# AIR TRAFFIC AND NAVIGATION SERVICES CO. LTD

# REPUBLIC OF SOUTH AFRICA

## APPOINTMENT OF A SERVICE PROVIDER FOR SUPPLY, DELIVERY, INSTALLATION AND COMMISSIONING OF SECURITY SYSTEMS AT NON-ACSA AIR TRAFFIC SERVICES UNITS WITHIN THE JOHANNESBURG REGION THAT INCLUDES ACCESS CONTROL SYSTEMS, CLOSED-CIRCUIT TELEVISION (CCTV) SYSTEMS, INTRUDER ALARM SYSTEMS AND INTERCOM SYSTEMS INCLUDING THE SUPPORT AND MAINTENANCE OF THE NEW SECURITY SYSTEMS AND DECOMMISSIONING AND DISPOSAL OF THE EXISTING REPLACED SECURITY SYSTEMS.

## APRIL 2024

### TECHNICAL SPECIFICATIONS (ANNEXURE A)

## APRIL 2024

**The information contained within this document is confidential to ATNS in all respects and it is hereby acknowledged that the information as provided shall only be used for the preparation of a response to this document.  The information furnished will not be used for any other purpose than stated and that the information will not directly or indirectly, by agent, employee or representative, be disclosed either in whole or in part, to any other third party without the express written consent by the Company or its representative.**

## TABLE OF CONTENTS

ABBREVIATIONS....................................4

1. SCOPE OF WORK....................................6

2. SUMMARY OF REQUIREMENTS....................................6

2.1 Location Description....................................6

2.2 Items Required....................................6

CHAPTER 1: GENERAL REQUIREMENTS....................................8

1. ENVIRONMENTAL CONDITIONS....................................8

2. MAINS SUPPLY....................................8

3. SYSTEM LIFESPAN....................................8

4. SYSTEM HOUSING....................................9

5. USER CAPABILITIES....................................9

6. SOFTWARE REQUIREMENTS....................................9

7. NETWORK COMMUNICATION LAYOUT....................................9

8. DECOMMISSIONING AND DISPOSAL....................................10

CHAPTER 2: ACCESS CONTROL SYSTEM....................................11

1. MAIN ACCESS CONTROL SYSTEM....................................11

1.1 General....................................11

1.2 Access Control Management System....................................12

2. AUXILIARIES AND SUPPORT SYSTEMS....................................12

2.1 Proximity Reader....................................12

2.2 Door Controller....................................14

2.3 Access Cards and Card Printing Machine....................................15

2.4 Locking Mechanism....................................15

2.5 Automatic Door Closures....................................16

2.6 Door Open/Close Sensor....................................16

2.7 Network Connectivity....................................16

CHAPTER 3: CCTV SYSTEM....................................18

1. CCTV SYSTEM....................................18

2. CAMERA SPECIFICATIONS....................................18

3. OPERATOR POSITIONS....................................19

4. NETWORK VIDEO RECORDER....................................19

CHAPTER 4: INTRUDER ALARM SYSTEM....................................21

1. GENERAL....................................21

2. ALARM CONTROL PANEL....................................21

3. MAGNETIC CONTACTS....................................21

4. MOTION DETECTORS....................................21

CHAPTER 5: INTERCOM SYSTEM....................................22

1. INTERCOM SPECIFICATIONS ........ 22
CHAPTER 6: SYSTEM INTEGRATION ........ 23
1. SYSTEM INTEGRATION ........ 23
CHAPTER 7: PROJECT MANAGEMENT SPECIFICATIONS ........ 24
1. PROJECT MANAGEMENT REQUIREMENTS ........ 24
1.1 Draft Plans ........ 24
1.2 Project Management Plan ........ 24
1.3 Project Schedule ........ 24
1.4 Resource Management ........ 25
1.5 Risk Management ........ 25
1.6 Quality Management ........ 25
1.7 Installation, Transitioning and Commissioning ........ 25
1.8 Environmental Management Programme ........ 25
2. SYSTEMS ENGINEERING ........ 26
CHAPTER 8: ........ 27
LOGISTIC SUPPORT REQUIREMENTS ........ 27
1. TRAINING ........ 27
2. WARRANTY ........ 27
3. SPARES ........ 27
4. SUPPORT CONTRACT ........ 27

