
g)	The system shall conform to Eskom cybersecurity standards for operational technology with AES-256 and IPsec as a minimum.	comply			
h)	When the system detects that the alarm event cannot be sent, it should store the alert information in its memory and try every 5min to resend the event from the device memory until successful alert has been sent.	comply			
i)	The system shall support SMS and email notifications.	comply			
j)	The system shall support a stand-alone mode as well as a hierarchical architecture with client/server mode with a centralised management system.	comply			
k)	The application software shall be compatible and upgradable to support the latest Microsoft Windows operating system.	comply			

**COPYRIGHT PROTECTED**

l)	The system shall support industry open communication protocols to integrate seamlessly to a centralised Physical Security Information Management (PSIM) system without requiring extensive reengineering. The supplier to list communication protocols supported.	comply			
m)	The system shall be able to automatically poll each unit/sensor at least once every 24 hours to confirm both its health status and GPS coordinates and send alert information to the control station.	comply			
n)	The system shall allow a system administrator with the appropriate user-level authorization and two-way factor authentication to remotely configure it including arming/on, disarming/off and setting changes.	comply			
o)	The status of the field units/sensors shall be periodically and automatically checked and reported to the control monitoring/viewing stations. The frequency of these reporting shall be configurable.	comply			
<b>3.6</b>	<b>Cybersecurity</b>				
a)	The system shall comply with 240-55410927 (“Cybersecurity Standard for Operational Technology”), which serves to guide the implementation of cybersecurity principles in the OT environment.	comply			
b)	All connections to the Eskom OT networks shall be firewalled as per 240-79669677 (“Demilitarised Zone (DMZ) Designs for Operational Technology”).	comply			

**COPYRIGHT PROTECTED**

c)	All connections to the Eskom corporate network shall be firewalled and approved by Eskom Group IT.	comply			
d)	Remote access to the Eskom network shall adhere to 32-273 ("Information Security – IT/OT and Third-Party Remote Access Standard").	comply			
<b>3.7</b>	<b>Cabling</b>				
a)	All cabling as circumstances dictate to be placed in trenching at least 300mm deep or as Eskom regulations dictate and encased in conduit or armoured cabling shall be used. This will be clarified by Eskom on a site to site basis.	comply			
b)	Data and low voltage (0-48V DC/AC) cable installations shall be separated from mains power installations by a minimum of 500mm.	comply			
c)	Where data and low voltage cabling has to cross power cabling, this shall always be at 90° angles.	comply			
d)	Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.	comply			
e)	Cabling in manholes shall be kept above the manhole floor level to avoid water contact.	comply			
f)	Where any power reticulation work has been undertaken, contractors shall make provision to submit an approved reticulation certificate issued by an authorised electrical Contractor.	comply			

**COPYRIGHT PROTECTED**

3.8	<b>Environmental operating Conditions</b>	X	X		
a)	The system shall function normally under the following environmental conditions:	X	X		
	1) System frequency: 50Hz	comply			
	2) Altitude: 0m to 2500m above sea level	comply			
	3) Ambient temperature: -20°C to 50°C	comply			
	4) Maximum relative humidity: 100%	comply			
b)	The system shall not be susceptible to environmental factors such as wind, rain, heat, etc.	comply			
c)	The sensors shall be inconspicuous to reduce likelihood of vandalism and other physical hazards.	comply			
d)	The system will be installed where it will be subject to voltage surges due to lightning, a variety of line faults, power interruptions and high voltage switching conditions. The system shall be able to operate without failure under all of the above-mentioned conditions.	comply			

**COPYRIGHT PROTECTED**



e)	Protection against high voltage transients shall be provided on both the signal and power circuitry, without impairing the system's electrical parameters, sensitivity, or performance.	comply			
f)	The system shall comply with the relevant EMC standards regulated by ICASA. The system ECM shall ensure correct operation in the a substation environment and EMI performance shall not interfere with any power system or its operations, including any onsite communication infrastructure.	comply			
g)	Alarm module of the system shall comply to environmental testing requirements outlined in [10], SANS 60839-1-3 (Alarm systems Part 1: General requirements Section Three: Environmental testing).	comply			
<b>3.9</b>	<b>Power Supply</b>				
a)	The system shall be supplied with 240V mains AC 50Hz available at site.	comply			
b)	The system shall have a capability to be powered by a DC source.	comply			
c)	The existing standby power systems on site shall be used as the primary standby power source, provided that the standby time (autonomy) requirements of the site are not adversely affected.	comply			

