Eskom	**Standard**	**Technology**

Title: **PHYSICAL SECURITY INTEGRATION STANDARD**

Unique Identifier:	**240-170000096**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**1**
Total Pages:	**19**
Next Review Date:	**July 2025**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Approved by**	**Authorized by**
Donald Moshoeshoe	**Prince Moyo**	**Dr. Titus Mathe**
Engineer	**General Manager: Power Delivery Engineering**	**General Manager: Asset Management**
Date: 22/02/2020	Date: 3/08/2020	Date: 03 August 2020

Supported by SCOT/SC

Richard McCurrach

PTM&C TC Chairperson

Date: 22 July 2020

PCM Reference: **240-43542545**

SCOT Study Committee Number/Name: **Part 16 – DC and Auxiliary Supplies**

Content

Figures

Tables

Executive summary

The increasing threat to the safety and security of people, information, and assets at Eskom substations is affecting Eskom's operations and its ability to deliver the required level of service. The safety of people and the integrity of assets are key priorities at Eskom.

The integration of the physical security equipment at substations with a centralised physical security management system is a necessity for Eskom to integrate the various physical security elements which would allow protection of Eskom's assets. This standard details the requirements to integrate the different physical security equipment (subsystems) at the substation level to interface with a common security management system. This standard also specifies that the different physical security equipment (subsystems) must be able to communicate (be interoperable) with equipment from different suppliers.

The purpose of the integrated system is, furthermore, to give users the ability to achieve maximum benefit from each individual system, while reducing the time, cost, and risk that come with operating and maintaining a number of individual, stand-alone systems.

1. Introduction

A surge in crime-related incidents at Eskom sites has prompted a requirement to initiate security projects that will interface with a centralised management system. The increasing threat to the safety and security of people, information, and assets is affecting Eskom's operations and its ability to deliver a world-class service. The safety of people and the integrity of information and assets are key priorities at Eskom.

The document details the integration and interoperability requirements of the physical security systems at substations to a centralised security management system.

2. Supporting clauses

2.1 Scope

The document details integration and interoperability requirements for a number of security subsystems to a centralised management system. The security subsystems consist of a number of different security systems, among others, the integrated security alarm system, the non-lethal energised perimeter detection system (NLEPDS), the CCTV surveillance, the intruder detection systems, the integrated access control system (IACS), and the public address system.

2.1.1 Purpose

The purpose of the document is to provide requirements that must be met to ensure that the different physical security equipment and systems can be integrated and are interoperable.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited.

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] 240-86738968 – Specification for Integrated Security Alarm System for Protection of Eskom Installations and its Subsidiaries

[3] 240-78980848 – Specification for Non-Lethal Energised Perimeter Detection System (NLEPDS) for Protection of Eskom Installations and its Subsidiaries

[4] 240-91190304 – Specification for CCTV Surveillance with Intruder Detection

[5] 240-102220945 – Specification for Integrated Access Control System (IACS) for Eskom Sites

[6] 240-170000098 – Security Public Address System for Substations and Telecoms High Sites

[7] 240-139282493 – Security Lighting for Eskom Applications

[8] 240-46264031 – Fibre-Optic Design Standard – Part 2: Substations

[9] 240-91190294 – DC and Auxiliary Supplies Philosophy

[10] 240-118870219 – Standby Power Systems Topology and Autonomy for Eskom Sites

[11] 240-56360086 – Stationary Vented Nickel Cadmium Batteries Standard

[12] 240-56360034 – Stationary Vented Lead Acid Batteries Standard

[13] 240-51999453 – Standard Specification for Valve-Regulated Lead Acid Cells

[14] 240-53114248 – Thyristor and Switch Mode Chargers, AC/DC to DC/AC Converters, and Inverter/Uninterruptible Power Supplies Standard

[15] 240-64139144 – AC Boards and Junction Boxes for Substations

[16] 240-76628687 – AC/DC Reticulation Equipment for Breaker-and-a-Half Substations

[17] 240-75658628 – Distribution Group's Specific Requirements for AC/DC Distribution Units

[18] 240-60725641 – Specification for Standard (19-Inch) Equipment Cabinets

[19] 240-55410927 – Cybersecurity Standard for Operational Technology

[20] 240-79669677 – Demilitarised Zone (DMZ) Designs for Operational Technology

[21] 32-273 – Information Security – IT/OT and Third-Party Remote Access Standard

[22] 240-55863502 – Definition of OT and OT/IT Collaboration Accountabilities

[23] 240-170000086 Roles and Accountabilities for Lifecycle Management of Physical Security Systems in the Transmission Division

2.2.2 Informative

None.