# ABBREVIATIONS

| | |
|---|---|
| ATC | Air Traffic Controller |
| ATNS | Air Traffic and Navigation Services SOC Ltd |
| ATSU | Air Traffic Services Unit |
| CCTV | Closed-Circuit Television |
| COC | Certificate of Compliance |
| EMPr | Environmental Management Programme |
| ET | Engineering Technician |
| FAGM | Rand Airport |
| FAKN | Kruger Mpumalanga Airport |
| FALA | Lanseria Airport |
| FAMM | Mahikeng Airport |
| FAPP | Polokwane Airport |
| FAR | False Acceptance Rate |
| FAWB | Wonderboom Airport |
| FRR | False Rejection Rate |
| HD | High Definition |
| HDMI | High-Definition Media Interface |
| HMI | Human Machine Interface |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronic Engineers |
| IP | Ingress Protection |
| LAN | Local Area Network |
| LED | Light Emitting Diode |
| MATS | Manager Air Traffic Services |
| MTS | Manager Technical Services |
| N/C | Normally Closed |
| N/O | Normally Open |
| NVR | Network Video Recorder |
| OIC | Operator in Charge |
| ONVIF | Open Network Video Interface Forum |

| | |
|---|---|
| PC | Personal Computer |
| PIN | Personal Identification Number |
| PIR | Passive Infrared |
| PMP | Project Management Plan |
| PoE | Power over Ethernet |
| PVC | Polyvinyl Chloride |
| RFID | Radio Frequency Identification |
| SANS | South African National Standards |
| SAWS | South African Weather Services |
| SSD | Solid State Drive |
| STS | Supervisor Technical Services |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| UML | Unified Modelling Language |
| UPS | Uninterrupted Power Supply |
| WBS | Work Breakdown Structure |
| WDR | Wide Dynamic Range |

# 1. SCOPE OF WORK

The project calls for the procurement, delivery, installation and commissioning of security systems at non-ACSA Air Traffic Services Units within the Johannesburg Region that includes access control systems, Closed-Circuit Television (CCTV) systems, intruder alarm systems and intercom systems. The security systems will be deployed in the following Air Traffic Services Units (ATSUs):

- Lanseria Airport (FALA)
- Wonderboom Airport (FAWB)
- Rand Airport (FAGM)
- Mahikeng Airport (FAMM)
- Polokwane Airport (FAPP)
- Kruger Mpumalanga Airport (FAKN)

The scope of the project further includes the support and maintenance of the new security systems and decommissioning and disposal of the existing replaced security systems.

# 2. SUMMARY OF REQUIREMENTS

## 2.1 Location Description

The table below provides a high-level description of each location.

**Table 1: Description of each site.**

| NAME | TYPE | DESCRIPTION |
|---|---|---|
| Lanseria Airport (FALA) | ATSU | Building |
| Wonderboom Airport (FAWB) | ATSU | Building (part of the rescue and fire building) |
| Rand Airport (FAGM) | ATSU | Building (part of the main airport building) |
| Mahikeng Airport (FAMM) | ATSU | Building |
| Polokwane Airport (FAPP) | ATSU | Building |
| Kruger Mpumalanga Airport (FAKN) | ATSU | Building |

## 2.2 Items Required

The tables below summarise the items required per location.

**Table 2: ATSU items required.**

| ATSU | Requirements | Quantity / Capacity |
|---|---|---|
| Lanseria Airport (FALA) | CCTV System | 2 Cameras |
| | | |

| | | |
|---|---|---|
| Wonderboom Airport (FAWB) | Access Control System | 2 Access points<br>1 Card printing machine |
| | CCTV System | 3 Cameras |
| | Intercom | 1 Gate Station<br>1 Handset |
| | | |
| Rand Airport (FAGM) | Access Control System | 2 Access points |
| | CCTV System | 2 Cameras |
| | Intruder Alarm System | 1 Control Panel<br>1 Perimeter Door<br>1 Zone |
| | Intercom | 1 Gate Station<br>1 Handset |
| | | |
| Mahikeng Airport (FAMM) | Access Control System | 3 Access points |
| | CCTV System | 3 Cameras |
| | Intercom | 1 Gate Station<br>1 Handset |
| | | |
| Polokwane Airport (FAPP) | Access Control System | 2 Access points |
| | CCTV System | 2 Cameras |
| | Intercom | 1 Gate Station<br>1 Handset |
| | | |
| Kruger Mpumalanga Airport (FAKN) | Access Control System | 3 Access points |
| | CCTV System | 2 Cameras |
| | Intercom | 1 Gate Station<br>1 Handset |
| | | |

# CHAPTER 1: GENERAL REQUIREMENTS

## 1. ENVIRONMENTAL CONDITIONS

[A] The security systems and its auxiliary components offered shall operate within specifications without any degradation in performance under the following environmental conditions and tolerances.