**COPYRIGHT PROTECTED**

d)	Where the existing standby power systems on site cannot be used, the alternative standby power systems proposed shall comply with the requirements of [3], 240-91190294 (DC and Auxiliary Supplies Philosophy).	comply			
e)	The standby time of the system shall be in line with the overall required standby time for the site. The requirements of [4], 240-118870219 (Standby Power Systems Topology and Autonomy for Eskom Sites) shall be adhered to.	comply			
f)	Power units for alarm module shall comply to requirements of [13] , SANS 2220-1-7 (Electrical Security Systems, Part 1.7: Intruder alarm systems: Power units).	comply			
g)	The system shall have an additional power failure alarm indication that shall be sent through to the Eskom control room should the power supply be interrupted.	comply			
h)	All electrical components shall be protected against excess current and short-circuit by adequately rated overload protective devices.	comply			
<b>4</b>	<b>Management and Monitoring requirements</b>				
a)	On-site (local) management of the system shall be via human interface through a computerised system.	comply			
b)	The system shall enable monitoring of alarms both locally and remotely.	comply			

**COPYRIGHT PROTECTED**

c)	Hardware: Management platform shall comprise of a desktop computer and minimum 17" Flat Screen monitor to support rapid execution of maintenance and reporting routines.	comply			
d)	Software: Management/administrative software and licensing shall execute maintenance routines of the entire system, monitor the operational status of all components of the system and changing the configuration parameters of the system both on site and remotely.	comply			
e)	Access to an on-site management system service terminal must be password protected.	comply			
f)	The remote management must not require any specialised remote management platform to access the installed location/s remotely.	comply			
g)	The supplier to state previous PSIMs which they have integrated to and provide API/SDK information flow details (not the code, just the information and object descriptions.)	comply			
h)	List all the functionalities provided over remote access configuration.	comply			
l)	The system software shall maintain a real-time sequential record (on the hard disk) of sensor events, alarm events and all operator programming events. If so required, these events shall be stored in such a format that it is possible for other operators to sort and analyse them.	comply			

**COPYRIGHT PROTECTED**

j)	Transactions shall be recorded in a database with different level of administrative rights (write, read only etc).	comply			
k)	Database reports shall be capable of being exported and transmitted electronically in different formats (e.g., MS excel, PDF, etc).	comply			
l)	The supplier shall provide details of the backup strategy and off-site storage procedures.	comply			
<b>5</b>	<b>Support services</b>				
a)	Supplier shall offer support and maintenance for all product(s), equipment and/or solutions offered. The detailed description of the services required will be stipulated in the enquiry documentation	comply			
<b>6</b>	<b>System Documentation</b>				
a)	The system shall be supplied together with the following documentation:				
1)	Technical description of the proposed system including the following:				

**COPYRIGHT PROTECTED**

	i) Types of sensors used and method of pre-detection;	comply			
	ii) Method of communication between field units/sensors and central master station;	comply			
	iii) Method of false alarms elimination;	comply			
	iv) Expected failure rate as a percentage of Units installed;	comply			
	v) Cost of the System operation;	comply			
2)	Instructions for the installation. Any component that may be damaged by the reversal of the input polarity shall have this fact clearly stated in the instructions.	comply			
3)	List of all field replaceable spare parts	comply			
4)	Electrical and mechanical specifications and parameters for the equipment	comply			
5)	Wiring diagrams of the equipment	comply			
6)	Installation, commissioning and maintenance procedures	comply			
7)	All modules and circuit diagrams	comply			
8)	Schematic diagrams	comply			

**COPYRIGHT PROTECTED**

9)	Installation drawings	Comply			
10)	Power supply requirements	comply			
11)	Performance characteristics, including the MTBF	comply			
12)	Wiring and mounting instructions	comply			
13)	Output ratings	comply			
14)	Instructions for adjustment, including specification of any special tools required	comply			
15)	Programme for maintenance, testing and servicing	comply			
<b>7</b>	<b>Design acceptance</b>				
a)	The successful supplier will be required to obtain design review governance approval for both the basic design as well as the detailed design.	comply			
b)	All design documents to be provided in Eskom approved formats.	comply			

**COPYRIGHT PROTECTED**