Eskom	Standard	Technology

Title: **SPECIFICATION FOR INTEGERATED ACCESS CONTROL SYSTEM (IACS) FOR ESKOM SITES**

Unique Identifier:	**240-102220945**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**Draft 0.1**
Total Pages:	**50**
Next Review Date:	**January 2021**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Donald Moshoeshoe	**Thomas Jacobs**	**Willy Majola**
Engineer	**DC & Auxiliary Supplies SC Chairperson**	**Engineering SGM**
Date:	Date:	Date:

Supported by SCOT/SC

Richard McCurrach

PTM&C TC Chairperson

Date:

PCM Reference: **240-43542545**

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

Content

Tables

1. Introduction

A surge in crime related incidents at Eskom sites has prompted a mandate to initiate a Security Improvement Plan (SIP). The increasing threat to the safety and security of people, information and assets is impacting Eskom operations and its ability to deliver a world class service, and in turn, public confidence in Eskom. The safety of people and the integrity of information and assets is a key priority in Eskom.

The Integrated Access Control System (IACS) is aimed at improving and effectively managing physical access and security at Eskom sites.

2. Supporting clauses

2.1 Scope

2.1.1 Purpose

To outline the technical specifications for the Eskom standard Integrated Access Control System (IACS).

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions.

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] SANS 2220-2-1 Access control systems Part 2-1: General characteristics

[3] SANS 2220-2-2 Access control systems Part 2-2: Central processors

[4] SANS 2220-2-3 Access control systems Part 2-3: Card readers

[5] SANS 2220-2-4 Access control systems Part 2-4: Reader controllers

[6] SANS 2220-2-5 Access control systems Part 2-5: Biometric readers

[7] SANS 2220-2-6 Access control systems Part 2-6: Access cards

[8] SANS 2220-1-7 Electrical security systems Part 1.7: Intruder alarm systems: Power units

[9] SANS 61000-1-2 Electromagnetic compatibility (EMC) Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena

[10] 240-86738968: Specification for Integrated Security Alarm System for Protection of Eskom Installations and its Subsidiaries

[11] 240-55410927, Cyber security standard for Operational Technology

[12] 240-55683502 - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities

[13] 240-64636794, Standard for Wiring and Cable Marking in Substations

[14] 240-70413291, Specification for Electrical Terminal Blocks

2.2.2 Informative

[15] 240-78980848: Specification for Non-Lethal Energized Perimeter Detection System (NLEPDS) for protection of Eskom Installations and its subsidiaries

[16] 240-79537982, Security Threat and Risk Assessments

[17] 240-44175038, Control of Non-Conforming Product or Service Procedure

2.3 Definitions

2.3.1 General

None

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
ACS	Access Control System
AES	Advanced Encryption Standard
CAD	Computer Aided Design
CCTV	Closed circuit television
DC	Direct Current
DVR	Digital Video Recorder
Dx	Distribution
EBI	Enterprise Buildings Integrator
EMC	Electro-magnetic Coupling
FAT	Factory Acceptance Test
GUI	Graphical user interface
Gx	Generation
h	hour
HD	High definition
HR	Human resources
HV	High Voltage
HVAC	Heating, Ventilating, and air Conditioning
IAC	Integrated Access Control
IACS	Integrated Access Control System
ID	Identity Document

Abbreviation	Description
IEC	International Electrotechnical Commission
IP	Internet Protocol
IT	Information Technology
kg	Kilogram
km	Kilometre
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LON	Local Operating Network
m	meter
mA	milliampere
mm	millimetre
MTBF	Mean Time Between Failures
MWP	Megawatt Park
NSCC	National Security Control Centre
NVR	Network Video Recorder
OMA	Outdoor Morpho Access
OT	Operational Technology
PA	Public Address
PIN	Personal Identification Number
PIR	Passive Infrared Sensor
POE	Power Over Ethernet
Prox	Proximity
SANS	South African National Standard
SAT	Site Acceptance Test
SIP	Security Improvement Plan
SQL	Structured Query Language
Tx	Transmission
UPS	Uninterruptable Power Supply
VIP	Very Important Person
VLAN	Virtual Local Area Network
WAN	Wide Area Network

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 and during the product development phase.

d) Substation Maintenance personnel shall be responsible for maintenance of equipment as per the standard

2.6 Process for monitoring

Group Security risk analysis will determine the effectiveness of this standard.

2.7 Related/supporting documents

None

3. Access control systems classification

3.1 General

Access control systems are classified by the degree of security they provide, the supplier of the system shall indicate the classification of the system in accordance with 4.1 of SANS 2220-2-1, the classification being related to the nature of the risk and the level of security that is provided.

3.2 Class 1 — Common code

A class 1 access control system shall allow access to persons who key in a single common code. The code may be alphabetic, numeric or alphanumeric.

3.3 Class 2 — Common access card

In a class 2 access control system, each card shall have the same encoded data chosen from at least 10 000 possibilities.

3.4 Class 3 — System coded access card

In a class 3 access control system, each card shall have a system code chosen from at least 200 possibilities and an individual code chosen from at least 10 000 possibilities. It shall be possible to add cards to or delete cards from the system. The cards shall not be accepted by any system other than the one in which they are intended to operate. Biometrics on its own may be used instead of a card. This class of access control system shall incorporate a central control and monitoring system whereby the central processor software can be used to generate reports on the status of any card. The overall system shall have sufficient redundancy to achieve an MTBF (mean time between failures) of 15 000 h, assessed in accordance with IEC 60050-191 and IEC 60300 (all parts).

3.5 Class 4 — Unique access card

In a class 4 access control system, it shall be possible to decentralize the intelligence. Each card shall have a code chosen from at least ten million possibilities and any attempt to change or modify the code shall destroy the card. It shall be possible to add cards to or delete cards from the system.

The cards shall not be accepted by any system other than the one in which they are intended to operate.

This class of access control system shall incorporate a central control and monitoring system whereby the central processor software can be used to generate reports on the status of any card. The overall system shall have sufficient redundancy to achieve an MTBF of 25 000 h, assessed in accordance with IEC 60050-191 and IEC 60300 (all parts).

3.6 Class 5 — Unique access card and personal identification number (PIN)

A class 5 access control system shall have at least the same features as a class 4 system but shall also use a PIN of at least four digits or use biometrics.

4. System role players/actors

The system shall have role players/actors as defined in table 1 below:

Table 1: IACS role players/actors

Actor	Role
Gate Access Operator	Allow Access at main/site entrances and exit
Reception Operator	Enrol/Register a Visitor
Registration Operator	Enrol/Register an Employee or Contractor
Employee/Contractor	• Pre-Register • Host a visitor • Visitor to another Eskom site • Card Holder
Visitor	External Visitor, Card Holder
Security Administrator	EBI Super user: Attend to alarms; site / zone update, setup and configuration of IACS
IT Administrator	IT System monitoring, troubleshooting and escalates issues
Control Room Operator	Monitor and Escalate Alarms
Security Manager	Generates Reports to Manage Security and Investigate.

5. Operational requirements

5.1 General operational requirements

The IAC (Integrated Access Control System) system shall be the standard Physical Access Control across Eskom with capabilities to integrate with CCTV, HVAC, building management systems and other security / business subsystems to provide a unified security management system . The system shall be capable of providing access control for Corporate Offices and buildings, Power Stations, Dx and Tx substations, Sites under construction, Control Rooms, Technical Services Centres, Customer Walk-in Centres, Laboratories, Water treatment plants, Visitor Centres, Stores, Workshops, Canteens, Medical Centres, Fire Stations, Boardrooms, Conference facilities, Maintenance or service centres, Server Rooms, Gyms, Kitchens, Boarding/Accommodation and Bus areas. The integrated Access Control system shall achieve the following general requirements:

a) The system shall be able to transfer data to SAP for Time and attendance data.

b) Each user authorization shall be uniquely definable.

c) Operator terminals shall be protected by an authorization.

d) All actions on the system shall be traceable and auditable.

e) The system shall allow for a company number to be changed when a contractor or visitor becomes a permanent employee with Eskom (i.e. a scenario must be allowed for whereby a person can initially be registered as a visitor/contractor and then upgraded to permanent employee status, without having to re-register the person).

f) The system shall be able to automatically disable a visitor or contractor on the required date of termination as entered by the registrar on the registration facility at the date of registering.

g) A visitor shall be disabled after leaving the site or designated place of visit/work, this function must be reversible whereby a person can be enabled should he require entering the premises again.

h) The system shall have a full anti-pass back facility to control the flow of personnel from one zone to the other, (i.e. once a person has successfully fingerprinted and has passed through the access control point, access must be blocked in terms of the zone he has just left – i.e. preventing a scenario whereby a person can allow another person through an access control point based on his fingerprint).

i) High risk areas access shall be granted only to personnel working in that area. Additional access shall only be granted if the necessary approval has been given by the responsible person of that area and shall be automatically disabled as soon as that person leaves the area.

j) The system shall allow for overrides, interlocking and other functions as they become necessary to operate and optimize the system by the administrator at a remote location.

k) The system shall be able to interface with existing software packages and therefore an open protocol software platform will be required.

l) The system shall allow for override functions on turnstiles and lanes in the event somebody is stuck in the system.

m) It shall be possible for the operator to bypass anti-passback rules selectively.

n) There shall be functionality to lock up systems for security reasons or open the system in case of an emergency.

o) System shall allow for online changes to be made.

p) Real-time online debugging shall be possible.

q) The system shall be either fail safe or fail secure, as required.

r) The application for change or update of access shall be completed on a standardised eForm.