**Table 3: Environmental Conditions.**

| **Parameter** | **Value** |
|---|---|
| **Outdoors** | |
| Temperature | -10° to +55°C |
| Relative Humidity | 10% to 90% (non-condensing) |
| **Indoors** | |
| Temperature | -5 °C to +35 °C |
| Relative Humidity | 10% to 80% (non-condensing) |
| **Protection Rating** | |
| Ingress Protection (IP) Rating | IP65 (Except where indicated otherwise) |
| Mechanical impact protection rating | IK08 |

## 2. MAINS SUPPLY

[A] The security systems shall be powered from an existing online Uninterrupted Power Supply (UPS) to protect the system from surge currents/voltages and provide continuous backup power should the main power supply be interrupted.

[B] Those devices that cannot be supported by the UPS shall be provided with a battery backup. The battery backup shall be able to keep the device operational for a minimum period of 6 hours after a power failure. The devices that will require a battery backup shall be capable of providing a low battery alert.

[C] All electrical work shall comply to SANS 10142-1.

[D] A Certificate of Compliance (COC) for all electrical work performed shall be supplied.

## 3. SYSTEM LIFESPAN

[A] The design life of the security systems offered shall be at least 10 years.

## 4. SYSTEM HOUSING

[A] One (1) dedicated 19-inch, wall mountable equipment cabinet shall be provided to house the equipment for the security systems as well as the associated support and auxiliary hardware offered for each of the other ATSU's.

[B] The wall mountable equipment cabinet shall be installed in the equipment room at each of the other ATSU's.

## 5. USER CAPABILITIES

[A] The security systems shall cater for different users with configurable user permissions.

[B] The security systems shall be configurable to cater for at least three (3) user levels and associated permissions as shown in the table below.

**Table 4: User permissions.**

| # | USER | PERMISSIONS |
|---|---|---|
| 1 | Super User | Full system access |
| 2 | Administrator | All access excluding configuration changes. |
| 3 | General User | View only with limit control (e.g., 5-min playback, camera selection) |

## 6. SOFTWARE REQUIREMENTS

[A] Software updates, patches, new versions, and new releases on all systems shall not overwrite, alter, amend or impact on the operational system configuration and operational system parameters. All systems shall be able to revert to previous software versions.

## 7. NETWORK COMMUNICATION LAYOUT

[A] The Access Control System and the CCTV System shall make use of the existing network, where applicable, for communication between the various components (i.e., door controllers, cameras, etc.).

[B] New CAT6 Ethernet cables shall be installed to connect the necessary equipment (i.e., cameras, door controllers, etc.) to the network. A maximum length of 30m of cable per item, shall be quoted for at each location to cater for each of the items (camera, door controllers, etc.).

[C] All cabling shall be neatly installed in cable ducting/trunking.

[D] Once the installation is completed, the total length of cable, trunking and ducting used will be audited and ATNS will pay the contractor accordingly.

## 8. DECOMMISSIONING AND DISPOSAL

[A] The existing security equipment that are replaced shall be uninstalled, disassembled and disposed of in an environmentally friendly manner and in line with current environmental laws.

[B] Waste shall be managed according to the ATNS waste management policies and there shall be adherence to the requirements of the National Waste Management Act: Waste  Act (No.59 of 2008).

[C] Records of disposal shall be kept at sites and also sent to ATNS Environment & Sustainability Department.

# CHAPTER 2: ACCESS CONTROL SYSTEM

## 1. MAIN ACCESS CONTROL SYSTEM

### 1.1 General

[A] The access control system shall consist of, the following devices, including but not limited to:

I. Server
II. Proximity readers
III. Door controllers
IV. Desktop for enrolment of new users - biometrics, Radio Frequency Identification (RFID) and Personal Identification Number (PIN) code registration
V. Biometrics enrolment reader/writer
VI. Card printing machine
VII. Locking mechanisms (Magnetic door lock)

[B] The access control system shall be scalable.

