Annex C – Technical Schedules A/B for the IACS

TECHNICAL SCHEDULES A & B FOR

SPECIFICATION FOR INTEGRATED ACCESS CONTROL SYSTEM (IACS) FOR ESKOM SITES STANDARD IN ACCORDANCE WITH ESKOM STANDARD 240-102220945

Schedule A: Purcha'er's specifications

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

The clauses and numbering in this table are not necessarily the verbatim clauses as per 240-102220945. Therefore it is OBLIGATORY on the TENDERER to review the applicable clauses in 240-102220945 in order to provide an informed response.

When completing the Schedule B and the References section, The Tenderer is required to state clearly, for each clause that requires a statement of compliance, with one of the following options:

Comply – Confirmation of FULL Compliance to all clauses of the applicable section of the Technical Standard. No deviations.

Partially Comply – Confirmation of PARTIAL Compliance and that FULL Compliance is not possible. Deviations taken.

Do Not Comply - Conformation of Non-Compliance to ALL requirements in the applicable section

Reference to evidence in the form of datasheets, equipment manuals, drawings, hyperlinks shall be included in the References section if required.

Where there are any deviations taken from the clauses in the applicable section, these should be indicated under the References and Deviations section.

	Description	Schedule A	Schedule B (Suppl'er's statements of compliance)	References/ Statement (supporting evidence) if required & Deviations
5	Operational requirements			
5.1	General operational requirements			
5.1 (1)	The system shall be able to transfer data to SAP for Time and attendance data.			
5.1 (2)	Each user authorization shall be uniquely definable.	Comply with reference.		
5.1 (3)	Operator terminals shall be protected by terminal security such as password policy.	Comply with reference.		
5.1(4)	All actions on the system shall be traceable and auditable. These actions must be kept for a minimum period of 90 days.	Comply with reference.		

5.1 (5)	The system shall allow for an allocated employee number (unique number) to be changed when a contractor or visitor becomes a permanent employee with Eskom without having to re-register.	Comply		
5.1 (6)	Automatic disabling of a visitor/contractor on the required date.	Comply		
5.1 (7)	A visitor shall be disabled after leaving the site or designated place of visit/work	Comply		
5.1 (8)	The system shall have a full anti-pass back facility to control the flow of personnel from one zone to the other.	Comply with reference where applicable.		
5.1(9)	High risk areas access shall be granted only to personnel working in that area, additional access shall be automatically disabled as soon as that person leaves the area.	Comply		
5.1(10)	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.	Comply		
5.1 (11)	The system shall be able to interface with existing software packages and therefore an open protocol software platform will be required.	Comply		
5.1 (12)	It shall be possible for the operator to bypass anti-pass back rules selectively such as one host having multiple visitors.	Comply		
5.1(13)	The system shall have lockdown functionality in emergency situations.	Comply		
5.1 (14)	System shall allow for online changes to be made.	Comply		
5.1 (15)	Real-time online debugging shall be possible.	Comply		
5.1 (16)	The system shall be either fail safe or fail secure, as required.	Comply		

5.1(17)	The application for change or update of access shall be completed on a standardised eForm.	Comply		
5.1 (18)	There shall be a dedicated “Master” station to assist in roll call in the event of an evacuation.	Comply		
5.1(19)	The system shall have a built in Fitness For Duty (FFD) program or interface to the FFD program.			
6	Access Control Models			
6.1(i)	The system shall be able to enforce access through the different types of controls such as:			
	1) Attribute-based Access Control (ABAC)	Comply		
	2) Discretionary Access Control (DAC)	Comply		
	3) History-Based Access Control (HBAC)	Comply		
	4) Identity-Based Access Control (IBAC)	Comply		
	5) Mandatory Access Control (MAC)	Comply		
	6) Organization-Based Access control (OrBAC)	Comply		
	7) Role-Based Access Control (RBAC)	Comply		
7	System architecture			
7.1	The system should have a distributed architecture with tiered model comprising Primary Servers, Regional Servers and Site Servers.			
7(1)	There shall be a primary server hosted at the main Security control centre which shall act as a single source for all Eskom’s card Holder data.	Comply		
7(2)	The primary server shall have redundancy with real time synchronisation with the secondary/ back-up server.	Comply		
7(3)	At regional level there shall be regional servers connected to the Primary server via the Eskom Telecoms IP network.			