6. Hardware requirements

6.1 Server requirements

a) The server shall comply with the requirements of SANS 2220-2-2.

b) There shall be an EBI based primary server where all the system configuration and event data is stored. The applications on this server shall run on Windows server with an SQL database.

c) There shall be an EBI redundant sever which is a mirror of the primary server. This server is used in case of primary server failure.

d) There shall be a regional server containing hardware configuration data for the region. This server subscribes the cardholder information of the primary server, and therefor shall have the same cardholders as on the primary server.

e) There shall be a test server which is a mirror of the primary server. The function of this server is to perform all testing related activities before moving the changes into production.

f) The sever shall automatically upload the transaction records from each reader and place the uploaded data into a database.

g) The server shall automatically back up data, this data shall be stored for a minimum period of 36 months.

h) There shall be LAN points for servers with connectivity to IAC VLAN.

i) There shall be servers that handle administration at each site that can be diverted to a central server that is situated at control centre.

j) The server be able to handle the automatic deletion of visitor and contractor account/profile after the expiry date.

k) The server shall be able to handle the deletion and removal of redundant account/profile based on information received from an administrator workstation.

l) IP 65 Wall mount cabinets shall be used for servers, these shall be housed inside the nearest guard house or access control building.

m) The server shall have an MTBF (mean time between failures) (guaranteed by the supplier) of at least 15 000 h, assessed in accordance with IEC 60050-191 and IEC 60300 (all relevant parts).

n) The sever shall be of a modular design.

o) The server shall contain a hard-disk drive or similar device with an MTBF (guaranteed by the supplier) of at least 15 000 h under continuous operation.

p) The server shall contain a real-time clock circuit capable of maintaining and displaying real time (month, day, hour, minute and second).

q) Interface between the server and the peripheral devices (such as readers and reader controllers) shall be by means of standard communications protocol.

r) Server decision making process shall not exceed 1s.

s) The server shall allow entry to the system parameters by password only, and there shall be at least three levels of password to allow three levels of access.

t) The server software shall maintain a real-time sequential record (on the hard disk) of reader 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.

u) The software and hardware for the server shall comply with comply with requirements of Table 1: EBI Server Platform Specification in Annex A of this document.

v) The server sizing shall comply with requirements of Table 2: Eskom standard Sever Sizing Specification (Per Server) in Annex A of this document.

6.2 Registration stations

a) The system administrator shall be a security personnel or appointed person

b) The registration facility shall enable appointed personnel to be able to register, disable, enable and change personnel details of employees, Visitors and other personnel onto the Biometric system for them to be able to gain access into the approved areas as approved by the designated management staff via the Biometric Finger print readers.

c) A full audit-trail shall be provided for all registration transactions.

d) Registration shall be fingerprint protected – i.e. the access control administrator shall be required to fingerprint in order to login to the registration application.

e) The registration stations shall be integrated to the Bio-Metric server.

f) Permanent employees shall only be registered once authorization has been given by the HR department. Registration should only be authorised when an Identity document and SAP company number are produced by the employee.

g) Visitors shall only be authorised for registration when a valid identity document is produced.

h) Contractors shall only be authorised for registration after producing a valid labour requisition form with start and end date captured and a valid identity document is produced.

i) Permanent employee's access rights shall only be disabled on request from HR department.

j) Visitors' access rights shall be disabled by the access control auto-disabling function at the end of the schedule visiting time/period.

k) Contractors and sub-contractors access rights shall be disabled once the term that is recorded expires. A reminder shall be generated by the system 48 hours prior to disabling the access rights.

l) The HR department shall notify the systems administrator to extend or terminate the access rights, the system shall generate automated reminders to the HR department and system administrators for access rights expiry dates.

m) The hardware and software for registration stations shall comply with the requirements of Table 3: EBI standard Registration Station Specification in Annex A of this document.

6.3 Client stations

a) The IACS shall use a client/server architecture

b) The client stations shall be used by the operator to view alarm/events and manage the system. This system shall have a standard Eskom desktop image loaded on to it.

c) The reception stations shall be used by the operator to manage visitors. This system shall have a standard Eskom desktop image loaded on to it.

d) The software installed on the client stations shall cater for the following requirements and customization options.

1) Screen modification programs.
2) Menu modification programs
3) Keyboard modification programs
4) Colour modification programs
5) Icon menu modification programs
6) System monitor programs
7) Logbook reset program
8) Graphical font modification program
9) System message modification program

e) The hardware and software for the client stations shall comply with the requirements of Table 4: EBI Reception Station Specification in Annex A of this document.

6.4 Readers and reader controllers (for both outdoor and indoor use)

a) It shall be possible to assign to any reader an IN or OUT function in any geographic area or any combination of areas.

b) It shall be possible for the operator to declare any reader as either card only, or card plus PIN, or to switch from one state to the other. The central processor shall automatically do the necessary status checking and send the appropriate command to the reader controller.

c) It shall be possible to attach a 10 character name to each reader to assist in identifying reader locations for record purposes.

d) It shall be possible to assign to any card reader a time and attendance function. This function shall be independent of the access control function. Time and attendance events shall be recorded sequentially in a separate record.

e) It shall be possible for the processor software to enable or disable any reader at any time or to switch from one state to the other. The central processor shall generate a report showing which readers are currently enabled or disabled.

6.4.1 Card readers

a) Card readers shall comply with requirements of SANS 2220-2-3.

b) A card reader shall accept access cards presented in one of the following ways:

1) swallow: the card is drawn into the reader for later retrieval;

2) swipe: the card is swiped through a slot in one direction past the reader sensor;

3) push: the card is pushed into a slot and then pulled out;

4) proximity: the card is brought within a specified angle and specified distance of the reader sensor.

c) Except in the case of proximity-type card readers, the reader shall use light-emitting diodes to show whether access was granted or denied. In the case of a stand-alone card reader, the response shall be within 2 s of presentation of the access card.

d) If a PIN keypad is included in a card reader, access shall only be granted when the card and its associated PIN have been validated.

e) The readers shall be configured to read the following 2 technologies simultaneously:

f) HID Prox

g) Mifare DesFire EV1 256-Bit AES

h) There shall be readers capable of reading Mifare Desfire EV1 cards and sends data via Wiegand standard data to a Wiegand interface.

i) A card reader shall be capable of indicating failures as well as an alarm condition.

6.4.2 Biometric readers

a) Biometric readers shall comply with requirements of SANS 2220-2-5.

b) A biometric device shall contain a sensor that recognizes a person's physical characteristics, such as:

1) fingerprints;

2) hand geometry (finger position and length);

3) retina patterns;

4) voice patterns; or

5) signature

c) If a PIN keypad (from which a personal identification number can be entered) is used, access shall only be granted on validation of both the PIN and the measured physical characteristics.

d) There shall be biometric readers capable of requesting biometric validation after presenting of Mifare Desfire EV1 card, then is shall send Wiegand standard data to a Wiegand interface.

e) There shall be biometric readers capable of requesting biometric validation after presenting of Mifare Desfire EV1 card, , then it shall send Wiegand standard data to a Wiegand interface, also it shall include a display of user interaction.

f) The MTBF (mean time between failures) of biometric readers shall comply with section 4.1.5 of SANS 2220-2-5.

g) If a biometric reader is connected to a central processor, it shall be by means of standard communications protocol.

h) The biometric device shall comply with all relevant health and safety requirements and regulations.

i) Markings for biometric readers shall comply with section 5 of SANS 2220-2-5.

6.4.3 Reader controllers

a) Reader controllers shall comply with requirements of SANS 2220-2-4.

b) A reader controller shall be used where a reader cannot be connected directly to a central processor.

c) Construction of reader controllers shall comply with section 4.1.1 of SANS 2220-2-4.

d) The MTBF (mean time between failures) (guaranteed by the supplier) of a reader controller (assessed in accordance with IEC 60050-191 and IEC 60300 (all relevant parts)) under normal operating conditions shall be at least 8 000 h.

e) All door controllers shall be connected and controlled from a dedicated server.

f) There shall be a controller with wiegand interface to the access control card/biometric reader that manages the physical door.

6.5 Goosenecks

a) Goosenecks with base plate and front mounting shall be provided, for cars these goosenecks shall be 1.1 meters high and for trucks these shall be 1.83 meters high.

b) Goosenecks for double height shall be provided.

c) The rain covers for goosenecks shall be capable of fitting an OMA520 reader.

6.6 Access Cards

a) Access cards shall comply with the requirements of SANS 2220-2-6.

b) An access card shall be made of a durable material that can display the following information, as required

1) an ID photograph;

2) a serial number;

3) a company logo;

4) a name, signature and other information of bearer.

c) Card printers shall be used to print the employee details and card layout on top of the cards before issuing.

d) The standard card format utilized by Eskom shall be Corp 1000 Desfire EV1 -128 Bit Encryption.

e) The cards shall have support for random ID.

f) Dimensions of access cards shall comply with section 4.1.2 of SANS 2220-2-6.

g) An ACS card encoder shall be used to encode cards by loading the required information regarding the card owner before issuing of the card, attempting to change the code shall destroy the card.

h) A Life Cam HD Photo ID Camera shall be used to capture the photograph of the card holder before issuing the card.

i) It shall be possible to laminate an access card by means of a hot or cold lamination process. It shall be possible to punch a hole in the card to allow a carrying clip to be fitted. The appropriate laminating process and the punch location shall be identified in the manufacturer's documentation.

j) The card shall be water resistant and resistant to wear and tear caused by extended use.

k) The location of the contacts and the microchip shall not cause surface irregularities on the back of the card or in the magnetic stripe area.

l) It shall be possible to print a list of all card numbers and their cardholder names which conform to a combination of specific and non-specific parameters.

m) When so required, the central processor shall be able to provide a print-out of all activities of a card.