[C] The access control system shall cater for multiple entry/exit points.

[D] The access control system shall allow for the configuration of different zones with different access rights. The access control system shall thus allow for the configuration of zones to have restricted access to authorised personnel only.

[E] Each zone shall be monitored by the access control system and a record of users entering and exiting the zone shall be kept.

[F] The cabling for the new access control system shall be installed in the existing cable routes, ducts and trays as far as possible.

[G] The access control system shall allow for visitors and contractors to be enrolled on a temporary basis with an access time or duration limit. Visitors and contractor's identification details shall be stored on the database.

[H] All devices associated with the access control system shall have a power status indicator.

[I] The access control system shall cater for an interface from the existing fire detection system. The interface shall be a N/O (normally open) relay contact or a N/C (normally closed) relay contact.

[J] In the event of a fire and during an emergency evacuation, the access control system shall unlock all doors automatically.

### 1.2 Access Control Management System

[A] A central access management system shall be provided to manage the access control system.

[B] The access management system shall have a user-friendly Human Machine Interface (HMI).

[C] The access management system shall cater for administrator access to the server and database where users and events are stored.

[D] The access management system shall allow for the setting up of access zone profiles. The system shall allow for the different zone profiles to be applied to specific user types. The system shall allow for access to be scheduled and restricted during specific times.

[E] The access management system shall generate a visual and audible alarm/alert when an entry/exit door is left open for longer than a configurable duration.

[F] The access management system shall log and track all system changes. The system shall be capable of extracting all system changes into a report in pdf format.

[G] The Unified Modelling Language (UML) architecture of the access management system software shall be provided.

## 2. AUXILIARIES AND SUPPORT SYSTEMS

### 2.1 Proximity Reader

[A] There shall be 2 proximity readers installed for each of the entry/exit points as defined in the table below.

| **Location** | **Entry/Exit Points** | **Associated Readers** |
|---|---|---|
| FAWB | 2 | 4 |
| FAGM | 2 | 4 |
| FAMM | 3 | 6 |
| FAPP | 2 | 4 |
| FAKN | 3 | 6 |

[B] The proximity readers shall have the ability to identify personnel by means of:

I. RFID cards
II. Fingerprints
III. Keypad PIN codes
IV. Any combination of the above

[C] The proximity readers shall support Transmission Control Protocol/Internet Protocol (TCP/IP) network communication.

[D] The proximity readers shall support PoE (Power over Ethernet).

[E] The proximity readers shall provide an indication to show when access is granted or denied. If the indication is in the form of a LED light, the LED shall glow green when access is granted and red when access is denied.

[F] The proximity reader shall support the following RFID technologies, including but not limited to:

I. HID 125KHz
II. MIFARE 1K
III. MIFARE 4K
IV. MIFARE Ultralight / C
V. MIFARE DESFire / EV1
VI. MIFARE Mini

[G] The proximity reader shall have a card reading distance of 0 to 5cm.

[H] The proximity reader shall have a card reading duration of less than 1 second.

[I] The proximity reader shall have an optical fingerprint module.

[J] The proximity reader shall have a fingerprint comparing mode of 1:1 and 1:N.

[K] The proximity reader shall have a fingerprint False Acceptance Rate (FAR) of less than 0.001%.

[L] The proximity reader shall have a fingerprint False Rejection Rate (FRR) of less than 0.01%.

[M] The proximity reader shall be plug-and-play and seamlessly integrate with the access management system.

[N] All outdoor proximity readers shall have an IP67 rating and shall be fitted with an outdoor weatherproof housing to protect the unit from direct sunlight. Weatherproof housings shall be provided for as per the table below.

| **Location** | **Positions** | **Weatherproof housings** |
|---|---|---|
| FAGM | • Main Entrance | 1 |
| FAKN | • Main Entrance | 1 |

## 2.2 Door Controller

[A] The access control system shall incorporate door controller(s). Door controllers can be associated per system, or per zone, or per door or per proximity reader.