7(4)	The regional servers shall have real time synchronisation of card holder information with the Primary server. These servers shall have a daily full server backup.			
7(5)	At site level (where applicable), there shall be site server(s) installed with various security end point devices. The sites server(s) shall be capable of operating in isolation if it loses connectivity to the regional sever to ensure business continuity.	Comply		
7(6)	Firewalls and servers shall be managed by Eskom to ensure confidentiality and integrity of information. Where a third-party is appointed for management of firewalls and servers, there shall be a non-disclosure agreement signed between Eskom and the third-party and Eskom shall be approached for approval of any planned upgrades or changes before they are implemented.	Comply		
8	Communication and network requirements			
8.1	General communication requirements			
8.1 (1)	Suppliers shall ensure that the system is capable of using Eskom's existing communication infrastructure.	Comply		
8.1 (2)	The network infrastructure shall adhere to the principles laid out in the following documents which will be made available to the contracted supplier:			
	a) **240-554109–7** - Cyber Security Standard for Operational Technology	Comply		
	b) **240-556835–2** - Definition of Operational Technology (OT) and OT / IT Collaboration Accountabilities	Comply		
	c) **32-1203** – Eskom Telecommunications User Requirements Specification	Comply		
	d) **240-941363–6** - IP Voice and Data Network Design Guideline.	Comply		

	e) **240-46264031** – Fibre Optic Design Standard – Part 2: Substations.	Comply		
	f) **IEC 62645** Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programme for Computer-based Systems.			
8.1(4)	The system shall allow IP to IP connection between the servers.	Comply		
8.1 (5)	The system shall allow multi-casting for distributing status information between servers.	Comply		
8.1 (6)	The servers shall be time synchronised.	Comply		
8.1 (7)	There shall be LAN points for servers with connectivity to IAC VLAN.	Comply		
8.1 (9)	Severs shall be configured with static IP addresses.	Comply		
8.1 (10)	All reader controllers shall have interface capabilities stipulated under section 4.1.3 of SANS 2220-2-4.	Comply		
8.1(11)	The System shall at minimum cater for Ethernet 10/100/1000 with auto negotiation, the supplier shall also indicate if their equipment supports the following I/O ports:			
	a) RS-232	Comply		
	b) RS-485	Comply		
	c) Wiegand in/out	Comply		
	d) TTL in/out	Comply		
	e) Modem (to provide alternative Comms where there is no network infrastructure installed).			
8.2	Supported communication standards			
8.2(1)	The system shall support open communication standards/protocols	comply		
8.3	Bandwidth requirements			

8.3 (a)	Bandwidth allocation for the system shall Comply with the requirements of Eskom Telecommunications User Requirement Specification (Unique identifier: 32-1203).	Comply		
9	Cyber security			
9(1)	The system shall Comply with Eskom' Cyber Security standard for Operational Technology (Unique identifier: 240-55410927).	comply		
9(2)	The system shall Comply with the requirements of Demilitarised Zone (DMZ) designs for Operational Technology (Unique identifier: 240-79669677).	comply		
9(3)	For nuclear sites the system shall Comply with site specific cyber security procedures and programs.			
10	Hardware requirements			
10.1	Server requirements			
10.1 (1)	The server shall Comply with the requirements of SANS 2220-2-2.	Comply with reference.		
10.1 (2)	There shall be a primary server where all the system configurations and event data is stored.	Comply		
10.1(3)	There shall be a redundant sever which is a mirror of the primary server	Comply		
10.1(6)	There shall be synchronization between field devices and server network such that transaction records are automatically uploaded from each reader to the relevant database.	Comply		
10.1(7)	The server shall automatically back up data, this data shall be stored for a minimum period of 36 months.	Comply		
10.1 (8)	There shall be LAN points for servers with connectivity to the IAC VLAN.	Comply		

10.1(9)	There shall be servers that handle administration at each site that can be diverted to a central server that is situated at the security control centre	Comply		
10.1(10)	The server shall be able to handle the automatic deletion of visitor and contractor account/profile after the expiry date.	Comply		
10.1(11)	The server shall be able to handle the deletion and removal of redundant account/profile based on information received from an administrator workstation.	Comply		
10.1(12)	Cabinets with minimum IP 65 rating shall be used for servers. These shall be housed inside the nearest restricted building such as guard house or access control building.	Comply		
10.1(13)	The server shall have 99.99 % availability.	Comply		
10.1 (14)	The server shall be of a modular design.	Comply		
10.1(15)	The server shall contain a real-time clock circuit synched with a GPS time clock, capable of maintaining and displaying real time (month, day, hour, minute and second).	Comply		
10.1(16)	Interface between the server and the peripheral devices (such as readers and reader controllers) shall be by means of a standard communications protocol.	Comply		
10.1(17)	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.	Comply		
10.1 (18)	The server software shall maintain a real-time sequential record (on the hard disk) of reader events, alarm events and all operator programming events	Comply		

