1. Description of the service

THE PROVISION FOR SUPPORT AND MAINTENANCE FOR CCTV CAMERAS, PA SYSTEMS, ACCESS CONTROL SOFTWARE INCLUDING VISITOR MANAGEMENT SYSTEMS AND THE PHYSICAL ACCESS CONTROL SECURITY INFRASTRUCTURE, IE. BOOMS, GATES, TURNSTILES, GATES MOTORS AT FACILITIES UNDER THE GEMMA CLUSTER.

Scope Purpose

The purpose of the scope is to outline the requirements for the undertaking of support and maintenance services to the security technology systems, ie. IP CCTV (Closed Circuit Television) cameras, the Physical Access Control Systems (PACS), ie, (Booms, gates, gate motors, non-lethal energised fencing) access control software and the related field equipment, Public Address Systems, headend and filed equipment infrastructure. ie, Video Management Systems (VMS) and Network Video Recorders (NVRs), network switches including the training of select engineers and technicians within the GEMMA Cluster.

The scope of work includes:

The services defined will be a combination of strategic and technical response to the cluster requirements for support and Maintenance solutions for various technology solutions. The services will include among others, the following: -

- Planned preventative maintenance to all installed and integrated field hardware.
- Planned preventative and reactive maintenance to the applications and databases.
- Training for Eskom 1st line support team
- Preparation of maintenance plans
- The service may include Priority 1 and Priority 2 spares holding
- The incumbent service provider shall undertake visits to the premises to visually assess, inspect, test, bond, repair, do programming and configuration of the existing security technology systems to OEM Specifications and ensure that all the listed systems are returned to service and are operable from the Cluster Security Control Centre.
- The appointed service providers must install the necessary equipment, software and also work with Eskom Telecoms Department to ensure that the security technology systems are integrated and are operable from the Cluster Security Control centre.

Eskom Telecoms build and provide the necessary field network equipment and bandwidth to ensure connectivity to the Cluster security Control Centre.

Operational activities per area of specialisation CCTV Cameras

- Check history of CCTV system and other peripheral equipment
- Visually inspect all major equipment components including cabling & connections where accessible for signs of deterioration or damage and undertake repairs
- Check all CCTV control equipment (monitors, NVR's, network switches, cabling etc.)

and Physical Access Control infrastructure.

- Check and clean cameras, readers, lenses and housings as necessary.
- Check lenses for correct field of view and adjust as necessary
- Check pictures for correct field of view and adjust as necessary.
- Check and test remote signalling equipment
- Check recording and playback quality
- Check the satisfactory transmission of images to remote control centre
- Repair minor faults where necessary.
- Training of the users on how to use, maintain and support the system in order to operate more effectively and efficiently.
- Log all systems test results
- Return all security equipment, components and systems to operational status.
- Respond to faults and queries within specified response period.
- In the instance of cameras and other equipment failure, a swap-out must be used to ensure that downtime is kept to a minimum.
- Removal, safekeeping and re-installation of existing CCTV cameras and other security infrastructure.

ACCESS CONTROL SYSTEMS (SOFTWARE and hardware).

- Check whether personnel have experienced any problems with the system.
- Check history of Access control system since last operating period.
- Check connection between Main Power Supply and Backup Battery test to ensure that enough power is being supplied to the panel
- Visually inspect all fields devices for Access Control System
- Walk test some devices either manually and or using a card, finger in the case of readers.
- Check operation of emergency break glasses and mechanical exits.
- Check operation of readers.
- Check operation of maglocks and LEDs.
- Check communications with all controllers and reset error log.
- Check communication between Server and field devices (door controllers)
- Check operation of Input / Output controller and relays.
- Check access control software.
- Re-program any minor changes as required by the client

- Check door open times.
- Back-up historic data and database. Ensure the customer keeps this in a secure location.
- Verify correct operation of doors in a fire condition.
- Test the system for all alarm and ensure that alarms desired are received by the system
- Carry out minor adjustments.
- Training of the users on how to use, maintain and support the system in order to operate more effectively and efficiently.

Implement remote support by means of a telephone or remote-control software to troubleshoot any minor adjustments that need to be made.

PHYSICAL ACCESS CONTROL SYSTEMS (Booms, doors, Turnstiles, Gates, gate motors, etc.).