[B] The supplier's system configuration shall determine the number of door controllers to accommodate the number of entry/exit points and associated proximity readers per location as indicated in the table below.

| **Location** | **Entry/Exit Points** | **Associated Readers** |
|---|---|---|
| FAWB | 2 | 4 |
| FAGM | 2 | 4 |
| FAMM | 3 | 6 |
| FAPP | 2 | 4 |
| FAKN | 3 | 6 |

[C] All door controllers shall be installed in a manner that the controller and all cables connected to it are secured and temper proof.

[D] The door controller(s) shall have a storage capacity that can accommodate the database, of unique identification (biometrics, RFID card and PIN code) information, for a minimum of 100 people per location.

[E] The database on the door controller(s) shall be updated/synchronised when changes are made at the access management system.

[F] All events from the door controllers shall be recorded and stored on the central server. During a power or network outage, the door controller(s) shall have a storage capacity to cater for at least 100,000 events until the power or network is restored.

[G] The door controller(s) and all associated devices (i.e., proximity readers, locking mechanisms, etc.) shall be able to function independently of the connection to the server and the backup power supply.

[H] All data stored on the door controller(s) shall be retained during a power failure.

[I] A bypass key switch shall be installed on the unsecured side of each door where a door controller is installed. All bypass keys for one location shall be keyed alike. At least four (4) copies of the bypass keys shall be provided at each location.

[J] A green resettable emergency door release call point shall be installed on the secure side of each door where a door controller is installed.

## 2.3 Access Cards and Card Printing Machine

[A] RFID cards which are compatible with the access control system shall be provided with the system.

[B] Blank Polyvinyl chloride (PVC) cards shall be provided for ATNS employee credentials to be printed on.

[C] There shall be at least fifty (50) RFID cards and one hundred (100) PVC cards provided per location.

[D] Three (3) types of printing templates for the employee cards shall be designed and supplied. The layout of the templates shall be provided by ATNS after contracting.

[E] There shall be one (1) user registration workstations with a biometric reader/writer and associated card printing station installed in the tower cab at each location.

[F] All workstations shall have the capability to enrol new users and print access cards.

[G] Card printing machines shall be delivered with a colour printer ribbon. Each printer ribbon shall have a yield of at least 500 cards.

[H] One spare colour printer ribbon shall be provided for each card printing machine.

## 2.4 Locking Mechanism

[A] A locking mechanism shall be provided for each of the entry/exit doors where a door controller is installed.

[B] The locking mechanism shall be a magnetic lock or equivalent.

[C] The locking mechanism shall have minimum break force of 500kg.

[D] The locking mechanism shall be compatible with the proposed door controller.

[E] The locking mechanism shall be installed on the inside of the door and the design shall cater for doors opening to the outside as well as to the inside.

[F] The locking mechanism shall have an LED to display the lock status.

[G] The locking mechanism shall generate an output signal to provide the lock status to the door controller and the access management system.

[H] The locking mechanism shall cater for an interface from the intercom system, where applicable, so that it can be unlocked from the intercom's handset.

## 2.5 Automatic Door Closures

[A] All doors and gates, where a door controller is installed, shall be fitted with an automatic door closure.

[B] The door closure shall be able to cater for a door weight of up to 50kg.

[C] All door closures shall be installed indoor.

[D] The closing and latching speed of the door closures shall be adjustable.

## 2.6 Door Open/Close Sensor

[A] A door open/close sensor shall be installed on all entry/exit points where a door controller is installed.

[B] The door open/close sensor shall communicate the status of the door to the door controller and the access management system.

[C] An audible alarm, configurable per door, shall be generated at each door, if the door is left open for longer than a configurable duration. This will mostly be required at external access points and will be de-activated for internal access points. It must be possible to cancel the alarm, locally at the door, by means of a cancellation pin code.

## 2.7 Network Connectivity

[A] The access control system and all associated devices shall support TCP/IP for network connectivity.

[B] All the devices associated with the access control system shall support Power over Ethernet (PoE).

# CHAPTER 3: CCTV SYSTEM

## 1. CCTV SYSTEM

[A] A CCTV surveillance system shall be installed at the locations as indicated in Table 2.

[B] The CCTV system shall be at least an 8-channel system.

[C] The CCTV system shall cater for remote monitoring on a mobile device. The remote mobile monitoring shall be made available for the respective Operator in Charge (OIC) at each location. ATNS shall provide the internet connection for remote monitoring.