6.7 Barriers

a) A barrier shall be one of the following devices intended to prevent unauthorized access to a controlled area:

1) an access booth;
2) a door (with door closer or monitor or both);
3) a vehicle boom;
4) a vehicle gate;
5) a vehicle stopper;
6) a turnstile.

b) A barrier shall at minimum, consist of the following components:

1) a physical barrier;
2) a detection unit ;
3) an interface to a control unit operated manually or by some access control facility;
4) a forced entry alarm; and
5) a tamper protection device.

c) The mean time between failures (MTBF) of a barrier shall be such that, under normal operating conditions, there are at least 100 000 operations with specified maintenance and 50 000 operations without maintenance. In the case of barriers of width more than 4 m and up to 10 m, the number of operations shall be 50 % of the above, and in the case of barriers of width more than 10 m, the number of operations shall be as specified by the manufacturer.

d) When an access booth is tested in accordance with section 6.3 of SANS 2220-2-7, the mechanism shall be activated by the access control system and an override switch. In the case of a power failure, the outside door of the booth shall unlock automatically, and the inside door shall lock automatically. The booth shall have a preset timer to re-lock the door if the booth was not used within 30 s after a door has been unlocked.

e) A panic alarm facility shall be provided on the inside of the booth, to allow any person trapped inside the booth to initiate an alarm.

f) If a booth malfunctions, it shall be possible to unlock the door from the outside with an emergency key override.

g) A barrier shall have the necessary potential free contacts to indicate status (open/closed).

h) A cubicle shall be so constructed that it is possible to anchor the booth to a solid base by means such as expanding bolts.

i) A class 4 or class 5 access control system using an access booth shall have a system to detect when more than one person is using the booth. In such a case, access shall not be granted.

j) The operating mechanism of the access booth shall have a locked cover equipped with a tamper protection switch.

k) Turnstiles and booms

1) Turnstiles shall comply with section 4.7 of SANS 2220-2-7.

2) A vehicle boom shall consist of the following components:

- an enclosure for the operating mechanism;
- a boom;
- detector loops;
- a warning device;
- a mechanical crank;
- an operating mechanism;
- a boom rest (for a boom longer than 4 m).

3) The boom shall be able to be activated by a manual switch and some electronic means such as a reader controller.

4) The enclosure of an operating mechanism for a boom shall comply with the requirements for class IP45 of SANS 60529.

5) Doubles entry full height turnstiles shall be installed at main entrances.

6) Waist height turnstile shall be provided.

7) A Card capture unit shall be used for visitors to capture the card on exit.

8) Three meter vehicle barriers with ground loop sensors shall be installed.

9) Dual height gooseneck pedestals with rain covers, sized for 500 series OMA biometric readers shall be installed.

10) Detector loops shall be so constructed that they can be buried in a road to detect vehicle movement. The boom shall close only after the vehicle has moved over the loop.The boom shall lower 30 s after it has been raised. The sensitivity of the detector loops shall be adjustable.

11) Each boom shall incorporate a warning device such as lights or a siren, to indicate when the boom is in operation (opening or closing).

12) In case of a power failure, it shall be possible to mechanically raise and lower the boom.

13) The bearings of the boom shall be self-lubricating and maintenance free.

14) Wiegand interface modules shall be installed for boom gates, mounted inside one of the boom enclosures behind the maintenance lid, mounted on din rail.

15) One wiegand interface shall be installed for two readers, the interface units shall be housed on top of the turnstile under the maintenance lid, mounted on din rail.

16) Maximum run of wiegand bus between readers and Wiegand interfaces modules shall not exceed 150m.

17) Sagem OMA 520D biometric readers shall be installed for entry and exit points.

18) Fire override input shall be made available.

19) Turnstiles shall be powered by UPS or ordered with battery backup.

6.7.1 Doors

a) There shall be door monitors used to monitor status of the door.

b) Electromagnetic locks with specific beak force capacity shall be used, the maglocks shall be released with an authorized access card.

c) Door closers shall be used to keep the doors closed and locked.

d) All doors shall be fitted with a resettable break Glass unit. When the break glass is triggered, it shall override the door access and keeps the door unlocked. The break glass shall only be used during emergencies.

e) An electronic push bar shall be used on the fire exit doors to open the emergency escape from within the building.

f) Manual key overrides shall be installed for all critical doors; these should be wired in line with the break glass unit to cut power to any connected locks. The manual key overrides shall be mounted on the outside of entrances to critical areas, such as control rooms, server rooms and main entrance doors.

g) The door movement shall stop when the door meets an obstruction, e.g. a person, and an obstruction alarm signal shall be initiated.

h) There shall be a provision for exit pushbuttons.

i) All bearings of the doors shall be self-lubricating and maintenance free.

j) There shall be a wiegand interface mounted inside small enclosure located in the ceiling void, or mounted inside a central enclosure where multiple doors are access controlled within a small geographical area.

k) There shall be an electronic normally closed recessed door contact for door status.

l) There shall be an input/output module mounted inside small enclosure located in the ceiling void, or mounted inside a central enclosure where multiple doors are access controlled within a small geographical area to monitor fire escapes.

6.7.2 Vehicle gates

a) Motorized or hydraulic vehicle gates shall have the following components:

1) an enclosure for the operating mechanism;

2) an operating mechanism consisting, for example, of

- an electric motor for electrically operated gates, or
- a pump complete with gears and valves for hydraulically operated gates;

3) a control box (for electronic control or key switch operation);

4) a status detector mechanism;

5) an obstruction detector mechanism; and

6) a warning device.

b) There shall be an enclosure with locked cover that gives access to the operating mechanism, gears, etc. The cover shall be equipped with a tamper protection switch, and shall comply with the requirements for class IP45 of SANS 60529.

c) The operating mechanism shall be so constructed that a person could not physically move it from the closed to the open position without using special tools.

d) A sliding gate drive shall move the gate at a speed of at least 10 m per minute.

e) A swinging gate drive shall move the gate by 90° in not more than 20 s.

f) The control box shall have a locked cover that gives access to the electronic components. The operation of the gate shall be initiated by means of a PIN code, card reader or key switch attached to the control box.

g) The status detector mechanism shall indicate correctly whether the gate is open or closed.

h) The vehicle gate movement shall stop when the gate meets an obstruction, e.g. a vehicle, and an obstruction alarm signal shall be initiated.

i) Each vehicle gate shall incorporate a warning device such as lights or a siren, to indicate when the gate is in operation (opening or closing).

6.7.3 Vehicle stoppers

A vehicle stopper shall comply with requirements of section 4.6 of SANS 2220-2-7.

7. IACS device configuration for 3 tier fenced sites

Sites including power stations, Tx and Dx substations and Telecoms high sites etc. with 3 tier fences (outer, middle and inner fences) shall at minimum have the ACS devices configured as stipulated in table 2 below:

Table 2: ACS device configuration for 3 tier fenced sites

Area	Point	Device	Status Contact	Lock	Evacuation Device	Bypass
Main Gate (Inbound traffic)	Exterior Perimeter Fence (Gooseneck Mount)	Card + Biometric Reader	Gate Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Energized Fence Gate	Card + Biometric Reader	Gate Status Contact	Magnetic Lock	None	Mechanical Bypass
	Inner Perimeter Fence (Gooseneck Mount)	Card Reader	Gate Status Contact	Magnetic Lock	None	Mechanical Bypass
Outbound Traffic	Exterior Perimeter Fence (Gooseneck Mount)	Card Reader	Gate Status Contact	Magnetic Lock	None	Mechanical Bypass
	Energized Fence Gate	Card Reader	Gate Status Contact	Magnetic Lock	None	Mechanical Bypass
	Inner Perimeter Fence (Gooseneck Mount)	Card + Biometric Reader	Gate Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
Yard Access Gate	Exterior Perimeter Fence (Gooseneck Mount)	Card Reader (In) & Card Reader (Out)	Gate Status Contact	Magnetic Lock	None	Mechanical Bypass
Guard House	Entrance Door	Card + Biometric Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Server Room Door (Inside)	Card + Biometric Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
Oil Store (where applicable)	Double Door	Card Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass

Area	Point	Device	Status Contact	Lock	Evacuation Device	Bypass
Control Room Building	Office Door	Card Reader (In) & Card Reader (Out)	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Control Room Entrance Door	Card + Biometric Reader	Door Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Control Room Back Door (Emergency Exit)	None	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
HV Yard	Entrance Gate 1 (Pedestrian)	Card Reader (In) & Card Reader (Out)	Gate Status Contact	Magnetic Lock	Glass break	Mechanical Bypass
	Entrance Gate 2 (Emergency exit)	Card Reader (In) & Card Reader (Out)	Gate Status Contact	Magnetic Lock	Emergency Exit Button	Mechanical Bypass
	Entrance Gate 3 (other)	None	Gate Status Contact	None	None	None

8. Integration requirements

8.1.1 General

The IAC system is an efficient access control system. The selected EBI security technology is the standard for Physical Access Control across Eskom.

Enterprise Buildings Integrator (EBI) is a modular system with capabilities to serve as a “security backbone” and is capable of catering for future business requirements of integration with CCTV, HVAC, building management systems and other security / business subsystems to provide a unified security management system. The IAC system shall be integratable with the EBI core infrastructure.

8.1.2 Integration with Intrusion Detection System

a) The intrusion detection system shall be integrated with the Access Control System. The system shall predominantly focus on the securing of specific areas with two primary purposes, namely;

1) to detect if entry is gained into a secure area by any unauthorized manner; and

2) to verify that operational procedures are adhered to from a safety perspective (areas such as the HV Yard, Control Room and Battery Room)

b) Access control at all access points onto buildings and all buildings shall use an intrusion detection system which consists of a PIR and Door Contact to verify the status of the room when it is supposed to be unoccupied and subsequently generate an alarm if an intrusion is detected.

8.1.3 Integration with Access gates

a) Where applicable, gates shall be automated with industrial grade sliding gate operators. The gate operators shall be installed within the fence line with the exception of the inner perimeter gate which must be installed on the inside of the inner perimeter fence to allow access to the operator in case of failure.

b) Verification process at entrances shall be as follows:

1) Upon positive verification the energized fence gate shall open after which the outer barrier gate will open to allow the vehicle inside the sally point.

2) Upon entry into the sally point the outer barrier gate will close effectively locking the visitor in the sally point.

3) At this time the guard will be able to interact with the visitor and conduct searching of the person and vehicle.