2.3 Definitions

2.3.1 General

Definition	Description
PSIM	PSIM (Physical Security Information Management system) is a category of software that provides a platform and applications created by middleware developers, designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
A	Ampere
AC	Alternating current
CCTV	Closed-circuit television
DVR	Digital video recorder
EHW	Electronic hardware
EMC	Electromagnetic coupling
ENC	Eskom national contract
FAT	Factory acceptance testing
IP	Internet protocol
IT	Information technology
LAN	Local area network

Abbreviation	Description
NLEPDS	Non-lethal energised perimeter detection system
NVR	Network video recorder
PA	Public address
PSIM	Physical security information management
SAT	Site acceptance testing
SLA	Service-level agreement
SW	Software

2.5 Roles and responsibilities

The Security Systems Care Group, which operates under the DC and Auxiliary Supplies Study Committee, shall ensure that the technology developed is adequate for application across Eskom sites where it will be utilised.

2.6 Process for monitoring

The Security Systems Care Group will determine the effectiveness of this standard.

2.7 Related/Supporting documents

Not applicable

3. Requirements

This document describes the key requirements for the design philosophy to ensure integration and interoperability between the different security equipment and systems with the management (PSIM) system.

3.1 Integration requirements

3.1.1 High-level design objectives

This section describes the minimum design objectives of an integrated security system, which are as follows:

a) Open standards: in order to meet all the operational design requirements, it is necessary to integrate multiple systems from multiple manufacturers. These include both low-level electronic hardware (EHW) interfaces and high-level software (SW) interfaces. It is also a requirement to support legacy installations until such time that the equipment is upgraded or declared obsolete.

b) Scalability of design: the integrated system must be able to scale over multiple site sizes, from very small to very large sites.

c) Support for multiple manufacturers: from a business continuity perspective, it is required that equipment from multiple manufacturers can be integrated.

d) Operational availability and redundancy: the system should have a high level of availability once deployed. In addition, the system should be designed in such a way that a single point of failure does not disrupt the total system operation. The integrated solution shall be designed based on an “always-on principle”, where a failure in any subsystem shall not render the overall system non-operational.

e) Maintainability: the system should have diagnostic capabilities to monitor the health and status of the system and its various components. The situational awareness feature of the system shall indicate which functional output is affected by the failure of certain subsystems (for example, a dashboard feature reporting on the state of health of the different subsystems at a site).

f) Integration: the integrated security solution must effectively integrate and control different physical security subsystems at a site, with the objective of protecting the site against any physical intrusion threats. The system shall, furthermore, be effectively integrated with an off-site security management system (platform), which is deployed within an Eskom–owned site enabling remote monitoring and control functionality.

3.1.2 Design philosophy

To ensure integration and interoperability, the design philosophy requirements are as follows:

a) Open system electronic hardware (EHW) interfaces: all EHW components shall have open interfaces (e.g. IP) and shall be supported by more than one manufacturer. The hardware interfaces shall be an industry standard.

b) Open system software (SW) interfaces: all SW components shall have open interfaces where they integrate with higher- and lower-level system components and shall be supported by more than one manufacturer. The software interfaces shall be an industry standard.

c) Open system integration framework: the integration framework shall have open interfaces where they interface with higher- and lower-level system components and shall be supported by more than one manufacturer.

d) Simple and well-defined interfaces: where either EHW or SW interfaces are defined, it shall be done in such a way that it provides the least complex integration interface.

e) Generic design modules: common modules will be defined that may be reused over multiple sites. Commonality of design modules allows for a reduction in design effort as well as reduced procurement costs, maintenance costs and maintenance overhead costs.

f) Scalable interfaces and system architecture: to support future upgrading and expansion of the Physical Security Information Management system (PSIM), the system shall be scalable at an EHW and SW level.

g) System configuration and set-up: the design shall be done in such a way that the configuration effort for each site will be kept to a minimum. It shall be possible to load, update, and change site configurations remotely. User-friendly configuration files shall be used for this purpose.

h) System health and status monitoring: all critical interfaces and equipment shall provide an automated health and status monitoring function. The health and status monitoring functions shall also support the maintenance process.