[D] The CCTV system shall support the capability of offsite monitoring from a central control room. The bandwidth requirements to achieve this must be provided.

[E] The CCTV system devices shall be Open Network Video Interface Forum (ONVIF) compliant devices.

## 2. CAMERA SPECIFICATIONS

[A] The types of cameras required at each location are shown in the table below.

| Camera Type | FALA | FAWB | FAGM | FAMM | FAPP | FAKN |
|---|---|---|---|---|---|---|
| Indoor Dome | 2 | 2 | 1 | 3 | 2 | 1 |
| Outdoor Dome | 0 | 1 | 1 | 0 | 0 | 1 |

[B] The CCTV camera placement shall allow for viewing of all entry/exit points that will be controlled by the access control system.

[C] All cameras must be installed in manner that they are not easily accessible or cannot be tempered with.

[D] All cameras provided shall be wired cameras.

[E] All cameras shall support PoE and TCP/IP.

[F] All cameras shall have a minimum resolution of 2 megapixels.

[G] All cameras shall have a minimum video resolution of 1080p at a minimum frame rate of 20fps.

[H] All cameras shall support at least one of the following video compression formats; H.264, H.264+, H.265 or H.265+.

[I] All outdoor cameras shall have an IP67 rating.

[J] All cameras shall have an IR range of at least 20m for low light conditions.

[K] All cameras shall be equipped with motion sensors. Recordings shall only be created when motion is detected.

[L] The cameras shall have a minimum Wide Dynamic Range (WDR) of 120dB to ensure that images are not affected by backlight.

## 3. OPERATOR POSITIONS

[A] Operator positions shall be supplied with the CCTV system.

[B] An operator position shall be connected to the Network Video Recorder (NVR) and shall allow the user to view all camera feeds as well as select specific feeds to monitor. The operator positions shall have a playback function for the playback of recorded footage. The operator positions shall be restricted from making any configuration changes to the CCTV system.

[C] There shall be one (1) operator position installed in the tower at each ATSU. This position shall also work as a monitor position depending on the type of user that has logged in. Further details are provided under CHAPTER 6:.

## 4. NETWORK VIDEO RECORDER

[A] A Network Video Recorder (NVR) shall be provided for the CCTV system.

[B] The NVR shall have sufficient storage to store recorded footage for at least 30 days.

[C] The NVR shall have a Solid-State Drive/s (SSD) to store the footage.

[D] The NVR shall be capable of simultaneously recording of all available channels (i.e., the 8 channel NVR shall be capable of recording all 8 channels simultaneously).

[E] The NVR shall have a user-friendly graphical user interface.

[F] The NVR shall cater for comprehensive search and playback functions, including but not limited to:

[a] Play
[b] Pause
[c] Rewind
[d] Fast forward
[e] Screenshot

[G] The NVR shall allow for viewing and playback via a remote Web management connection.

[H] The NVR shall support the use of PC software or a built-in web application via a network for live viewing, playback and configuration.

[I] The NVR shall be capable of exporting video footage to a USB drive in mpeg4, MKV or any format suitable to be played on a windows-based PC.

[J] The NVR shall allow for the user to select the date, time and duration of the video to be exported.

[K] The NVR shall output video at a minimum resolution of 1080p.

[L] The NVR shall have at least 2 High-Definition Media Interface (HDMI) outputs.

[M] All recordings must be date and time stamped.

[N] The NVR shall be password protected.

[O] The NVR shall come pre-installed and pre-configured with all the necessary software.

[P] The NVR shall support multi-level access control based on usernames and passwords. Users' authorisation shall be configured according to Table 4.

[Q] The NVR shall have at least 1 ethernet port for connection to the Local Area Network (LAN).

[R] The NVR shall support TCP/IP.

[S] The NVR shall support the PoE standards IEEE 802.3af and IEEE 802.3at. The NVR shall have enough PoE supported ports to connect all cameras or a suitable PoE switch/switches shall be provided to compensate for the cameras that cannot be connected directly to NVR.

# CHAPTER 4: INTRUDER ALARM SYSTEM

## 1. GENERAL

[A] An intruder alarm system shall be provided and installed at FAGM.

[B] The intruder alarm systems supplied shall have the capability of linking to an off-site armed response company.