4) Only after the guard has completed his duties will the guard exit the sally point at which time the guard has to tag on the inside of the guard house to verify the completion of his activities.

5) The guard in turn will be required to tag on the inner perimeter pedestrian gate to enter the sally point, and then tag out of the sally point and only then tag in the guard house before the system will open.

6) This logic followed will force the guard to enter the sally point and conduct the searching rather than just tagging a visitor in through the guardhouse point.

7) When the visitor on his turn can then again tag in the reader in the sally point (Card reader only).

8) At this time the inner gate will open to allow the visitor into the restricted area.

9) Exiting of the site will be the reverse operation of the entry sequence.

8.1.4 Integration with intercom system

a) A video intercom system shall be installed at main gate entrances and the audio feed and camera feed from the unit shall be integrated into the local DVR to ensure both visual and audio recording of events.

b) Guards shall be able to interact with unannounced visitors and non-Eskom staff whom might not be accredited without leaving the safety of the guard house.

c) The communication shall be point-to-point between the gate and guard house and shall not be integrated with the gate control system.

d) The intercom function shall be extended to the control room office for intercom operation during daytime hours when guards will not be on duty.

8.1.5 Integration with CCTV system

a) The CCTV system shall be an IP based smart solution with the capability to integrate with the EBI Video Module for upstream video integration and streaming in emergency events.

b) A CCTV system shall provide the local guards with a single point from where they can view and verify alarm events from the pre-detection and energized fence triggers.

c) Guards shall be able verify positive alarm events in the event of an attempted or successful intrusion attempt on the fence system.

d) CCTV monitoring shall be conducted at the main vehicle entrance as an overview of the area and to serve as identification point for visitors.

e) The system shall utilize a video analytics system as pre-detection to automatically create alarms and perform event recording.

f) The CCTV system shall be integrated with video analytics installed on the outer perimeter fence units, and shall automatically record any alarm event on the fence by means of the 30second pre-event buffer, the actual event (For however long motion is detected by the camera) and at least a 30 second post event time period.

g) The CCTV system shall be connected to the Eskom WAN to enable event driven video streaming to Zero Control and ultimately the NSCC at MWP. Sufficient bandwidth to enable this requirement shall be installed.

8.1.6 Integration with security fences

a) This perimeter detection systems of the security fences shall be integrated into the IAC and CCTV systems to ensure effective access monitoring and control both locally and remotely.

8.1.7 Integration with security lighting

a) Security lighting shall be integrated with the ACS and CCTV system such that it provides a bright perimeter for guards to observe the perimeter during evening patrols and in situation where responding to fence alarms.

8.1.8 Integration with Guard Tour System

a) Guard Tour System shall be integrated to the ACS to serve as a control measure to monitor compulsory patrols on site and to act as a safety system to alert the control room of the patrol incident, where a guard fails to clock at a point within the allowed/ prescribed time limits so that investigation can be conducted into the whereabouts and safety of the guard.

8.1.9 Integration with the PA system

a) The PA system shall be used to engage potential intruders and issue warnings before the intrusion takes place as a deterrence measure. The system shall be operable via the guard house and remotely via the responsible control rooms to warn attackers of the restriction of access to the site. Voice recordings must be synchronized with the cameras and recorder on the local NVR via audio input to ensure synchronization of events.

9. Buildings access control

a) All entry points into buildings shall be secured by the Access Control system.

b) All windows shall be protected by burglar proofing, apart from areas where HV Regulations require otherwise.

c) All non-automated doors shall be fitted with a suitable grade security lock.

d) In the administration building all offices shall have security gates installed on the doors, a suitable key control system shall be introduced to manage access to offices and the safekeeping of duplicate keys.

10. Databases

10.1 General database requirements

a) Database shall provide for regular reports and specific database queries.

b) The system shall allow for Logbook entries with the following as minimum features:

1) Alarm logbook for alarmed events generated by the system or peripheral devices

2) System logbook for all actions performed on the system

3) Event logbook for all events generated by the peripheral devices or by programs that are started up automatically in the background

4) Access logbook from all the readers

5) Time logbook for all time management related readings received from all the readers

6) Trend logbooks

7) Error logbook which is used for system errors as well for unauthorized access requests

8) Visitor logbook

9) Video logbook

c) Database reports shall provide for the following functions:

1) Time and Attendance

2) Personnel tracking (Individual's historical movements to and from the various access points)

3) Date and time movements of Individuals or groups through the system

10.2 Database structure

a) The database shall allow for the following information to be included:

b) Eskom company number

c) Access ID (this shall be generated automatically by the system)

d) Full names and surnames

e) ID Number

f) Selection of access levels whereby the level where access is required is selected at the registration facility

g) The employee status shall be either of the following:

1) Eskom employee

2) Sub-contractor

3) Visitor

4) Contractor

5) Security services

6) Vendor (to be used for regular visitor)

11. Alarms

a) The system alarms shall comply with Specification for Integrated security Alarm system for protection of Eskom installations and its subsidiaries (240-86738968).

b) Where access control and alarm monitoring are carried out on the same central display screen, the central display screen shall:

1) Serve as a logged message output device and an operator's screen;

2) Be capable of being used as an alarm display terminal;

3) give the alarm message the highest screen priority and cause it to override all other displays, but it shall be possible to recall the last text display by acknowledging the alarm display; and

4) While the screen is being used by the operator for card or system programming, allow logging to occur.

c) Error messages shall cause a beep tone to be sounded. The message shall stand until the error is acknowledged by the operator. All events printed on the printer shall include the time of the event to the nearest second, and details of the event.

d) System shall have the following alarms capabilities:

1) Alarm handling screen

2) Graphics associated with alarms

3) Alarm classification

4) Report back facility why the alarm occurred

5) Logging of all transactions in the alarm logbook

12. Communication and network requirements

a) The network infrastructure shall adhere to the principles laid out in the following Eskom Documents:

1) 240-55410927 - Cyber Security Standard for Operational Technology

2) 240-55683502 - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities

b) The network provided shall link all the controller servers and client stations

c) There shall be a LAN points for servers with connectivity to IAC VLAN.

d) There shall be LON bus provision from servers to IACS field devices, this can be extended beyond 1km with LON repeaters.

e) Severs shall be configured with static IP addresses.

f) A multicore cable shall be used from Biometric readers to Wiegand interfaces.

g) A card reader shall be connected to the reader controller by means of standard communications protocol or a 20 mA current loop. This connection shall be protected against induced voltage surges.

h) All reader controllers shall have interface capabilities stipulated under section 4.1.3 of SANS 2220-2-4.

i) System shall cater for the following I/O ports

1) Ethernet 10/100 Base T

2) RS-232

3) RS-485

4) Wiegand in/out

5) TTL in/out

6) Modem

12.1 Cyber security

a) The system shall comply with Eskom' Cyber Security standard for Operational Technology (240-55410927)

13. Power supply

a) The power unit of an access control system shall comply with the requirements of SANS 2220-1-7.

b) There shall be an intelligent power supply that monitors incoming power, battery status and only supply power to the servers.

c) There shall be a backup battery that ensures at least 4 hours autonomy.

d) The system shall still operate in the event of a main power failure.

e) 12VDC 4A Power Supply with battery backup for readers shall be provided.

f) The battery system shall be maintenance free with a 3 year guarantee.

g) Each system or subsystem shall have a dedicated circuit breaker and supply circuit.

h) There shall be UPS with sufficient capacity to support all equipment for at least 1 hour.

i) There shall be provision for POE.

j) Electro-magnetic radiation from the UPS shall not affect the operation of other electronic equipment in the equipment room

k) The battery system shall be maintenance free with a 5 year guarantee.

14. Cabling requirements

a) Cables shall comply with the requirements of Eskom's Standard for Wiring and Cable marking in Substations (240-64636794)

b) Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.

c) All wiring shall be concealed inside trunking or conduit. No exposed wiring will be accepted.

d) Cabling in roof or floor voids shall be installed in cable trays. Where cable trays are not available or viable, conduit will be acceptable.

e) Cabling in trays shall be tied off at a maximum of 1.5m interval.

f) Data and low voltage (0-48V DC/AC) cable installations shall be separated from mains power installations by a minimum of 500mm.

g) Where data and low voltage cabling has to cross power cabling, this shall always be at 90° angles.

h) Cabling in manholes shall be kept above the manhole floor level to avoid water contact.

i) Cable shall be handled with care and not pulled with excessive force that may cause internal damage.

j) The installer must adhere to the drawings and specifications at all times. Where a discrepancy exists between a drawing and these specifications, the higher of the two standards is to be followed.

k) The installation contractor shall provide detailed as built drawings indicating cable routes, installation locations and unique equipment identifiers on completion of each logical section of an installation.

l) Cables are not to be bent at a radius of less than four times the diameter of the cable or tighter than specified by the manufacturer.

m) There shall be no cables running next to devices that may cause electro-magnetic interference.

n) Tensioning of cables shall not exceed 10kg.

o) Correct wiring schematic shall be followed.

p) All wiring shall be terminated with bootlace ferrules of the appropriate size and colour to match the cable.

q) All bootlace ferrules shall be properly crimped and shall have good mechanical and electrical connection.

r) A dedicated ferrule crimper when crimping bootlace ferrules shall be used. The use of side-cutters , pliers or other tools for crimping is not acceptable.

s) No short circuits shall be caused when cutting cables

t) Where cables are laid in trenches, they shall be armoured

u) Cable trenches shall be excavated according to the Standard Technical Specification. Trenches shall be 600 mm deep measured from average ground level to the top of the upper sleeve or cable. Contractors shall allow for the excavation, bedding, laying of cables and sleeves and graded back-filling of all trenches as specified.

v) Where any power reticulation work has been undertaken, contractors shall make provision to submit an approved reticulation certificate issued by an authorised electrical Contractor.

w) With respect to site cabling, no cable joints shall be accepted between buildings and control room. In the event that the distance exceeds the length of a standard cable drum, the Project Manager's ruling shall be obtained. The Project Manager will then determine where the cable may be joined and which jointing materials would be acceptable. The Contractor shall indicate the positions of all joints on the final as-built Drawings.