i) Security process traceability: traceability for the security process shall be provided by logging and reporting of security occurrences and the resolution actions performed. All security system-related events shall be date-time stamped and descriptive.

j) Maintenance traceability: traceability for the maintenance process shall be provided by logging and reporting of maintenance events and the resolution actions performed.

k) Custom hardware or software development may be required where equipment from two different manufacturers needs to be integrated. In the event that there are no other options than to develop custom software or hardware, this development effort shall be kept to a minimum, and the responsibility shall be with the supplier of the integrated security solution.

l) The integrated security system shall be flexible and capable of integrating some or all of the security equipment (subsystems) depending on the project-specific requirements. The design (layout) of the integrated security system is not fixed, and there could be a number of variations, as this would depend on specific project requirements. However, this design (layout) shall have to be approved by Eskom. Figure 1 is an example of a high-level layout of the integrated security system.

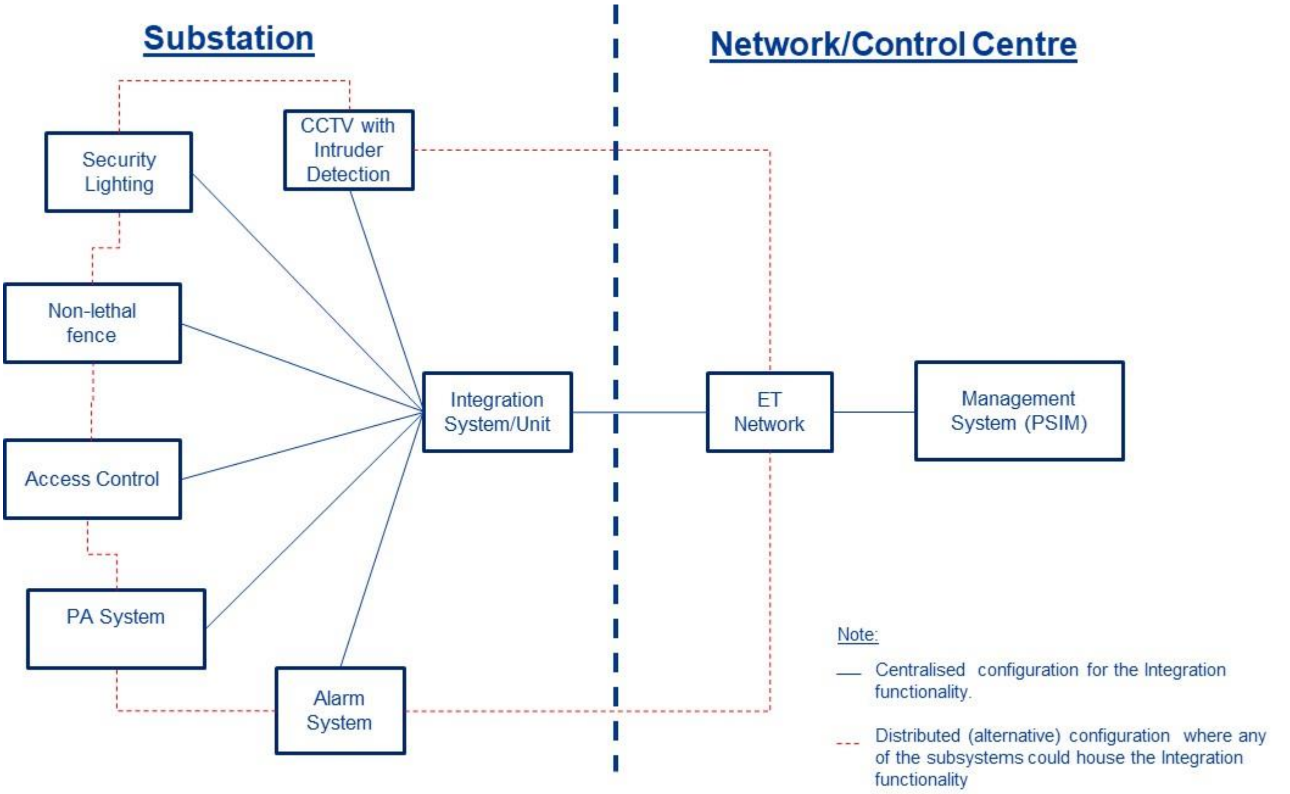
Substation
Network/Control Centre
Security Lighting
CCTV with Intruder Detection
Non-lethal fence
Access Control
PA System
Alarm System
Integration System/Unit
ET Network
Management System (PSIM)
Note:
— Centralised configuration for the Integration functionality.
--- Distributed (alternative) configuration where any of the subsystems could house the Integration functionality