10.1 (19)	Server sizing shall be guided by factors such as number of estimated card holders, information retention period and storage for backups	Comply		
10.2	Registration stations			
10.2(1)	The Security Manager shall be the owner and main operator of the system responsible to provide any changes and permissions to the system.	Comply		
10.2 (2)	The registration facility shall enable the Security Manager to be able to register, disable, enable and change personnel details of employees, Visitors and other personnel onto the access control system for them to be able to gain access into the approved areas as approved by the security management team.	Comply with reference.		
10.2 (3)	A full audit-trail shall be provided for all registration transactions.	Comply		
10.2(4)	Registration shall be fingerprint protected – i.e. the access control administrator shall be required to fingerprint in order to login to the registration application.	Comply		
10.2(5)	The registration stations shall be integrated to the database where the access control data is kept.	Comply		
10.2 (6)	Permanent employees shall only be registered once authorization has been given.	comply		
10.2 (7)	Visitors shall only be authorised for registration when a valid identity document is produced and confirmation from the Eskom employee been visited has been received.	comply		
10.2 (8)	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. There shall be automatic lockout after completion of the work related to the contract.	Comply		

10.2(9)	Permanent employee's access rights shall only be disabled on request from the Security and/or HR department.	comply		
10.2(10)	Visitors' access rights shall be disabled by the access control auto-disabling function at the end of the scheduled visiting time/period and/or at the return of the visitor access card in the drop box.	Comply		
10.2 (11)	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. This reminder shall be sent to HR department, affected contractors and project managers.	Comply		
10.2 (12)	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.			
10.3	Client stations			
10.3(1)	The IACS shall use a client/server architecture	Comply		
10.3 (2)	The client stations shall be used by the operator to view alarm/events and manage the system. This client station shall have a standard Eskom desktop image loaded.	Comply		
10.3 (3)	The reception stations shall be used by the operator to manage visitors. This reception station shall have a standard Eskom desktop image loaded.	Comply		
10.3(4)	The software installed on the client stations shall cater for the following requirements:			
	a) Screen modification programs.	Comply		
	b) Menu modification programs	Comply		
	c) Keyboard modification programs	Comply		

	d) Colour modification programs	Comply		
	e) Icon menu modification programs	Comply		
	f) System monitor programs	Comply		
	g) Logbook reset program	Comply		
	h) Graphical font modification program	Comply		
	i) System message modification program	Comply		
10.4	Readers and reader controllers (for both outdoor and indoor use)			
10.4.1	General			
10.4.1 (1)	It shall be possible to assign to any reader an IN or OUT function in any geographic area or any combination of areas.	Comply		
10.4.1 (2)	It shall be possible for the operator to declare any reader as either card only, card plus biometrics, card plus PIN, or to switch from one state to the other.	Comply with reference.		
10.4.1 (3)	It shall be possible to attach an identifier to each reader to assist in identifying reader locations for record purposes.	Comply with reference.		
10.4.1 (4)	It shall be possible to assign to any 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.			
10.4.1 (5)	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. There shall be an audit trail of the user who completed the change and authorization.	Comply		
10.4.2	Card readers			
10.4.2 (1)	Card readers shall Comply with requirements of SANS 2220-2-3.	Comply with reference.		

10.4.2 (2)	A card reader shall accept cards presented to it through proximity, or long distance reading or remote controls linked to access cards such that systems can be armed/disarmed and access be granted without exiting the vehicles at sites located in risky areas.	Comply		
10.4.2 (3)	The reader shall use visual confirmation e.g. light-emitting diodes to show whether access was granted or denied. The response shall be within 100 milliseconds of presentation of the access card.	Comply		
10.4.2 (4)	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.	Comply		
10.4.2 (5)	The readers shall be capable of reading access cards and send data to an associated interface.	Comply		
10.4.2 (6)	A card reader shall be capable of indicating failures as well as an alarm condition.	Comply		
10.4.3	Biometric readers			
10.4.3 (1)	Biometric readers shall Comply with requirements of SANS 2220-2-5.			
10.4.3 (2)	A biometric device shall contain a sensor that recognizes a per'on's physical characteristics, such as the following:			
	a) fingerprints;			
	b) hand geometry (finger position and length);			
	c) retina patterns;			
	d) voice patterns; or			
	e) signature			
10.4.3 (3)	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.			

10.4.3 (4)	There shall be biometric readers capable of requesting biometric validation after presentation of the access card, after which it shall send data to an associated interface.			
10.4.3 (5)	The MTBF (mean time between failures) of biometric readers shall Comply with section 4.1.5 of SANS 2220-2-5.			
10.4.3 (6)	If a biometric reader is connected to a central processor, it shall be by means of standard communications protocol.			
10.4.3 (7)	The biometric device shall Comply with all relevant health and safety requirements and regulations.			
10.4.3 (8)	Markings for biometric readers shall Comply with section 5 of SANS 2220-2-5.			
10.4.4	Reader controllers			
10.4.4 (1)	Reader controllers shall Comply with requirements of SANS 2220-2-4.	Comply with reference.		
10.4.4 (2)	A reader controller shall be used where a reader cannot be connected directly to a central processor.	Comply		
10.4.4 (3)	Construction of reader controllers shall Comply with section 4.1.1 of SANS 2220-2-4.	Comply with reference.		
10.4.4 (4)	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.	Comply with reference.		
10.4.4 (5)	A site server shall be used to control all reader controllers for a site.	Comply		
10.4.4 (6)	The reader/door controller must keep a local copy of the access control lists and logs, so that stand-alone operation is possible for a defined time in the event of a communications failure.	Comply		
10.6	Access cards			