15. Physical requirements

15.1 Tamper protection

a) Tamper protection for the electrical components of the IACS shall be in accordance with section 4.10 of SANS 2220-2-1 such that the following shall not be possible:

1) To Alter the enclosure arrangement without causing an alarm signal to be generated;

2) To gain access to the electrical circuits, adjustment controls and temper protection devices without the tamper protection device causing the component to generate an alarm signal

3) To disable the tamper protection device by means of normally available tools such as knives, pliers and screw drivers.

Compliance is checked in accordance with section 6 of SANS 2220-2-2: *tamper protection test*

15.2 Ingress protection

a) The enclosures for the electrical and electronic circuits shall, unless otherwise specified, provide protection of class IP41 in accordance with SANS 60529.

15.3 Safety

a) 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.

16. Environmental requirements

16.1 General

a) Access cards shall comply with environmental requirements of 4.2 of SANS 2220-2-6.

b) Biometric readers shall comply with environmental requirements of 4.2 of SANS 2220-2-5.

c) Servers/central processors shall comply with environmental requirements of 4.2 of SANS 2220-2-2.

d) Card readers shall comply with environmental requirements of 4.2 of SANS 2220-2-3.

e) Barriers shall comply with environmental requirements of 4.8 of SANS 2220-2-7.

16.2 Operating conditions

a) All the elements of the IACS shall be able to function in all climatic conditions prevailing in South Africa, without the performance being out of limits or the life cycle being shortened:

b) The system and associated equipment shall be protected against dust and any other coastal condition such as corrosion.

c) Mechanical shock and vibration shall not affect the functioning of the system and associated equipment for the life cycle of at least 20 years.

d) Protection shall be provided for short or long term over voltages or under voltages, impulses, transients, spikes, surges, brownouts, mains borne interference's or power failures and the equipment shall be suitable for continuous and reliable operation under these circumstances.

e) The equipment shall not generate any interference, which could hinder its own performance or the performance of the other equipment in its vicinity.

16.3 EMC requirements

a) Signal, voltage and electromagnetic radiation levels in readily accessible areas shall not be dangerous.

b) System and its components shall comply with requirements of SANS 61000-1-2.

16.4 Earthing

a) Earthing of equipment shall comply with latest Eskom earthing standard.

17. Labelling and numbering

a) Terminal boxes and terminals shall be numbered and labelled accordingly.

b) Numbering and labelling shall be executed in such a way that it can be guaranteed that a maintenance artisan can trace wiring (cores) with the as-built information only.

18. Markings

a) Markings for access cards shall comply with section 5 of SANS 2220-2-6

b) Markings for biometric readers shall comply with section 5 of SANS 2220-2-5.

c) Markings for servers/central processors shall comply with section 5 of SANS 2220-2-2.

d) Markings for card readers for shall comply with section 5 of SANS 2220-2-3.

e) Markings for barriers shall comply with section 5 of SANS 2220-2-7.

19. Inspections and methods of tests

a) Inspections and methods of test for servers/central processors shall comply with section 6 of SANS 2220-2-2.

b) Card reader inspections and methods of tests shall comply with section 6 of SANS 2220-2-3.

c) Inspection and tests methods for biometric readers shall comply with section 6 SANS 2220-2-5.

d) Inspection and methods of tests for reader controllers shall comply with section 6 of SANS 2220-2-4.

e) Inspections and methods of tests for access cards shall comply with section 6 of SANS 2220-2-6.

f) Inspections and methods of tests for barriers shall comply with section 6 of SANS 2220-2-7.

20. Spares

a) All emergency spares shall be held by the Contractor. Eskom shall not be required to hold any spares. The Contractor shall hold sufficient stock of all critical spares and consumables required for the due and proper performance of his obligations in terms of the Maintenance Contract as specified in this document.

b) A 10% spares holding is required.

21. Maintenance

a) Maintenance procedures shall be provided

b) The estimated maintenance frequency and durations shall be specified

c) A repair procedure shall be specified (e.g. on site repair, bring in repair, fixed price exchange) and shall include current costs and time to repair.

d) Spares for the system shall be available 10 years even after the model has been discontinued.

e) The equipment shall have a minimum of two years guarantee.

f) A warranty repair schedule shall be provided.

22. IACS processes and associated activities

22.1 General

This section contains requirements for the IACS processes and their respective activities.

22.2 Employee and contractor Enrolment

22.2.1 Validate employee / contractor

a) Verify photo ID

b) Approval of access

c) Validity of criminal verification

d) Validity of health records

e) Validity background check

f) Validity of qualifications

22.2.2 Enrol user into security system

a) Verify vehicle registration number

b) Verify / capture contact number/s

c) Capture / verify asset Serial number for laptop

d) Capture photograph

e) Select and add the behaviour model/access right

f) Choose card type/layout (Contractor/Permanent)

g) Print access card

h) Capture biometric fingerprints / PIN code

i) Load biometric fingerprints / PIN code, card number, name and Ssurname to the Mifare portion of the access card.

j) Issue access card

22.2.3 Test card

a) Shall badge the card and test biometric fingerprint on a reader

22.3 Maintaining access (renew/change access rights)

22.3.1 General

In the event that an individual's location changes, if they have been promoted or for any other reason that would impact the access level they have to be changed, the individual is required to go through the security process of Access Right change. This must be a form that has been completed with all relevant information of the individual as well as the approving Line and Facility Managers. The approval process must finally reach the respective site's Security Manager before access may be granted on the individual's security profile.

A security operator shall perform the change of access rights to the respective individual's profile once the approvals have been completed for the change in access.

22.3.2 Validate employee / contractor

a) Verify photo ID

b) Approval of access

c) Validity of criminal verification

d) Validity of health records

e) Validity background check

f) Validity of qualifications

22.3.3 Select and add/remove the behaviour model/access right as per the approved form

Although an individual may be granted approval for access for sensitive areas / sites such as a power station, the individual is required to comply with the site specific rules before gaining entry to the site e.g.: Complete the safety and security induction, Medical checks must have been completed.

22.4 Re-issuing of Access Card

22.4.1 General

Any individual (Employee, Contractor, Visitor etc.) on the Integrated Access Control System must have only one access card assigned to his / her security profile. In the event that an access card has been lost, stolen or the individual has been promoted / demoted, the individual would have had to report it to the security operator/office. The process for re-issuing an access card should be followed and must contain the following activities:

22.4.2 Search and open the individual's profile

a) Verify Name, Surname, Employee (Unique) number, photograph

22.4.3 Validate employee / contractor

a) Verify photo ID

b) Approval of access

c) Validity of criminal verification

d) Validity of health records

e) Validity background check

f) Validity of qualifications

22.4.4 Remove the access card from the individuals profile

a) Issue another access card

1) Print Access Card

2) Update Card number that is linked to the Biometric Fingerprints

3) Re-load Biometric finger prints and new Card Number to Mifare on the access card

22.4.5 Test Card

a) User shall badge the card and test biometric fingerprint on a reader

22.5 Physical access termination

a) Termination shall occur on the Integrated Access Control System when:

1) Contract is completed or expired (for a contract worker)

2) Sanction is applied (for a supplier)

3) A change in HR data that indicates a requirement for access termination (where an employee has resigned, retired, is deceased etc.)

b) The process for termination shall be handled by the System and its Integration with the SAP-HR. The IACS shall receive flags for the individual that is to be terminated. The Security Manager will be responsible for completing the termination process for that individual.

c) A manual suspension of access is also required as not all incidents will come from the SAP-HR system. Security or other management may enforce a suspension of access for an individual due to an incident that has occurred.

d) Further to removing access rights from an individual's profile, the access card attached to his / her profile also needs to be removed. When an individual's access has been terminated from Eskom and his / her access has been revoked on the Integrated Access Control System, the Operator shall remove the access card off an employee/contractor's security profile.

e) Visitors' access shall be automatically disabled on the system on exit or; The card on the respective visitor's profile may be disabled in the event of a security breach / incident requiring access revoking.

22.6 Visitor management

a) This is the process of registering visitors for temporary access to any Eskom premises. Visitor management is broken down into two main categories namely:

1) Gate management: This is done at the site entry and exit points

2) Reception management: This is the management of visitors within a building / site from the reception area

b) Visitors may be categorised into planned visitors, unplanned visitors, conference visitors and ad-hoc contractors.

c) Visitor Management shall include host tagging functionality or security escorting depending on the site type.

d) The overall process for visitor management shall include the following activities:

1) Pre-registration / Registration of a visitor
2) Vehicle Tagging
3) Verification of Visitor
4) Tagging visitor with a host for specific sites
5) Escorting of a visitor (based on site rules)
6) Granting visitor access
7) Granting visitor access

22.7 Gate Management

a) Gate Management has been identified as the first process of Physical Access Control. It is a requirement that IAC makes available technologies that has the capability to scan the following:

1) Vehicle licence disc,
2) Driver's id or driver's licence and
3) Driver's biometrics within a maximum of 30 seconds.

b) It is required to tag a vehicle to a driver at the gate and pass on this information to the reception desk prior to the visitor arriving at the reception.

c) It is a requirement for the security at the gate to be able to verify the captured details on Exit to ensure that the same driver is driving out the same vehicle with which he/she had entered with.

d) The software system for Visitor Management at the main entrances to site is required to allow for the following:

1) Vehicle barcode (license disc) scanning
2) ID barcode scanning
3) Driver Licence barcode scanning
4) Biometric fingerprint scanning

e) The system is required to link multiple people to a vehicle at sensitive and high priority sites

1) The system is required to generate reports from the data captured.