- Check history of operating period.
- Check current operation of the Equipment
- Check and verify all incoming Voltage to the equipment
- Dust and Clean all parts
- Grease and Oil all moving parts as required
- Fasten any loose moving parts
- Tune Wings and gears movement to allow for smooth operation
- Photocell testing ensures the correct and safe operation of the Arms
- Automatic Testing to check all necessary functions of the Turnstile
- Check for any scratches and rust and accordingly clean and fill using red-oxide
- Check battery operations
- Check all terminations and cables for wear and tear
- Check all insulations of all cables is in good condition and rectify as required
- Check all physical access control systems including doors to ensure that they are mechanically sound to be able to ensure seamless integration with the electronic access control solutions.
- All doors to the building must be armed and integrated with the access control system to ensure that they are able to trigger all alerts including door adjar signal and timing and irregular exit from the emergency exit.
- Simulate fault logic to check for alarms and errors.
- Training of the users on how to use, maintain and support the system in order to operate more effectively and efficiently.

Public Address systems

- Check installation against records, report and record any discrepancies.
- Check operation of the system.
- Check, (under full connected load), the audio quality for any discernible distortion.
- Check cable terminations and check cable termination records.
- Measure and record resistance of all speaker lines at main equipment.
- Check labelling of speaker selection unit.
- Check all equipment for damaged, stressed or heated components.
- Check output voltage regulation of power supplies.
- Check equipment for proper ventilation.
- Record all results in logbooks.
- Training of the users on how to use, maintain and support the system in order to operate more effectively and efficiently.

BREAK GLASS UNITS

- Each break glass unit shall be activated and checked for correct operation including all remote indication associated with the relevant break glass unit.
- Each break glass unit shall be inspected during the service to be in a good condition and not damaged.
- Each break glass unit or shall be wiped clean during the service.
- Ensure that during the service each break glass unit is recorded as per its number on the service report sheet and checked accordingly.
- Training of the users on how to use, maintain and support the system in order to operate more effectively and efficiently.
- The break units shall be synchronised with the access control system to trigger alarms into the security control centre every time they are irregularly broken to gain unauthorised exit.

Remedial Actions and Documentation

- Any equipment, etc. failures must be immediately reported to Eskom.
- All routine maintenance four (4) times a year shall be documented (3 monthly), and these records shall be held by Eskom for a minimum of 3 years.
- On completion of each inspection and maintenance service, the service providers shall present, for the customer’s signature, an acceptance certificate, which will be a condition for invoice payment.

Ad hoc Maintenance (Faults)

- All equipment identified as faulty shall be brought to the attention of Eskom.
- There shall be a clear, documented, process for reporting faults on the security system, including expected timelines and names of responsible people.
- Response will be required on the same day unless otherwise negotiated.
- In the case of an emergency, meaning a situation with life threatening consequences or situation that will cause damage to property or equipment, Eskom representative will state clearly that this is an "Emergency situation and immediate response will be required.
- There can as part of the contract render a repair service of faulty equipment at a rate & condition submitted. This process will be finalised at the contract awarding stage.
- On arrival at site, the service providers' field staff will first report to the security

control centre and Eskom representative on site if applicable.

- Once the repair or replacement is completed, relevant Site Acceptance Tests shall be conducted and documented before the work shall be signed as accepted by Eskom.
- On completion of each inspection and maintenance service, the service providers shall present, for the customer's signature, an acceptance certificate, which will be a condition for invoice payment.
- Equipment replaced on site remains the property of Eskom and this original (broken) equipment must be returned.
- In the invent where equipment is unrepairable the scrapping process must be followed.
- All equipment that fails within the warranty period will be replaced at the service

providers' expense.

- All equipment replaced will have a new full warranty period as with the original installed equipment.
- Equipment repaired will have a pro rata warranty as agreed to upfront – at tender award stage
- When replacing a camera, a licence for the replaced camera must be issued to Eskom.
- Additional support – commissioning of new sites onto the VMS system
- Provide support and configure new sites onto the VMS system at the security control room. As and when needed.

Integration of subsystems Integration with Security fences

- The perimeter non-lethal electric fence system shall be connected to the Surveillance system and shall be integrated into the overall security system to ensure effective access monitoring and control both locally and remotely from the Security Control Centre.
- Alarms will be automatically triggered with CCTV needing to highlight the triggered area.

Integration with CCTV system

- The CCTV system shall be an IP based smart solution.
- 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.
- Guards shall be able verify positive alarm events in the event of an attempted or successful intrusion attempt on the fence system.
- CCTV monitoring shall be conducted at the main vehicle entrance as an overview of the area and to serve as identification point for visitors.
- The system shall utilize a video analytics system as pre-detection to automatically create alarms and perform event recording.
- 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.
- The CCTV system shall be connected to the Eskom WAN to enable event driven video streaming to The Security Control Room. Sufficient bandwidth to enable this requirement shall be provided by Eskom.

Integration with Intrusion Detection System

- 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;

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

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

- 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.