Figure 1: Example of an integrated security system

3.1.3 Site security LAN, telecommunications, and data interface requirements

The telecommunications design requirements are listed below.

a) All off-site communications shall be IP based through the Eskom telecommunications network.

b) All communications on site shall be IP based, with the exception of the final communication leg to the sensor or actuator. In this regard, connections to sensors may use other signals or bus standards, but shall transform them into an IP-based network format.

c) 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”).

d) The integrated system shall be required to communicate with interfaces and protocols from legacy equipment on site.

e) Development to ensure that these legacy interface systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

3.1.4 CCTV surveillance

The CCTV cameras and DVR/NVR equipment and systems integration requirements are as follows:

a) The integrated system shall be able to integrate a range of cameras and DVR/NVR systems from different manufacturers as specified in standard 240-91190304.

b) Although the CCTV cameras and DVR/NVR are ONVIF compliant, it must, however, be noted that ONVIF compliance does not guarantee compatibility between systems.

c) Development to ensure that the existing CCTV cameras and DVR/NVR systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

d) The open industry protocols (that is, IP should be considered as a default interface for all future cameras) supported by the equipment above shall be listed.

3.1.5 Intruder detection systems

The following intruder detection equipment and systems integration requirements apply:

a) The integrated system shall be able to integrate the offered and existing intrusion detection systems from different manufacturers as specified in standards 240-91190304 and 240-86738968.

b) The integrated system shall be required to communicate with interfaces and protocols from the legacy equipment on site.

c) Development to ensure that the existing intrusion detection systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

d) The open industry protocols supported by the equipment above shall be listed.

3.1.6 Security lighting controller

The security lighting controller equipment and systems design requirements are listed below.

a) The integrated system shall be able to integrate a wide range of lighting controllers from different manufacturers as specified in standards 240-139282493 and 240-78980848.

b) The integrated system shall be required to communicate with interfaces and protocols from the legacy equipment on site.

c) Development to ensure that these legacy interface systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

d) The open industry protocols supported by the equipment above shall be listed.

3.1.7 Non-lethal energised perimeter detection system (NLEPDS)

The NLEPDS equipment and systems design requirements are listed below.

a) The integrated system shall be able to integrate a wide range of NLEPDS equipment and systems from different manufacturers as specified in standard 240-78980848.

b) The integrated system shall be required to communicate with interfaces and protocols from the legacy equipment on site.

c) Development to ensure that these legacy interface systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

d) The open industry protocols supported by the equipment above shall be listed.

3.1.8 Integrated access control system (IACS)

The IACS equipment and systems design requirements are as follows:

a) The integrated system shall be able to integrate a wide range of IACS equipment and systems from different manufacturers as specified in standard 240-102220945.

b) The integrated system shall be required to communicate with interfaces and protocols from the legacy equipment on site.

c) Development to ensure that these legacy interface systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

d) The open industry protocols supported by the equipment above shall be listed.

3.1.9 Public address systems

The following public address equipment and systems design requirements apply:

a) The integrated system shall be able to integrate a wide range of public address equipment and systems from different manufacturers as specified in standard 240-170000098.

b) The integrated system shall be required to communicate with interfaces and protocols from the legacy equipment on site.

c) Development to ensure that these legacy interface systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

d) The open industry protocols supported by the equipment above shall be listed.

3.1.10 Integrated security alarm system

The integrated security alarm equipment and systems design requirements are listed below.

a) The integrated system shall be able to integrate a wide range of integrated security alarm equipment and systems from different manufacturers as specified in standard 240-86738968.

b) The integrated system shall be required to communicate with interfaces and protocols from the legacy equipment on site.

c) Development to ensure that these legacy interface systems and equipment are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution.

d) The open industry protocols supported by the equipment above shall be listed.