22.8 Reception Management

a) Access control for visitors is required to be managed via host or conference facility tagging.

b) Host Tagging: A visitor shall badge at a reader point followed by his/her respective host. Only then shall access be granted to the respective zone/access point.

c) In the case of conference facility tagging, a single badge will only be required by the visitor to access a point within that area.

d) In the case of an employee / contractor visiting another Eskom site, he /she will not require a host or host tagging in the General Access Area. This is only if the site is not a key / priority site and is also dependant on the site specific requirements.

e) In the case of an employee / contractor visiting another Eskom site, he /she will not require a host or host tagging in the General Access Area. This is only if the site is not a key / priority site and is also dependant on the site specific requirements.

f) The set of standard reports shall be the following:

1) Pre-registered visitors report
2) Visit history report
3) Visitors per host report
4) Visits per visitor report
5) Visitor details Report

g) Reception management application shall contain the following role based access to the application:

1) Supervisor – All web reception access rights
2) Operator – All web reception functional rights
3) View Only – Reporting access rights
4) Employee – Web reception pre-registration access rights

h) Eskom employees / contractors utilise a Novell Logon ID and password. The Web Reception must identify a user by this Logon ID when they access the web portal.

i) System shall contain a Web portal on Eskom's intranet site for employees and contractors to pre-register visitors or pre-register a visit to a different Eskom site as a visitor. The web portal shall follow the same theme as Eskom's other intranet sites.

j) System shall cater for LDAP authentication.

k) System shall cater for visitors to be pre-registered (planned) as well as registration of visitors in person (unplanned).

l) Planned visitors shall be pre-registered by their host on the Web Portal hosted on the Eskom Intranet.

m) Unplanned visitors shall be registered at the building reception area by reception operators

n) Pre-registration shall cater for the following:

1) Be done on the application's (Web Reception) standard Web interface
2) Send a Confirmation of pre-registration to the Host. It shall use the e-mail address stored on the Host's EBI profile.
3) Allow Lookup for previous registration/s
4) Edit/alter registrations
5) Cancel/Delete/Remove a registration/s
6) Allow the specific Employee to view his/her registered visitors

o) The pre-registration form shall provide the option for selecting the type of Visitor, i.e. External Visitor (from an outside company) or an Eskom Employee / Contractor that requires temporary access to visit another Eskom site.

p) The visitor shall have access rights assigned to him / her. This should be General access and could be the same as the Host's access rights where required.

q) Termination of access for visitors shall be an automated process and must be based on a 1 day visit concept. Exceptions can be made based on site types for visitors that are resident on the Eskom site. A visitor's card will be valid for use during the official working hours (8am – 5pm). For resident visitors the validity period should be tied to the stay period.

r) The visitor card template shall be aligned to the Standard Security Access Card layout for Employees and Contractors.

s) There shall be a separate card designed for VIP type visitors. This card should have VIP Guest printed in bold to easily identify these individuals.

t) The reverse side of the card shall contain the site name to which the card belongs together with the Security office and emergency contact numbers. The Eskom and site specific security rules must be printed on the back of the card.

u) Collection of a visitor's access card shall be an automated process and driven via a drop-box at the exit point. The visitor's card must be cleared of any access rights and unallocated from the visitors profile once it has been dropped into the box.

22.9 Reporting

The Integrated Access Control System must have Reporting capability. The system should have a set of standard off the shelf reports. The system must allow for custom development of reports. The business requirement is to build a set of custom reports that are specific to the Eskom environment and these reports should be a standard set of reports for any Eskom site nationally. Both standard and custom reports should have capability of being scheduled to run at specific dates and times and/or recurring. The system is required to contain functionality for reports to be e-mailed from within the application. The reports are required to have an export / save functionality for at least the following file formats: .xls, .pdf.

22.9.1 Customised System Reports

Table 3: Customised System Reports

Report Name	Description of Intended use	System type	Motivation
Attendance Register	Designed to replace the current manual attendance registers.	Parameters: Start date; end date; site; zone; behaviour model	Business requirement to replace manual attendance register.
Cardholders Per Behaviour Model	Designed to ensure accuracy of assigned access rights per employee.	Parameters: Site; behaviour model	This report is distributed to designated signatories for validation of assigned access rights.
Cards issued per day	Details the amount of access cards issued.	Parameters: Start date; end date	Business Requirement to control stock of cards.
Clock History	Records history of clock IN and OUT dates and time.	Parameters: Start date; end date; employee number; site; cost centre	Business requirement to manage employee traffic flow.
Doors Per Behaviour Model	Designed to ensure accuracy of assigned doors per entry and exit point.	Parameters: Site; behaviour model	This report is distributed to designated signatories for validation of assigned doors.
Employee List	Custom report which lists employee details imported into EBI.	Report	To test the accuracy of the information imported and captured.
Enrolment Status	List all employees who have an enrolled biometric element.	Report	Business requirement to test occurrence of enrolment.
Health and safety	Health and safety report.	Parameters: Start date; end date; employee number; site	Business requirement to be used by health and safety in the event of an emergency.
Integrity Report	Test the validity and accuracy of information across the EBI platform.	Report	Business requirement to act as an internal control.
Security Management Report	Highlights all alarms in EBI that are triggered or tampered with.	Parameters: Start date; end date	Designed to act as a control to manage access.
Zone Access Per Behaviour Model	Tracks unauthorised entry.	Parameters: Start date; end date; site; zone; behaviour model	Business requirement detailed report to highlight intrusion.
Zone History	Zoning with detail of areas being accessed.	Parameters: Start date; end date; cost centre; zone.	Business requirement to track movement within premises.

22.9.2 Attendance Register

1) A field labelled “Flexible time” must be added to the report as this is currently contained in the manual attendance register form. Managers and staff often agree on Flexible time and the hours. This information is passed onto the HR department. A “yes / no” value should populate the Flexible Time field to indicate to a person looking at the report that the individual has an earlier / later start and end time due to the flexible time agreement.

2) A filed labelled “Leave” must be added to the report as this is currently contained in the manual attendance register form. A “yes / no” value should populate the Leave field to indicate to a person looking at the report that the individual is not just absent from work but on Leave.

3) A filed labelled “Leave Type” must be added to the report to enable Management viewing the report to understand whether a person is on their Annual leave or sick leave etc.

22.9.3 Clock History:

The following fields must be added to this report:

a) Site

b) Area

c) Zone

22.9.4 Visitor reports

a) Visitor reports shall comply with the requirements in table 5 below:

Table 4: Visitor reports requirements

Report Name	Description	Report Input			Report Header			Report Output Fields		
Pre-registered visitors report	Provides a list of visitors that are / have been pre-registered on Web Reception	*Date	Site Name	-	Report Name, Period for Report	Date of Pre-registration	Site Name	Visitor Name	Visitor Last Name	-
Visit History report	Provides a list of visitors that have visited a or all sites in a specific period	*Date	Site Name	-	Report Name, Period for Report	Visitor Name	Date and Time of Visit	Site Name	Host Name	-
Visitors per Host report	Shows the visitors that a host has had over a specific period of time	*Date	*Host Name	-	Report Name, Period for Report, Host Name	Visitor Name	Date and Time of Visit	Site Name	-	-
Visits per Visitor report	Shows a visitor and their visits to a / all Eskom sites	*Date	Site Name	*Visitor Name	Report Name, Period for Report	Date and Time of Visit	Site Name	Visitor Last Name	Visitor First Name	Host Name
Visitor Details report	Displays all the captured details of a visitor from registration / enrolment	*Visitor Name	-	-	Report Name, Visitor Name			All Visitor Registration Fields		

22.9.5 Visitor/Host registration information

The system shall cater for the following information fields on information forms and databases to facilitate the ACS processes.

22.9.5.1 Pre-registration information

Table 5: Preregistration information/fields

Required Functionality	Current Functionality	Importance	Mandatory
Form Attributes		L/M/H	
Main Menu			
Search	X	H	
Pre-registered Visitors	X	H	
Previous Visitors	X	H	
Visitor Personal Info			
Visitor Last Name	X	H	X
Visitor First Name	X	H	X
Visitor Company	X	M	
Date of Birth	X	M	X
ID / Passport Number	X	H	X
Telephone Number	X	M	X
Cell / Mobile Number	X	H	X
E-Mail Address	X	M	
Date of Visit		H	X
Time of Visit	X	H	X
Vehicle Registration	X	H	X
Duration of visit	X	L	
Meeting Room	X	M	
Reason for Visit		M	X
Comments / Notes		M	
Visitor Host Details			
Name Search			
Advanced Search			
First Name	X	H	X
Last Name	X	H	X
Unique Number		H	X
Telephone Number	X	H	X
Cell / Mobile Number	X	H	X
E-Mail Address	X	L	

Required Functionality	Current Functionality	Importance	Mandatory
Office / Site / Location		H	
Host Advanced Search Options			
Visitor Last Name	X	H	
Visitor Name	X	L	
Unique Number		H	
Mobile Number		M	
Visitor Type Selection			
Employee / Contractor registering External Visitor		H	
Employee / Contractor visiting other site		H	
System Functionality			
Allow 1:1 host card tagging	X	H	
One card per visitor	X	H	
Notification of registration sent via e-mail	X	M	

22.9.5.2 Registration (Check in/out) Fields

Table 6: Registration (Check in/out) Fields

Required Functionality	Current Functionality	Importance	Mandatory
Form Attributes		L/M/H	
Main Menu			
Search	X	H	
Pre-registered Visitors	X	H	
Previous Visitors	X	H	
Current Visitors	X	H	
Current Cards	X	M	
Visitor Personal Info			
Visitor Last Name	X	H	X
Visitor First Name	X	H	X
Visitor Company	X	M	
Date of Birth	X	M	X
ID / Passport Number	X	H	X
Telephone Number	X	M	X

Required Functionality	Current Functionality	Importance	Mandatory
Cell / Mobile Number	X	H	X
E-Mail Address	X	M	
Date of Visit		H	X
Time of Visit		H	X
Vehicle Registration	X	H	X
Duration of visit		L	
Meeting Room		M	
Reason for Visit		M	X
Comments / Notes		M	
Capture / Import Photograph	X	H	
Visitor Host Details			
Name Search			
Advanced Search			
First Name	X	H	X
Last Name	X	H	X
Unique Number		H	X
Telephone Number	X	H	X
Cell / Mobile Number	X	H	X
E-Mail Address	X	L	
Type of Employee	X	H	
Office / Site / Location		H	
Host Advanced Search			
Visitor Last Name	X	H	
Visitor Name	X	L	
Unique Number		H	
Mobile Number		M	
Card Details			
Card Number	X	H	
Commence Date and Time	X	H	
Expiry Date and Time	X	H	
Host Card Number		H	
Visit Menu			
Start Visit	X	H	
Place Visit On Hold (Suspend)	X	H	
End Visit	X	H	
Delete Visit	X	H	

22.9.6 Additional Reports

The Business requires a report/s to provide information regarding Volumes. E.g. Number of people that have been through the Visitor gate in a specific time period. Business would be able to understand the number of employees, contractors and visitors by using filters on this report. The value is that business would be able to understand the high traffic areas and which hardware / equipment is working more often and may need servicing or inspection more often.