10.6 (1)	Access cards shall Comply with the requirements of SANS 2220-2-6.	Comply with reference.		
10.6 (2)	Access shall be available in the formats below:			
	a) swipe cards	Comply		
	b) contact cards	Comply		
	c) passive proximity cards	Comply		
	d) active proximity cards	Comply		
10.6 (3)	Access cards shall be Eskom's approved corporate identity template and be made of a durable material that can display the following information, as required:			
	a) an ID photograph;	Comply		
	b) Employee number (unique number);	Comply		
	c) a company logo;	Comply		
	d) name and other information of bearer (e.g. vehicle permit information).	Comply		
10.6 (4)	Card printers shall be used to print the employee details and card layout directly to the cards before issuing.	Comply		
10.6 (5)	The standard card format shall at minimum have 128 Bit Encryption.	Comply with reference.		
10.6 (6)	The cards shall have support for random ID, each card shall have a unique serial number printed on the card.	Comply		
10.6 (7)	Dimensions of access cards shall Comply with section 4.1.2 of SANS 2220-2-6.	Comply with reference.		
10.6 (8)	An ACS card encoder shall be used to encode cards by loading the required information regarding the card owner before issuing of the card. Any attempt to change the code shall destroy the card.	Comply		
10.6 (9)	A photograph of the card holder shall be captured using a digital HD camera before issuing the card.	Comply		

10.6 (10)	The card shall be water resistant and resistant to wear and tear caused by extended use.	Comply		
10.6 (11)	The location of the contacts and the microchip shall not cause surface irregularities on the back of the card or in the magnetic strip area.	Comply		
10.6 (12)	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.	Comply		
10.6 (13)	When so required, the central processor shall be able to provide a print-out of all activities of a card.	Comply		
10.7	Barriers			
10.7 (1)	A barrier shall be one of the following devices intended to prevent unauthorized access to a controlled area:			
	a) an access booth;			
	b) a door (with door closer or monitor or both);			
	c) a vehicle boom;			
	d) a vehicle gate;			
	e) a vehicle stopper;			
	f) a turnstile.			
10.7 (2)	A barrier shall at minimum, consist of the following components:			
	a) a physical barrier;	Comply		
	b) a detection unit, this can be used to detect an object in the path of the barrier which could obstruct the barrier movement;	Comply		
	c) an interface to a control unit operated manually or by some access control facility;	Comply		
	d) a barrier status device, and	Comply		
	e) a tamper protection device.	Comply		

10.7 (3)	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	Comply with reference.		
10.7 (4)	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 relock the door if the booth was not used within 30 s after a door has been unlocked.	Comply		
10.7 (5)	A panic/emergency alarm facility shall be provided on the inside of the booth, to allow any person trapped inside the booth to initiate an alarm.	Comply		
10.7 (6)	If a booth malfunctions, it shall be possible to unlock the door from the outside with an emergency key override.	Comply		
10.7 (7)	A barrier shall have the necessary potential free contacts to indicate status (open/closed).	Comply		
10.7 (8)	A cubicle shall be so constructed that it is possible to anchor the booth to a solid base by means such as expanding bolts.	Comply		
10.7 (9)	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.	Comply		
10.7 (10)	The operating mechanism of the access booth shall have a locked cover equipped with a tamper protection switch.	Comply		
10.7 (11)	Turnstiles and booms			

10.7 (11)(a)	Turnstiles shall Comply with section 4.7 of SANS 2220-2-7.	Comply with reference.		
10.7 (11)(b)	A vehicle boom shall consist of the following components:	Comply		
	i. an enclosure for the operating mechanism;	Comply		
	ii. a boom;	Comply		
	iii. detector loops;	Comply		
	iv. a warning device;	Comply		
	v. a mechanical crank;	Comply		
	vi. an operating mechanism;	Comply		
	vii. a boom rest (for a boom longer than 4 m).	Comply		
10.7 (11) C)	The boom shall be activated by electronic means such as a reader controller.	Comply		
10.7 (11)(d)	The enclosure of an operating mechanism for a boom shall at minimum Comply with the requirements of class IP45 of SANS 60529.	Comply with reference.		
10.7 (11) e)	There shall be provision for single and double height turnstiles.	Comply		
10.7 (11)(f)	A drop box shall be used for visitors to capture the card on exit.	Comply		
10.7 (11)(g)	Vehicle barriers with ground loop sensors shall be installed.	Comply		
10.7(11) (h)	At vehicle entrances dual height gooseneck pedestals with rain covers for biometric readers shall be installed.	Comply		
10.7 (11)(i)	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.	Comply		
10.7 (11)(j)	Each boom shall incorporate a warning device such as lights or a siren, to indicate when the boom is in operation (opening or closing).	Comply		