3.1.11 Security management system

The Physical Security Information Management system (PSIM) equipment design requirements are listed below.

a) The integrated system shall be the interface between all the security equipment on site as listed in sections 3.1.3 to 3.1.10 above and the PSIM system.

b) The integrated system shall be able to operate with a number of management systems (PSIM) from different manufacturers.

c) The integrated system shall be required to communicate through Ethernet interfaces with the PSIM system.

d) Development to ensure that the PSIM system are compatible with the integrated system shall be the responsibility of the supplier of the integrated security solution and the supplier of the PSIM system.

e) The open industry protocols supported by the equipment/system above shall be listed.

3.1.12 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.

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

e) The engineering design shall follow both IT and OT governance processes as per 240-55863502 ("Definition of OT and OT/IT Collaboration Accountabilities").

3.1.13 EMC, housing, and power supply requirements

a) The system shall comply with the relevant EMC standards regulated by ICASA.

b) All system equipment 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.

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) In cases where the above is not possible, the standby power systems requirements for security systems at Eskom sites shall comply with the following:

1) The system design shall comply with the requirements of 240-91190294 ("DC and Auxiliary Supplies Philosophy").

2) 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 240-118870219 ("Standby Power Systems Topology and Autonomy for Eskom Sites") shall be adhered to.

3) Standard or technically acceptable equipment shall be used. This equipment is available on Eskom national contracts (ENCs) or recommended technically acceptable equipment lists.

4) In the absence of ENCs for specific equipment or recommended technically acceptable equipment, the offered equipment shall comply with the technical standards as indicated in Table 1.

Table 1: Technical standards for standby power systems equipment

Equipment	Technical standard
Nickel cadmium batteries	240-56360086 – Stationary Vented Nickel Cadmium Batteries Standard
Vented lead acid batteries	240-56360034 – Stationary Vented Lead Acid Batteries Standard
Valve-regulated lead acid batteries	240-51999453 – Standard Specification for Valve-Regulated Lead Acid Cells
Power electronics	240-53114248 – Thyristor and Switch Mode Chargers, AC/DC to DC/AC Converters, and Inverter/Uninterruptible Power Supplies Standard
Low-voltage protective devices, cubicles, and wiring	240-64139144 – AC Boards and Junction Boxes for Substations 240-76628687 – AC/DC Reticulation Equipment for Breaker-and-a-Half Substations 240-75658628 – Distribution Group's Specific Requirements for AC/DC Distribution Units

3.2 Factory acceptance testing (FAT)

a) The supplier shall configure and set up the system at its premises for factory acceptance testing by Eskom and the end user prior to deployment to the installation site.

b) All subsystems shall be tested to the integration system as listed in Table 2.

c) All subsystems shall be tested to the management system via the integration system as listed in Table 2.

d) All test procedures required to ensure the correct functioning shall be specified with a list of required test equipment and tools.

Table 2: Requirements for FAT and SAT

Subsystem	Integration system	Management system (PSIM)
CCTV surveillance	✓	✓
Intruder detection	✓	✓
Security lighting controller	✓	✓
Non-lethal energised perimeter detection system (NLEPDS)	✓	✓
Integrated access control system (IACS)	✓	✓
Public address system	✓	✓
Integrated security alarm system	✓	✓
PSIM system	✓	✓
Other subsystem 1 (if required)		
Other subsystem 2 (if required)		
Other subsystem 3 (if required)		

3.3 Site acceptance testing (SAT)

a) The supplier shall configure and install the system at the site(s).

b) All subsystems shall be tested to the integration system as listed in Table 2.

c) All subsystems shall be tested to the management system via the integration system as listed in Table 2.

d) All test procedures required to ensure the correct functioning shall be specified with a list of required test equipment and tools.

3.4 System manuals, documentation, and certificates

a) Multiple copies of the system design and architecture, system components, user manuals, and all other data sheets are to be supplied with the system.

b) The manuals, documentation, and certificates must be made available in both hard- and soft-copy formats.

3.5 Spares and system life cycle

a) The system life cycle of the proposed product must be a minimum of 10 years.

b) The life cycle of the product must be further supported in terms of spares availability for a minimum period of seven years after discontinuation of the product.