Integration with Access gates

- 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.
- Where applicable, the verification process at entrances shall be as follows: This is applicable where interlocking system is in place:
- Upon positive verification the energized gate shall open after which the outer barrier gate will open to allow the vehicle inside the sally point.

- Upon entry into the sally point, the outer barrier gate will close effectively locking the visitor in the sally point.
- At this time, the guard will be able to interact with the visitor and conduct searching of the person and vehicle.
- 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.
- 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 guardhouse before the system will open.
- 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.
- When the visitor on his turn can then again tag in the reader in the sally point data carrier only).
- At this time, the inner gate will open to allow the visitor into the restricted area.
- Exiting of the site will be the reverse operation of the entry sequence.

Integration with Intercom system

- A video intercom system shall be connected to the local NVR to ensure both visual and audio recording of events.
- Guards shall be able to interact with unannounced visitors and non-Eskom staff whom might not be accredited without leaving the safety of the guardhouse.
- The communication shall be point-to-point between the gates and guardhouses and shall not be integrated with the gate control system.
- The intercom function shall be extended to the control room office for intercom operation during daytime hours when guards will not be on duty.

Integration with Security lighting

- All entrances into ESKOM facilities shall be equipped with lighting to ensure visible security can be applied.
- Security lighting shall furthermore be integrated using motion detection through the intruder alarm system with the various security systems such that it provides a bright perimeter for guards to observe the perimeter during evening patrols and in situation where responding to fence alarms.

Integration with Guard Tour System (Where applicable)

- Guard Tour System shall be integrated to the Integrated Access Control System 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.

- This system shall be tied into the Intruder Alarm system for providing alerts in the Control Room.

Integration with the PA system

- 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 guardhouse and remotely via the central Control Room 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.

Dashboards

- Dashboards are used to present a wide range of different data metrics in a single comprehensive display of various sizes.

- Dashboards shall be customisable for use in large video wall size displays or for small smart-phone enabled devices as a quick comprehensive glimpse into the overall status of the building.

- Dynamic graphics shall be implemented in a responsive design manner with visualisation of facilities, plants, etc.

- Dashboards shall be device and operating system agnostic.

Management of Downtime

- After a fault has been logged and forwarded to the Service provider. The service provider are expected to respond within 12 hours and will be expected to minimise the maintenance time to ensure the minimal interference/disruption of the normal business as well as the downtime of the security installation.

Work Schedule/ Work order process.

Preventative maintenance – Plant to have a maintenance plan in place for all sites (4 x routine maintenance on a 3 monthly basis) for each annual term of the contract.

Faults – Security control room to alert service providers via issuing purchase orde

General

- The service providers' technicians shall perform all mandatory and optional security

compatible, and virus protected system software upgrades:

- Provide all manufacturers required maintenance services; conduct operational system tests; repair or replace all failed security system equipment, devices, or components and other duties as required by the Cluster to maintain the Security Technology Systems optimally operational and in good working order.

- The service provider shall perform mandatory software upgrades for the cluster at no additional cost to the cluster.

- Optional software upgrades shall be presented to the cluster for consideration and approval prior to installation.

- The costs associated with optional software upgrades shall be borne by the cluster.
- Prior to any software upgrade, the service providers shall insure that a copy of the existing operating system is on hand and the technicians shall make a copy of the system data file.
- Upon completion of the upgrade, the technician shall create two copies of the old and the new operating system software and data file software.
- The old software shall be labelled as “Replaced, with (revision #)”, “by (Technicians Name)”, and Date.
- The new software shall be labelled with “Current (revision #)”, “installed by (Technicians Name)”, and Date.
- One copy of each shall be retained by the technician onsite and one copy provided to the Client for archival storage.
- The service providers shall perform all manufacturers’ recommended maintenance for each security device, component, panel, subsystem, and system as a minimum each item shall be visually inspected, cleaned and documented.
- Network diagram for substations, facilities and control rooms must be established clearly mapping out the installation as well as the corresponding labels.
- The network diagram must be amended as and when changes occur ensuring, that it is always up to date.
- On completion of each inspection and maintenance service, the service providers shall present a report.
- The service provider shall provide a document to indicate the equipment’s functional status and All passwords, IP addresses and CMS licenses must be given to security control rooms prior to hand-over.
- At no given time will passwords and login credentials be changed without consensus from the security control room supervisor.
- A full handover shall be conducted. This will include a scheduled engagement with the succeeding service providers whereby all relevant documentation will be handed over.
- The engagement will be hosted by the contract owner.
- Documentation is to include details on the current equipment installed, status of the equipment, maintenance history on the equipment, login credentials and password information and the updated network diagram.
- After the documentation has been handed over, visual inspection will be done with both service providers to ensure that the documented information is correct.
- Once completed an official sign-off will be done.