10.7 (11)(k)	In case of a power failure, it shall be possible to mechanically raise and lower the boom.	Comply		
10.7 (11)(l)	The bearings of the boom shall be self-lubricating and maintenance free.	Comply with reference.		
11	Integration requirements			
11.1	General			
11.1(i)	The IACS shall be adaptable to cater for future integration requirements that Eskom will stipulate and at minimum it shall be integratable with the following systems:			
	1) Intrusion Detection system	Comply		
	2) Electric Fence system	Comply		
	3) Intercom and Public Address systems	Comply		
	4) CCTV system	Comply		
	5) Security Lighting system	Comply		
	6) Guard Tour system	Comply		
	7) Fire Detection system	Comply		
12	Buildings access control			
12 (1)	All entry points into buildings shall be secured by the Access Control system.	Comply		
12 (2)	Where viable, windows should be protected by burglar proofing, apart from areas where HV Regulations require otherwise.			
12(3)	All non-automated doors shall be fitted with a suitable grade security lock.			
12 (4)	In the administration buildings 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.			
13	Reporting			

13(i)	The Integrated Access Control System shall 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 xls, csv, and pdf file formats.	Comply with reference.		
13.1	Attendance Register			
13.1 (1)	A field labelled “Flexible time” should be added to the report			
13.1(2)	A field labelled “Leave” must be added to the report as this is currently contained in the manual attendance register form. This should integrate with SAP so leave is automatically filled in.			
13.1 (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.			
13.2	Visitor reports			
13.2 (1)	Visitor reports should cater for the requirements in Table 4 of 240-102220945	Comply		
13.2.1	Visitor/Host registration information			
13.2.1.1	The system shall cater for information fields depicted in Table 5 and Table 6 of 240-102220945 on information forms and databases to facilitate the ACS searches.	Comply		
13.3	Additional Reports			

13.3(i)	The system shall cater for additional reports as required by Eskom including but not limited to Access Denied Reports and Alarms reports	Comply		
13.4	Graphical User Interface Requirements			
13.4.1	Functional GUI Requirements			
13.4.1(1)	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.	Comply		
13.4.1(2)	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.	Comply		
13.4.1(3)	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.	Comply		
13.4.1(4)	The GUI must cater for importing drawing files of various types such as CAD files.	Comply		
13.4.1(5)	The GUI must cater for multiple floor levels – as required for buildings with more than a single floor.	Comply		
13.4.1(6)	The GUI should have the capability to display more than 1 screen (floor plan) at a time (split screens).	Comply		
13.4.1(7)	The GUI must cater for 3 dimensional models and views with related controls to navigate through the model.	Comply		
13.4.1(8)	The GUI must include a zoom function which allows for both zoom in and zoom out on floor plan views and 3 dimensional views.	Comply		
13.4.1(9)	The GUI must allow for colours to be configurable for the layouts	Comply		

13.4.1(10)	The system must cater for integration of various modules into this GUI. Readers, controllers, access points, cameras, intrusion detection system and other security 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	Comply		
13.4.1(11)	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.	Comply		
13.4.1(12)	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 converter connected to the door. The alarm should bring up details of what the hardware /tamper alert is.	Comply		
13.4.1(13)	The GUI should contain different icon types/styles for different equipment e.g. camera, reader, controller.	Comply		
13.4.1(14)	The GUI must have colour coding for hardware items depicted, i.e. use colour coding to indicate the status of hardware items.	Comply		
13.4.1(15)	Alarms must be 3 colours:	Comply		
	a) Red for high priority	Comply		
	b) Yellow for medium priority	Comply		
	c) Blue for low priority	Comply		
13.4.1(16)	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.	Comply		

13.4.1(17)	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.	Comply		
13.4.1(18)	A hardware failure or alarm should have an audible alarm sound together with the flashing icon.	Comply		
13.4.1(19)	The GUI should have a configurable threshold of the number of unacknowledged alarms and an automatic escalation via the e-mail / SMS gateway.	Comply		
13.4.1(20)	The GUI should have manual and automated methods of SMS and emailing alarms, especially for high priority alarms.	Comply		
13.4.1(21)	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.	Comply		
13.4.1(22)	Access to live and recorded camera footages must be possible from the camera links on the GUI.	Comply		
13.4.1(23)	The GUI should have an emergency contact list that the operators can quickly access in order to attend to an alarm.	Comply		
13.4.1(24)	On acknowledging/opening an alarm the GUI should display procedures to attending to the alarm.	Comply		
13.4.1(25)	The GUI should have the ability to capture sticky notes / comments to alarms and escalations.	Comply		
13.4.1(27)	GUI must show different zones and the number of people in each zone should be listed in the zone.	Comply		
13.4.1 (28)	Alarms should be displayed in real-time with the icons.	Comply		
13.4.1 (29)	Linked readers/controllers/power supplies etc. must open within 100 milliseconds requesting it to open.	Comply		