3.6 Warrantee and support

a) The system shall carry a minimum local (South African) warranty of 36 months with on-site, as well as telephonic, support from the date of the system being commissioned. After that, Eskom shall have the option to access ongoing support in terms of a subsequent agreement.

b) The supplier must have a technician on call on a 24-hour basis for purposes of telephonic support.

c) Supplier spares holding should include minimum replacement spares to restore service of the system in its entirety.

d) All support shall also include all firmware upgrades of the initial system version installed over the operational life of the system.

e) The support shall include first-line-level maintenance training.

f) The supplier shall also provide operator training on site to the end user.

g) Product support must include national, as well as international, support through the local branch.

h) The supplier shall be willing to enter into an SLA with Eskom.

i) The supplier should have a history of supplying products of this nature in South Africa for a minimum period of five years.

j) The supplier is to provide a list of reference sites where the product on offer has been installed and the year of implementation.

4. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Barry Clayton	Middle Manager – Transmission
Sikelela Mkhabela	Senior Manager – Distribution
Machiel Viljoen	Senior Manager – Generation
Kashveer Jagdaw	DC and Auxiliary Supplies SC Chairperson
Prudence Madiba	Senior Manager – Electrical and C&I Engineering
Karen Pillay	Senior Manager – Security Solutions – Physical
Cornelius Naidoo	Manager – Telecoms T&S CoE
Lenah Mothatha	Senior Manager – Transmission
Riaan Venter	Middle Manager – Civil and Structural CoE

5. Revisions

Date	Rev.	Compiler	Remarks
July 2020	1	D Moshoeshoe	A request for an integrated security solution due to business requirements

6. Development team

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

- Thomas Jacobs
- Tejin Gosai
- Ezzard de Lange

7. Acknowledgements

Not applicable.

Annex A – Technical Schedules A and B

TECHNICAL SCHEDULES A AND B FOR

PHYSICAL SECURITY INTEGRATION STANDARD IN ACCORDANCE WITH ESKOM STANDARD 240-170000096

Schedule A: Purchaser’s specifications

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

The following tabulated requirements follow the sectional numbering of Standard 240-170000096:

	Description	Schedule A	Schedule B	Provide the location in the tender documentation for evidence	Comments
3.	Requirements				
3.1	Integration requirements				
3.1.1	High-level design objectives				
	a) Comply with clause 3.1.1a) of this specification	Comply			
	b) Comply with clause 3.1.1b) of this specification	Comply			
	c) Comply with clause 3.1.1c) of this specification	Comply			
	d) Comply with clause 3.1.1d) of this specification	Comply			
	e) Comply with clause 3.1.1e) of this specification				
	f) Comply with clause 3.1.1f) of this specification				
3.1.2	Design philosophy				
	a) Comply with clause 3.1.2a) of this specification	Comply			
	b) Comply with clause 3.1.2b) of this specification	Comply			
	c) Comply with clause 3.1.2c) of this specification	Comply			
	d) Comply with clause 3.1.2d) of this specification	Comply			
	e) Comply with clause 3.1.2e) of this specification	Comply			
	f) Comply with clause 3.1.2f) of this specification	Comply			
	g) Comply with clause 3.1.2g) of this specification	Comply			
	h) Comply with clause 3.1.2h) of this specification	Comply			
	i) Comply with clause 3.1.2i) of this specification	Comply			
	j) Comply with clause 3.1.2j) of this specification	Comply			
	k) Comply with clause 3.1.2k) of this specification	Comply			
	l) Comply with clause 3.1.2l) of this specification	Comply			
3.1.3	Site security LAN, telecommunications, and data interface requirements				
	a) Comply with clause 3.1.3a) of this specification	Comply			

	b) Comply with clause 3.1.3b) of this specification	Comply			
	c) Comply with clause 3.1.3c) of this specification	Comply			
	d) Comply with clause 3.1.3d) of this specification	Comply			
	e) Comply with clause 3.1.3e) of this specification	Comply			
3.1.4	CCTV surveillance				
	a) Comply with clause 3.1.4a) of this specification	Comply			
	b) Comply with clause 3.1.4b) of this specification	Comply			
	c) Comply with clause 3.1.4c) of this specification	Comply			
	d) Comply with clause 3.1.4d) of this specification	Comply			
3.1.5	Intruder detection systems				
	a) Comply with clause 3.1.5a) of this specification	Comply			
	b) Comply with clause 3.1.5b) of this specification	Comply			
	c) Comply with clause 3.1.5c) of this specification	Comply			
	d) Comply with clause 3.1.5d) of this specification	Comply			
3.1.6	Security lighting controller				
	a) Comply with clause 3.1.6a) of this specification	Comply			
	b) Comply with clause 3.1.6b) of this specification	Comply			
	c) Comply with clause 3.1.6c) of this specification	Comply			
	d) Comply with clause 3.1.6d) of this specification	Comply			
3.1.7	Non-lethal energised perimeter detection system (NLEPDS)				
	a) Comply with clause 3.1.7a) of this specification	Comply			
	b) Comply with clause 3.1.7b) of this specification	Comply			
	c) Comply with clause 3.1.7c) of this specification	Comply			
	d) Comply with clause 3.1.7d) of this specification	Comply			
3.1.8	Integrated access control system (IACS)	Comply			
	a) Comply with clause 3.1.8a) of this specification	Comply			