The business requirement is for an Access Denied Report to be created. This must show the number of "Access Denied" attempts in a specific time period. It should also list each individual that has been denied access in the report. This will enable the business to conduct more training if necessary as the information would be indicative of how many people are possibly having problems at biometric fingerprint readers.

An Alarms Report must be created so that management as well as operations have a clear view of the number of alarms that have been reported on the system. The Alarms report must also show the number of alarms that have been acknowledged and those that are not acknowledged. The report should break down alarms into the various levels of alarms that have been already defined e.g. High and Low priority.

22.10 Canteen Management System

22.10.1 The Canteen System shall contain the following functionality:

1)	The integration using Web Services is to be used as the standard solution for all Eskom sites that require identification management services. E.g. Canteen Management.
2)	The user interfaces for the Canteen System must not be changed / affected following the implementation of the integration solution. I.e. When a cardholder badges at the Workstation's card reader, the cardholder's profile should open on the interface screen if he/she is a valid Canteen User.
3)	The process for loading credits / vouchers for a user is required to remain as-is following integration. I.e. When a card is badged at the Workstation's card reader or the self-service kiosk, the cardholder's remaining credits should appear on the screen if he/she is a valid Canteen User.
4)	The Canteen System is required to make use of the Standard Security Access Cards (HID and Mifare type Smart Cards – up to 35 bit).
5)	The Canteen system is required to make use of Contactless Card Readers that are both, able to read the Access Cards and are compatible with the Canteen system. The Canteen Management office has no requirement for Biometric verification due to hygienic concerns.
6)	The Card readers are required to be installed / replace all Magstrip type card readers at the following Canteen related areas: • Petty Cash Office/s • Canteen Workstation/s • Self-service kiosk/s • Coffee Shop/s
7)	The Canteen system requires the card number output from the reader to its system (input) in order to open the respective cardholder's profile. The Canteen system verifies the card number against a record in its database to open a profile. Currently the system uses Unique numbers and hence will require a batch update from EBI to load the card numbers together with Unique numbers into a card number field of the Canteen Management System.

8)	A batch update will be completed from EBI to the Canteen system using Web Services. This batch update will contain records for all active users and shall occur on a daily basis. Fields required from the Integrated Access Control System to the Canteen system are: • Card number • Employee Number (Unique number) • Name • Surname • Employee/Contractor end date • Department • Cost Centre
9)	A user is required to become inactive on the Canteen system when they have become inactive on the Integrated Access Control System e.g. resigned, suspended, retired, contract expired, etc.
10)	Credits / Vouchers purchased shall be stored on the Canteen system - against a user's profile as currently done. Credits / Vouchers purchased shall not be loaded/replicated onto the Access Card of the user.

22.11 Securing carry-on assets

22.11.1 Screen carry-on asset

a) The Screening of an individual's Carry-on assets shall include the following:

1) Screen for authorised carry-on assets
2) Screen for prohibited items
3) Screen for allowable items
4) Screen for alcohol substances
5) Screen for site specific carry-on asset requirements where applicable

22.11.2 Tag Vehicle

a) A vehicle is considered as an asset to the individual. This process deals with tagging a visitor's vehicle to the respective visitor:

1) Scan vehicle license disc
2) Scan barcoded ID / driver's license
3) Scan fingerprint

22.11.3 Issue asset permit or tag

A carry-on asset permit is issued by the Operator. The Registration operator shall complete this task for employees/contractors and Reception operators will do the same for visitors. This may be a temporary or permanent permit. The following steps shall be completed for issue asset permit:

a) Determine whether the individual has valid carry-on assets

1) Populate individual personal details from ID / access card

b) Validate Carry-on Asset

1) Capture / Verify the Asset Serial Number
2) Capture the asset permit or tag expiry date
3) Print carry-on asset permit

c) Issue Carry-on asset permit to individual

22.11.4 Verify asset permit or tag

Security official is required to check the asset permit or tag on exit and at any asset checkpoints within Eskom. The asset permit must match to the individual with whom it has been issued. The expiry date on the asset permit must not have expired for it to be valid. Activity is listed below:

a) Collect carry-on asset

b) Collect carry-on asset permit

c) Verify serial number on carry-on asset with number on permit

d) Verify asset permit holders name matches individual's access card or ID

e) Verify that the permit or tag expiry date has not been reached

22.12 Entry and Exit control

22.12.1 Individuals that enter and exit Eskom sites shall be classified into the following:

a) Employees and Contractors (walk-in or in vehicle)

b) Tenants (walk-in or in vehicle)

c) Visitors (walk-in or in vehicle)

22.12.2 Entry for Employees and Contractors

a) Employees and contractors shall be enrolled with biometric fingerprints. PIN codes are used where necessary e.g. People with disabilities. They have also been allocated a unique access card. On entry to a site the employee / contractor will be screened for unauthorised items and then badge their access card at the entry points to gain access.

b) At specific access points e.g. main work area entry and exit point (turnstiles), both card and fingerprint verification is required so that an employee / contractor cannot lend his / her card to someone to gain entry/exit.

c) At sensitive areas such as a power station, a visiting employee /contractor is required to follow the safety and security induction together with medical checks before gaining entry to the site.

22.12.3 Exit for Employees and Contractors

On exit from a site the employee / contractor shall utilise their standard access card at the exit points followed by a screening and carry-on asset verification.

22.12.4 Entry and Exit for Tenants

Tenants must be captured on the Integrated Access Control System as Employees, Contractors and Visitors are captured. Tenants must be classified into a separate category on the system e.g. "External Personnel, Tenant". Tenants are required to be issued with Access Cards so that they may gain entry and exit at the relevant site entry and exit points. Tenant's activities / badging at these points are required to be reported on the system. Tenants will follow the standard entry procedure where they are screened. On exit a tenant will also have to provide verification of their carry-on asset/s.

22.12.5 Entry and Exit for Visitors

This is captured in Gate Management and Reception Management

22.12.6 Perform site-specific induction

It is a business requirement that verification of whether safety and security induction for a specific site or area has been completed and is valid.

a) Cardinal rules

b) Restricted areas

c) Prohibited items

d) Speed limits

e) Declarations

f) Site-specific rules

22.12.7 Validate order

Validate an order (including work orders, permit to work and purchase orders) against a site-specific authorised list as justification for site access.

a) Scan barcode

b) Check zone access

c) Check access duration

d) Escort individual if vetting fail

22.13 Managing alarms

a) This is the process of identifying, acknowledging, responding and closing of an alarm generated by the Integrated Access Control System.

b) The business requirement is that the Integrated Access Control System contains a Graphical User interface that displays site maps, cameras on the sites, alarms and other security related data such as the state of the security device. The monitoring interface must provide a real-time view of the site. Each site's information (at least alarms and reporting) must feed into the Eskom National Security Control Centre.

22.13.1 Graphical User Interface Requirements

22.13.1.1 Functional Requirements

a) The GUI must implement a Role-based access and privilege model so that classes of users can be given access to functions appropriate to their assigned organisational responsibilities.

b) The GUI should primarily contain floor plan views per site. Alarms page / window should form part of screen to allow the user both graphical and data alarms to select from.

c) The GUI must cater for utilising photos as the background where icons can be mapped onto it. E.g. a picture of a zone with icons of readers and controllers mapped over the picture.

d) The GUI must cater for importing drawing files of various types such as CAD files.

e) The GUI must cater for multiple floor levels – as required for buildings with more than a single floor.

f) The GUI should have the capability to display more than 1 screen (floor plan) at a time (split screens).

g) The GUI must cater for 3 dimensional models and views with related controls to navigate through the model. This requirement should be based on the site type and criticality.

h) The GUI must include a zoom function which allows for both zoom in and zoom out on floor plan views and 3 dimensional views.

i) The GUI must allow for colours to be configurable for the layouts. E.g. Floor plan line colours can be green against a black background.

j) The EBI system must cater for integration of various modules into this GUI. Readers, controllers, access points, cameras, intrusion detection system and other security and BMS related hardware devices must be mapped/displayed on the GUI. The user should be able to select from a drop down list of various components to get a dynamic view of the same. E.g. if “Readers” were selected then the floor plan should only display the readers on that floor

k) All icons mapped on the GUI must be linked with the actual hardware devices installed in the field/building/site. The linking of this must include details such as the state of the device, the alarm state if any and last person that has accessed that point if it is a reader. There must be capability of using a pop-up screen to view this status.

l) The level of detail should be at a door level, i.e. the operator does not have to have a view of the server, and wiegand converter connected to the door. The alarm should bring up details of what the hardware /tamper alert is.

m) The GUI should contain different icon types/styles for different equipment e.g. camera, reader, controller.

n) The GUI must have colour coding for hardware items depicted, i.e. use colour coding to indicate the status of hardware items. Hardware must have the colour categories as depicted in Appendix A

o) Alarms must be 3 colours:

1) Red for high priority

2) Yellow for medium priority

3) Blue for low priority

p) The GUI must display all access points that are open e.g. doors, turnstiles especially in the case of an evacuation. A separate colour code should be used for this. Text should be displayed as well indicating emergency.

q) A flashing GUI icon should be used when a hardware failure occurs or an alarm is triggered at any specific point. The flashing should not stop until the alarm / failure has been acknowledged / opened.

r) A hardware failure or alarm should have an audible alarm sound together with the flashing icon. The alarm sound should increase automatically after every 2 minutes that the alarm has not been acknowledged / opened. This must be configurable to use for only certain alarm types / levels e.g. High Priority alarms

s) The GUI should have a configurable threshold of the number of unacknowledged alarms and an automatic escalation via the e-mail / SMS gateway.

t) The GUI should have manual and automated methods of SMS and emailing alarms, especially for high priority alarms.

u) The GUI must allow for clicking on the icons (cameras, readers, controllers, power supply etc.) that have been mapped on the interface. The system must then respond by opening details of the linked camera/reader/controller/power supply etc. The icon focus must return back to its original point on the map after closing this details screen.

v) The GUI should have an emergency contact list that the operators can quickly access in order to attend to an alarm.

w) On acknowledging/opening an alarm the GUI should display procedures to attending to the alarm. For each alarm type these may differ as there are different threat levels in the business and therefore should be configurable per alarm type.

x) The GUI should have the ability to capture sticky notes / comments to alarms and escalations.

y) The GUI should have both touch screen and keyboard/mouse/joystick device input/control.

z) Must show different zones and the number of people in each zone should be listed in the zone.

22.13.1.2 Additional alarm requirements

a) Alarms should be displayed in real-time with the icons.

b) Linked readers/controllers/power supplies etc. must open within 2 seconds requesting it to open.

c) Cameras should open in 2 seconds on a local site at 15 frames per second speed. The greater the speed, the longer the video screen will take to open. Also, if multiple cameras are opened at the same time, the system would take a larger amount of time to open these.

d) The GUI should allow for limitations on the network.

e) The GUI should be available 24 hours per day, 365 days per year.

f) It must cope with high volume of alarms and events between 8am-5pm, Mondays – Fridays.

g) 500 unacknowledged alarms must result in an escalation to the Security Manager.

h) The GUI must cater for high availability and redundancy as with the EBI system availability requirements.

i) The GUI must have a 98% availability, reliability, accessibility and dependability.

23. System development methodology

In order to meet the requirements of an effective EBI based Integrated Access Control System, the contractor shall design, manufacture, supply, deliver, develop user documentation, perform testing at works and training of Eskom personnel for application at Eskom sites of an EBI based Integrated Access Control System and associated equipment (hardware/software etc.) according the following project phases.

23.1 Phase 1-Functional Design specification

This phase shall consist of the production of a Functional Design Specification comprising of a functional specification document and a system design report.

The intention of this phase is to finalise all requirements and subsequently document the proposed design to form the baseline for the following phases.

23.1.1 Deliverables for phase-1

a) Functional Specification

b) Systems Design Report

c) Updated Project schedule

23.2 Phase 2-Detailed Design Specification

This phase shall consist of the production of a Detailed Design Specification for both hardware and software components of the system and specifies the procedures for testing.

23.2.1 Deliverables for phase-2

a) Detailed Design Specification

b) FAT Procedure document

c) SAT Procedure document

23.3 Phase 3- Development, System Integration and Factory Acceptance Test (FAT)

This phase shall consist of the procurement of hardware required for testing, any required development and supply of software, training of the Purchaser's personnel, database population and system integration which is to be followed by formal testing of the system at the Supplier's premises, in the presence of the Purchaser's personnel.

23.3.1 Deliverables for phase-3

A signed-off FAT report indicating accepted completion of FAT.

23.4 Phase 4- Delivery, Installation, Testing and Commissioning

This phase shall comprise of delivery of hardware, software, documentation and manuals to site, installation in conjunction with the Purchaser's personnel and training. Thereafter, the system shall be commissioned in accordance with operating constraints of the installation site.

23.4.1 Deliverables for phase-4

a) Equipment delivery and installation

b) System documentation in triplicate hardcopy and electronic format

c) Implementation Report to be approved by the Purchaser

d) Commissioned system

23.5 Phase 5- Site Acceptance Test (SAT) at Transmission substations

This phase consists of conducting tests according to the SAT Procedure document.

23.5.1 Deliverables for phase-5

a) A signed-off SAT report indicating accepted completion of SAT.

b) A hand-over Certificate.

c) Source code for all software delivered.

24. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Danie Odendaal	Engineering SGM (Acting)
Prince Moyo	Power Delivery Engineering GM
Richard McCurrach	Senior Manager – PTM&C CoE
Amelia Mtshali	Metering, DC & Security Technologies Manager – PTM&C CoE (Acting)
Prudence Madiba	Senior Manager Electrical and C&I Engineering
Lungile Malaza	Middle Manager – Electrical Plant COE
Thomas Jacobs	DC & Auxiliary Supplies SC Chairperson
Marius van Rensburg	Senior Manager – Transmission
Paul Grobler	Chief Engineer – Transmission

Name and surname	Designation
Sikelela Mkhabela	Senior Manager – Distribution

25. Revisions

Date	Rev	Compiler	Remarks
Jan 2016	Draft 0.1	R Moshoeshoe	First issue

26. Development team

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

- Donald Moshoeshoe
- Thomas Jacobs
- Sandi Ndamase

27. Acknowledgements

Group security

Annex A – Equipment sizing

Table A.1: EBI Server Platform Specification

Item	Eskom Recommended Standard Specification
Processor	Intel Core i7 860 2.80GHz
Memory	16 GB RAM
Hard Disk	RAID5 (If we are using local storage. SAN storage can be utilized for the data drives providing that the implementation is transparent to the OS and application layer) C-Drive - 250GB – for software (Card Layouts and User Photos) D-Drive - 500GB – for SQL Database files The estimate is based on the following assumptions: - 10 000 Cardholders - 4 Transactions per cardholder per day - 40 000 Transactions per Day - 2GB per month - 120GB for 5 year retention time. Additional 80GB storage for Event Management Data E-Drive - 100GB - for SQL Log Files F-Drive - 500GB - for Backups and Installation Media
DVDROM Drive	Dual layered DVD-ROM. (This is not an absolute requirement as long access to the installation media, i.e. ISO images or USB drive can be provided).
Keyboard	Standard keyboard with 12 function keys
Pointing Device	Standard Mouse
Video Resolution	Default 1280x1024 pixels; min 65K colors
Operating System	Windows Server 2008 R2 Standard 64 bit (Microsoft SQL 2008 Server and SQL 2008 Server Express are automatically installed by EBI.)
Network Card	Dual 1Gb/s NIC
Browser	Internet Explorer 8
Additional Software	Windows IIS Components (IIS 7 for W2K8 R2) Microsoft Net Framework 1.1 Microsoft Net Framework 3.5 Microsoft Office 2007 Up to date anti-virus Server recovery software Disk imaging software (for ISO images)

Table A.2: Eskom standard Sever Sizing Specification (Per Server)

Item	Sizing Specification (Per Server)
Cards	Greater than 100,000 subject to hardware limitations
Points	65,000 per server 180,000* per system * More than 180,000 with Technical Risk Review and Approval
Access Levels	1024
Zones	1024
Time Periods	256
Alarms	2000* unique concurrent alarms. * Each alarm is an aggregating on unlimited recurrences of the same alarm message
Operator Stations	Licensed individually up to 80 concurrent connections
Printers	50
Reports	1000 scheduled standard reports Custom Reports may be configured within SQL reporting Services and this number is not limited
Events	100,000 per 60 MB of disk space available
Assignable Hardware Locations	1000
Users (Operators)	1000
Number of DSA connected Servers	10* * More than 10 with Technical Risk Review and approval

Table A.3: EBI standard Registration Station Specification

Item	Eskom Standard Specification
Processor	Intel Core i5 U540 1.20GHz
Memory	4 GB RAM
Hard Disk	500GB (NTFS)
DVDROM Drive	DVD-ROM (Dual layered)
Keyboard	Standard keyboard with 12 function keys
Pointing Device	Standard Mouse
Video Resolution	Default 1280x1024 pixels; min 65K colors
Operating system	Windows 7 Professional 32 bit Service Pack 1
Network Card	Dual 1Gb/s NIC
Browser	Internet Explorer 8
Digital Camera	Canon Powershot A495 or any windows compatible camera that supports TWAIN. Typically Microsoft Lifecam FHD
Tripod stand	Standard off the shelf tripod for digital cameras
Biometric Capture Device	MorphoSmart Optic (MSO300)

Item	Eskom Standard Specification
Access Card Encoder	SCM Microsystems SDIO10/SDIO11 Smart Card Reader
USB Card Reader	Any reader type that is able to capture the card number into a field
USB Hub	Due to the number of USB devices per workstation a hub is required to cater for at least a total of 10 USB slots
Card Printer	Data card Colour SP35 Plus printer
Additional Software	As per Eskom standard workstation image
Comments	Active X enabled on Eskom image

Table A.4: EBI Reception Station Specification

Item	Eskom Standard Specification
Processor	Intel Core i5 U540 1.20GHz
Memory	4 GB RAM
Hard Disk	500GB (NTFS)
DVDROM Drive	DVD-ROM (Dual layered)
Keyboard	Standard keyboard with 12 function keys
Pointing Device	Standard Mouse
Video Resolution	Default 1280x1024 pixels; min 65K colors
Operating system	Windows 7 Professional 32 bit Service Pack 1
Network Card	Dual 1Gb/s NIC
Browser	Internet Explorer 8
Web Camera	Logitech Webcam Pro 9000 or similar.
Additional Software	As per Eskom standard workstation image
Comments	Active X enabled on Eskom image