13.5	Databases			
13.5.1	General database requirements			
13.5.1 (1)	Database shall provide for regular reports and specific database queries, these should be viewable both locally (onsite) and also retrievable remotely from security control centre(s).	Comply		
13.5.1 (2)	Copies of reports from the database shall be kept for at least three years or as long as required for legal proceedings.	Comply		
13.5.1 (3)	The system shall allow for Logbook entries with the following as minimum features:			
	a) Alarm logbook for alarmed events generated by the system or peripheral devices	Comply		
	b) System logbook for all actions performed on the system	Comply		
	c) Event logbook for all events generated by the peripheral devices or by programs that are started up automatically in the background	Comply		
	d) Access logbook from all the readers	Comply		
	e) Time logbook for all time management related readings received from all the readers	Comply		
	f) Trend logbooks	Comply		
	g) Error logbook which is used for system errors as well for unauthorized access requests	Comply		
	h) Visitor logbook	Comply		
	i) Video logbook	Comply		
13.5.1 (4)	Database reports shall provide for the following functions:			
	a) Time and Attendance	Comply		
	b) Personnel tracking (Individual's historical movements to and from the various access points)	Comply		
	c) Date and time movements of Individuals or groups through the system	Comply		
13.5.2	Database structure			

13.5.2 (1)	The database shall allow for the following information to be included:			
	a) Eskom employee number (unique number)	Comply		
	b) Access ID (this shall be generated automatically by the system)	Comply		
	c) Full names and surnames	Comply		
	d) ID Number	Comply		
	e) Selection of access levels whereby the level where access is required is selected at the registration facility	Comply		
13.5.2 (2)	The employee status shall be either of the following:			
	a) Eskom employee	Comply		
	b) Sub-contractor	Comply		
	c) Visitor	Comply		
	d) Contractor	Comply		
	e) Security services	Comply		
	f) Vendor (to be used for regular visitor)	Comply		
14	Alarms			
14 (1)	The system alarms shall Comply with Specification for Integrated security Alarm system for protection of Eskom installations and its subsidiaries (240-86738968).	Comply		
14 (2)	2) Where access control and alarm monitoring are carried out on the same central display screen, the central display screen shall:			
	a) Serve as a logged message output device and an opera'or's screen;	Comply		
	b) Be capable of being used as an alarm display terminal;	Comply		
	c) Be able to view the alarm display and other displays concurrently ; and	Comply		
	d) While the screen is being used by the operator for card or system programming, allow logging to occur.	Comply		

14 (3)	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.	Comply		
14 (4)	System shall have the following alarms capabilities:			
	a) Alarm handling screen	Comply		
	b) Graphics associated with alarms	Comply		
	c) Alarm classification	Comply		
	d) Report back facility why the alarm occurred	Comply		
	e) Logging of all transactions in the alarm logbook	Comply		
15	Power supply			
15 (1)	The power unit of an access control system shall Comply with the requirements of SANS 2220-1-7.	Comply with reference.		
15 (2)	All backup supplies shall Comply with 240-53114248, Thyristor and switch mode chargers, AC/DC to DC/AC converters and inverter/uninterruptable power supplies standard.	Comply with reference.		
15 (4)	There shall be an intelligent power supply that monitors incoming power, battery status and only supply power to the servers.	Comply		
15 (5)	There shall be a backup battery that ensures at least 12 hours autonomy.	Comply with Reference		
15 (6)	The system shall still operate in the event of a main power failure.	Comply		
15 (7)	Each system or subsystem shall have a dedicated circuit breaker and supply circuit.	Comply		
15 (8)	There shall be UPS with sufficient capacity to support all ACS equipment for a minimum of 8 hours.	Comply		