	b) Comply with clause 3.1.8b) of this specification	Comply			
	c) Comply with clause 3.1.8c) of this specification	Comply			
	d) Comply with clause 3.1.8d) of this specification	Comply			
3.1.9	Public address systems				
	a) Comply with clause 3.1.9a) of this specification	Comply			
	b) Comply with clause 3.1.9b) of this specification	Comply			
	c) Comply with clause 3.1.9c) of this specification	Comply			
	d) Comply with clause 3.1.9d) of this specification	Comply			
3.1.10	Integrated security alarm system				
	a) Comply with clause 3.1.10a) of this specification	Comply			
	b) Comply with clause 3.1.10b) of this specification	Comply			
	c) Comply with clause 3.1.10c) of this specification	Comply			
	d) Comply with clause 3.1.10d) of this specification	Comply			
3.1.11	Security management system				
	a) Comply with clause 3.1.11a) of this specification	Comply			
	b) Comply with clause 3.1.11b) of this specification	Comply			
	c) Comply with clause 3.1.11c) of this specification	Comply			
	d) Comply with clause 3.1.11d) of this specification	Comply			
3.1.12	Cybersecurity				
	a) Comply with clause 3.1.12a) of this specification	Comply			
	b) Comply with clause 3.1.12b) of this specification	Comply			
	c) Comply with clause 3.1.12c) of this specification	Comply			
	d) Comply with clause 3.1.12d) of this specification	Comply			
	e) Comply with clause 3.1.12e) of this specification	Comply			
3.1.13	Power supply and EMC requirements				
	a) Comply with clause 3.1.13a) of this specification	Comply			
	b) Comply with clause 3.1.13b) of this specification	Comply			

	c) Comply with clause 3.1.13c) of this specification	Comply			
	d)i) Comply with clause 3.1.13d)i) of this specification	Comply if required			
	d)ii) Comply with clause 3.1.13d)ii) of this specification	Comply if required			
	d)iii) Comply with clause 3.1.13d)iii) of this specification	Comply if required			
	d)iv) Comply with clause 3.1.13d)iv) of this specification	Comply if required			
3.2	Factory acceptance testing	☒	☒		
	a) Comply with clause 3.2a) of this specification	Comply			
	b) Comply with clause 3.2b) of this specification	Comply			
	c) Comply with clause 3.2c) of this specification	Comply			
	d) Comply with clause 3.2d) of this specification	Comply			
3.3	Site acceptance testing	☒	☒		
	a) Comply with clause 3.3a) of this specification	Comply			
	b) Comply with clause 3.3b) of this specification	Comply			
	c) Comply with clause 3.3c) of this specification	Comply			
	d) Comply with clause 3.3d) of this specification	Comply			
3.4	System manuals, documentation, and certificates	☒	☒		
	a) Comply with clause 3.4a) of this specification	Comply			
	b) Comply with clause 3.4b) of this specification	Comply			
3.5	Spares and system life cycle	☒	☒		
	a) Comply with clause 3.5a) of this specification	Comply			
	b) Comply with clause 3.5b) of this specification	Comply			
3.6	Warrantee and support	☒	☒		
	a) Comply with clause 3.6a) of this specification	Comply			
	b) Comply with clause 3.6b) of this specification	Comply			
	c) Comply with clause 3.6c) of this specification	Comply			
	d) Comply with clause 3.6d) of this specification	Comply			
	e) Comply with clause 3.6e) of this specification	Comply			
	f) Comply with clause 3.6f) of this specification	Comply			
	g) Comply with clause 3.6g) of this specification	Comply			
	h) Comply with clause 3.6h) of this specification	Comply			
	i) Comply with clause 3.6i) of this specification	Comply			
	j) Comply with clause 3.6j) of this specification	Comply			