[C] The intruder alarm shall comply with the following standards:

[a] SANS 60839-1-1:2007/IEC 60839-1-1:1988 Alarm systems Part 1: General requirements

[b] SANS 60839-1-3:2007/IEC 60839-1-3:1988 Environmental testing

[D] The intruder alarm system shall consist of the following components at a minimum:

[a] Alarm control panel and keypad

[b] Magnetic contacts

[c] Motion detectors

[E] The intruder alarm system shall be scalable and upgradable to cater for newer systems such as electric fencing, vibration sensors, Passive Infrared (PIR) Sensors as well as additional infrared beams and magnetic contacts.

## 2. ALARM CONTROL PANEL

[A] There shall be one (1) alarm control panel installed at eye-level in the tower cabin at FAGM.

[B] The keypad on the alarm control panel shall be backlit and remain illuminated in the event of power failure.

## 3. MAGNETIC CONTACTS

[A] Magnetic contacts shall be used to trigger the alarm if the perimeter door is opened when the alarm is in an armed state.

[B] There shall be one (1) magnetic contact installed at the main entrance of the tower cabin at FAGM.

## 4. MOTION DETECTORS

[A] There shall be two (2) PIR motion detectors installed in the tower cabin at FAGM.

# CHAPTER 5: INTERCOM SYSTEM

## 1. INTERCOM SPECIFICATIONS

[A] An intercom shall be installed at the FAWB, FAGM, FAMM, FAPP and FAKN ATSUs.

[B] The intercom shall consist of the following components, including but not limited to:

[a] Gate station

[b] Handset

[C] The intercom shall support 2-way voice communication.

[D] The gate station shall be installed at the main entrance.

[E] The gate station at FAGM and FAKN shall have an IP65 rating as they will be installed outdoor.

[F] The gate station shall consist of a speaker, microphone and a call button.

[G] The call button on the gate station shall have a proximity sensor so that it does not need any physical contact.

[H] The gate station shall be wall mounted.

[I] The handset shall be installed at the tower Air Traffic Controller's (ATC) position in an appropriate position determined by the operational staff and ATNS Human Factors department so that the equipment does not interfere/obstruct primary ATC functions.

[J] The handset shall have an unlock button, or similar functionality, that can be used to unlock the locking mechanism installed at the main entrance to grant visitor's access.

[K] The handset shall provide a visual and audio alert when someone presses the call button on the gate station. The audio alert volume shall be adjustable.

# CHAPTER 6: SYSTEM INTEGRATION

## 1. SYSTEM INTEGRATION

[A] Details of how the access control system and the CCTV system can be integrated shall be provided. The benefits and the added functionality of integrating the two systems shall be outlined.

[B] Details of an access control system with an integrated intercom shall be provided.

[C] There shall be one 20-inch All-in-one PC installed in the tower cabin at each location. The PC shall cater for the following functionality:

[a] CCTV operator position

[b] Management of the access control system and server

[c] Enrolment of new users

[d] Printing of employee cards

[D] The All-in-one PC shall have the following minimum specifications:

[a] Intel Core i7 or equivalent

[b] 4GB GDDR5 integrated Graphics card

[c] 16GB DDR4 RAM

[d] 1TB SSD

[e] USB Keyboard + Mouse

[f] Windows 10 Pro (Licence to be provided by ATNS)

[g] Built-in Ethernet Port

[E] All the systems shall be password protected, and each user shall have their own username and password to ensure accountability.

[F] All default passwords shall be changed once installation is complete.

[G] The placement of any equipment in the tower cabin, including the PC's and intercom handsets, shall be in consultation with the ATNS Human Factors department.

# CHAPTER 7: PROJECT MANAGEMENT SPECIFICATIONS

## 1. PROJECT MANAGEMENT REQUIREMENTS

### 1.1 Draft Plans

The PMP shall encompass draft plans that will be refined as necessary during the execution of the contract. These plans shall include:

[A] Project Management
[B] Resource management;
[C] Risk management;
[D] Quality management;
[E] Communication management;
[F] Installation, Transitioning and Commissioning; and
[G] Environmental Management Programme.