15(9)	Electro-magnetic radiation from the UPS shall not affect the operation of other electronic equipment in the equipment room	Comply		
15 (10)	The battery system shall be maintenance free with a 5 year guarantee.	Comply		
16	Cabling requirements			
16 (1)	Cables shall Comply with the requirements of Eskom's Standard for Wiring and Cable marking in Substations (240-64636794).	Comply		
16 (2)	Terminal blocks shall be in accordance with Eskom standard 240-70413291, Specification for Electrical Terminal Blocks.	Comply		
16 (3)	All wiring shall be concealed inside trunking or conduit. No exposed wiring will be accepted except at sites where suitable cable trays are installed.	Comply		
16(4)	Cabling in roof or floor voids shall be installed in cable trays. Where cable trays are not available or viable, conduit will be acceptable.	Comply		
16 (5)	Cabling in trays shall be tied off at a maximum of 1.5m interval.	Comply		
16 (6)	Data and low voltage (0-48V DC/AC) cable installations shall be separated from mains power installations by a minimum of 500mm.	Comply		
16 (7)	Where data and low voltage cabling has to cross power cabling, this shall always be at 90° angles.	Comply		
16 (8)	Cabling in manholes shall be kept above the manhole floor level to avoid water contact.	Comply		
16 (9)	Cable shall be handled with care and not pulled with excessive force that may cause internal damage.	Comply		
16 (10)	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.	Comply		

16 (11)	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.	Comply		
16 (12)	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.	Comply		
16(13)	There shall be no cables running next to devices that may cause electro-magnetic interference.	Comply		
16 (14)	Tensioning of cables shall not exceed 10kg.	Comply		
16 (15)	Correct wiring schematic shall be followed.	Comply		
16 (16)	All wiring shall be terminated with bootlace ferrules of the appropriate size and colour to match the cable.	Comply		
16(17)	All bootlace ferrules shall be properly crimped and shall have good mechanical and electrical connection.	Comply		
16(18)	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.	Comply		
16 (19)	No short circuits shall be caused when cutting cables.	Comply		
16 (20)	Where cables are laid in trenches, they shall be armoured.	Comply		
16 (21)	Trenches shall be 600 mm deep measured from average ground level to the top of the upper sleeve or cable.	Comply		
16 (22)	Where any power reticulation work has been undertaken, contractors shall make provision to submit an approved reticulation certificate issued by an authorised electrical Contractor.	Comply		
16 (23)	With respect to site cabling, no cable joints shall be accepted between buildings and control room.	Comply		

17	Physical requirements			
17.1	Tamper protection			
17.1 (1)	Tamper protection for the electrical components of the IACS shall be in accordance with section 4.10 of SANS 2220-2-1	Comply with reference.		
17.2	Ingress protection			
17.2 (1)	The enclosures for the electrical and electronic circuits shall, unless otherwise specified, provide protection of class IP65 in accordance with SANS 60529.	Comply with reference.		
17.3	Safety			
17.3(i)	The mechanical construction of any part of the system shall be such that injury caused by mechanical instability or by moving parts, protruding or sharp edges is prevented.	Comply		
18	Environmental requirements			
18.1	General			
18.1 (1)	Access cards shall Comply with environmental requirements of 4.2 of SANS 2220-2-6.	Comply with reference.		
18.2 (2)	Biometric readers shall Comply with environmental requirements of 4.2 of SANS 2220-2-5.			
18.2 (3)	Servers/central processors shall Comply with environmental requirements of 4.2 of SANS 2220-2-2.	Comply with reference.		
18.2 (4)	Card readers shall Comply with environmental requirements of 4.2 of SANS 2220-2-3.	Comply with reference.		
18.2 (5)	Barriers shall Comply with environmental requirements of 4.8 of SANS 2220-2-7.	Comply with reference.		
18.3	EMC requirements			
18.3 (1)	Signal, voltage and electromagnetic radiation levels in readily accessible areas shall not be dangerous.	Comply with reference.		
18.3 (2)	System and its components shall Comply with requirements of SANS 61000-1-2.	Comply with reference.		
18.4	Earthing			

18.4 (1)	The Earthing of the system shall Comply with Eskom's earthing standards below:			
	a) 240 – 56872313 – Radio Station Earthing and Bonding.	Comply		
	b) 240 – 56356396 – Earthing and Lightning Protection Standard.	Comply		
	c) TST41-8–7 - Transmission Substation Design Earthing Standard	Comply		
19	Labelling and numbering			
19 (1)	Terminal boxes and terminals shall be numbered and labelled accordingly in line with the approved labelling standards specific to area of applicability.	Comply		
19 (2)	Numbering and labelling of system components 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.	Comply		
19(3)	Labelling at power stations, excluding nuclear power stations shall Comply with requirements of Plant Labelling and Equipment Description Standard (240-71432150).	Comply		
19 (4)	Labelling at Transmission sites shall Comply with requirements of Standard for Labelling of Secondary Plant Equipment (240-62362652).	Comply		
20	Markings			
20 (1)	Markings for access cards shall Comply with section 5 of SANS 2220-2-6.	Comply with reference.		
20(2)	Markings for biometric readers shall Comply with section 5 of SANS 2220-2-5.			
20(3)	Markings for servers/central processors shall Comply with section 5 of SANS 2220-2-2.	Comply with reference.		
20 (4)	Markings for card readers for shall Comply with section 5 of SANS 2220-2-3.	Comply with reference.		

20(5)	5) Markings for barriers shall Comply with section 5 of SANS 2220-2-7.	Comply with reference.		
21	Inspections and methods of tests			
21(1)	Inspections and methods of test for servers/central processors shall comply with section 6 of SANS 2220-2-2.	Comply		
21(2)	Card reader inspections and methods of tests shall comply with section 6 of SANS 2220-2-3.	Comply		
21(3)	Inspection and tests methods for biometric readers shall comply with section 6 of SANS 2220-2-5.	Comply		
21(4)	Inspection and methods of tests for reader controllers shall comply with section 6 of SANS 2220-2-4.	Comply		
21(5)	Inspections and methods of tests for access cards shall comply with section 6 of SANS 2220-2-6.	Comply		
21(6)	Inspections and methods of tests for barriers shall comply with section 6 of SANS 2220-2-7.	Comply		
22	Miscellaneous requirements			
22.1	Spares			
22.1(1)	The contractor shall provide a priced spares breakdown for each item of equipment.	Comply with reference.		
22.1(2)	The supplier shall indicate explicitly any licence conditions for associated software, what the duration of the licence is, and whether periodic payments would have to be made.	Comply with reference. Specify.		
22.1(3)	The supplier shall provide a recommended list of spares that Eskom should hold. The quantity of such spares will be a function of the installed base and MFBF figures.	Comply with reference. Specify.		
22.1(4)	There shall be provision for direct replacement spares to be obtained from the manufactures.	Comply with reference. Specify. Provide details of OEMs.		

22.1(5)	There shall be a formal OEM support and agent agreement letter provided by the supplier for local availability of spares and repair services.	Comply with reference. Specify.		
22.1(6)	There shall be a provision for Eskom to Establish contracts with external companies to facilitate the repairs of faulty equipment.	Comply with reference. Specify.		
22.1(7)	There shall be a provision to keep portable (non-strategic) spares in strategic stores and dispatched when required.	Comply with reference. Specify minimum spares holding.		
22.1(8)	There shall be provision to keep critical spares at minimum levels as identified by the custodians in the critical spares stores.	Comply with reference. Specify.		
22.1(9)	For emergency replacements where it could be difficult to wait for the spares to be dispatched, there shall be a provision to keep the spares at local stores.	Comply with reference. Specify.		
22.1(10)	There shall be provision to channel the spares from grids and other stake holders via an identified stores custodian who will exchange the faulty spare for the working one	Comply		
22.1(11)	Lead time to replace a spare shall be a day, at maximum.	Comply		
22.1(12)	Suppliers shall notify Eskom before they discontinue or modify any part of the system to allow procurement arrangements for the installed spares base.	Comply		
22.3	Training			
22.3(1)	Training courses for Eskom technicians shall be provided in the Republic of South Africa.	Comply		

22.3(2)	Courses shall be structured on a modular basis by individual equipment, such that a series of modules may be run consecutively to meet the needs of a particular group of trainees	Comply with Reference. Provide the course curriculum and accreditation information.		
22.3(3)	Unless the training needs to be provided in a specialized facility in South Africa, it is desirable that courses be conducted at various Eskom centres around the country	Comply		
22.4	Warranty			
22.4(1)	Suppliers shall state the warranty period on all offered equipment and the terms thereof.	Comply with Reference.		
22.4(2)	It is a requirement that the supplier accepts that on-site fault investigation shall be carried out by Eskom technicians with the warranty remaining intact.	Comply		
22.4(3)	The supplier shall indicate explicitly whether the equipment is limited in any way by licences and/or software maintenance agreements. In addition, the supplier shall include in the price the cost of all features, capabilities and capacities (i.e. will one have to pay for extra licences when either scaling up the deployment, or to get full functionality.	Comply with Reference.		
22.4(4)	The supplier shall indicate available options and costs for maintenances, upgrades, etc. of the offered equipment. In addition, the supplier shall furnish Eskom with technology roadmaps for the offered equipment.	Comply with Reference.		
22.5	Support contract & Repairs requirements			
22.5(1)	The supplier shall provide a repair service for faulty units, subunits and modules removed from site by Eskom technicians.	Comply		

22.5(2)	Within the contracted repair turnaround time, the supplier shall return to Eskom either the repaired item or a replacement thereof	Comply		
22.5(3)	Repaired items shall be warranted against a repetition of the same fault for a period of three months from the date of return.	Comply		
22.5(4)	The turnaround time for the repair and return service shall be thirty (30) calendar days.	Comply		
22.5(5)	The contractor shall provide a 24 h standby service.	Comply with Reference. Contact details and response footprint.		
22.5(6)	The contractor shall provide a technical assistance and support service for second and third line maintenance locally.	Comply with Reference. Contact details and response footprint.		
22.5(7)	The contractor shall provide software updates, patches and/or firmware when they become available.	Comply		