### 1.2 Project Management Plan

Should outline all project management plans;

[A] Project scope and overview;
[B] Project deliverables;
[C] Work Breakdown Structure (WBS) defining the scope of work and resources necessary to meet the contract requirements;
[D] Project organization and responsibilities;
[E] Master Time Schedule (Gantt Chart);
[F] Quality assurance activities to be performed in the project by the Contractor;
[G] Configuration and integration management activities (regarding hardware, software and documentation version changes); and
[H] Cost management.

### 1.3 Project Schedule

[A] The schedule shall include all project activities needed to be undertaken for the successful completion of the project scope of works. It shall also include a Work Breakdown Structure (WBS) illustrating the breakdown of the project scope into activities that can be managed, monitored and measured in terms of duration, cost and resources.

### 1.4 Resource Management

[A] The contractor shall employ a qualified and experienced project team with clearly defined roles and responsibilities for carrying out the project tasks.

### 1.5 Risk Management

[A] The risk management plan shall outline how project-related risks will be identified, assessed and mitigated. The plan shall further articulate the assessment methodology to be used in quantifying risk ratings attached to each identified risk.

### 1.6 Quality Management

[B] The quality management plan for the project detailing how quality will be controlled, assured and maintained throughout the lifecycle of the project. It shall also include quality assurance policy and procedures and relevant accreditations held by the company.

### 1.7 Installation, Transitioning and Commissioning

[A] The plan shall detail how the installation, transitioning and commissioning to meet project's technical, operational, contractual and performance requirements. This plan shall include an Acceptance Matrix, which identifies all deliverables, and the methods of testing proposed to demonstrate compliance.

### 1.8 Environmental Management Programme

[A] The Environmental Management Programme (EMPr) based on identified activities which may have potential or actual environmental impacts before the commencement of work in accordance with the National Environmental Management Act (No. 107 of 1998) and associated environmental legislation as well as ATNS' environmental specifications. The environmental management programme shall address, without limitations, the following:

a. Energy efficiency pertaining to all aspects of the project;
b. The use of Environmentally sustainable materials and products; and
c. Waste management.

## 2. SYSTEMS ENGINEERING

[A] The system engineering plan shall be in accordance with IEEE STD 1220-2005 Annex B, where applicable, for the design, manufacture, integration, and testing of the overall system. The system definition shall show detail on at least the following, where applicable:

a. System concept;

b. Identified risks;

c. Initial project and technical plans;

d. Risk management;

e. Every single identified subsystem;

f. Every single identified interface;

g. Every single potential service provider;

h. Complete system and product specifications including software specifications;

i. Complete interface specifications;

j. Complete interface specifications with service providers;

k. Human/system interfaces;

l. Support issues if any;

m. Identified training issues if any;

n. Human resources issues if any;

o. Data flows with and within the system;

p. Identified baselines and proposals for the management thereof;

q. Proposed operational, technical and system reviews; and

r. Configuration management.

# CHAPTER 8: LOGISTIC SUPPORT REQUIREMENTS

## 1. TRAINING

[A] The Contractor shall provide training for each user type for the number people stipulated in the table below.

| User Type | FALA | FAWB | FAGM | FAMM | FAPP | FAKN |
|---|---|---|---|---|---|---|
| Super User | 2 | 2 | 2 | 2 | 2 | 2 |
| Administrator | 2 | 2 | 2 | 2 | 2 | 2 |
| General Users | 4 | 4 | 4 | 4 | 4 | 4 |

## 2. WARRANTY

[A] The warranty period for the equipment provided shall be at least 12 months.

## 3. SPARES

[A] The Bidder shall specify and include any recommended spares that should be kept by ATNS in their proposal.

## 4. SUPPORT CONTRACT

[A] The Bidder shall include a maintenance and support proposal for the duration of the specified life of the systems. The Bidder shall include any interventions that may be required to achieve the stipulated 10-year life span.

[B] The Contractor shall respond within 24 hours (Tmax) for  any system failures.

[C] Should the Contractor not meet the proposed response time, the penalty shall be imposed. Service penalties will be determined by the Actual response time (Tact) per incident and calculated as per the formula below: -
Service penalty = (Tact)(hours)/ (Tmax)(hours) * (Priority factor* )*(10%* next contract invoice value), up to a total maximum of the value of the Agreement per Agreement period where: Tmax (hours) = corresponding maximum agreed time to respond (arrive at the site).
Note: The penalty only applies to where the response time was exceeded. Priority factors for all types of failures is one (1).