



Provision of Armed Response, Alarm Monitoring, Data Communication and Maintenance services at all SABS sites nationwide for a period of 24 months , including the continuous monitoring of, and response to, activations from the installed visual verification intruder detection system.

1. PURPOSE

The South African Bureau of Standards (SABS) is inviting suitably qualified, PSIRA registered and experienced security service provider to provide Armed Response Service, 24-Hour Alarm Monitoring, Data Communication for Visual Verification Intrusion Detection System, Visual Verification Monitoring and panic/duress services to all applicable SABS sites nationwide for a period of thirty-six (36) months (three years).

The appointed service provider shall monitor and respond to alarm activations from the existing visual verification intruder detection system, as well as integrated roaming panic devices for patrolling Security Officers and static panic buttons installed at designated guardhouses/security posts.

2.SCOPE OF WORK

The appointed service provider shall provide, install where applicable, integrate, activate, monitor, maintain and support the following services:

2.1 Armed Response

The service provider shall provide a 24-hour, 365-day armed response service to all SABS sites (Groenkloof, Olifantsfontein, Secunda, Durban, Richards bay, Cape Town, Saldanha Bay and East London).

The service shall include:

- Deployment of appropriately trained, licensed and equipped armed response personnel.
- Immediate response to verified suspected intrusion and security alarm activations.
- Response to panic/duress, intrusion, tamper and other emergency signals.
- Securing and assessing the affected area upon arrival.
- Liaise with SABS Security Services, SAPS and emergency services where required.
- Completion of an incident/response report following significant activations.

2.2 Alarm Monitoring

The service provider shall operate a 24-hour central monitoring facility capable of receiving, processing and responding to alarm signals from all connected SABS sites.

The service shall include:

- Continuous monitoring of alarm systems.
 - Receipt and classification of alarm activations.
 - Verification of activations where visual verification is available.
 - Immediate escalation of confirmed or suspicious activations.
 - Dispatch of armed response in accordance with the agreed SLA.
 - Recording of all activations, dispatches, responses and outcomes.
 - Escalation of repeated or unresolved activations to designated SABS representatives.
-

2.3 Visual Verification Intruder Detection System

The service provider shall continuously monitor the installed visual verification intruder detection system at designated the following SABS sites: Pretoria, Olifantsfontein, Secunda, Richards Bay, Durban, Cape Town and East London.

The service shall include:

- Remote verification using pop up images, video or other visual information afterhours.
- Identification of the affected site, zone or activated area.
- Assessment of whether an activation represents a genuine or suspected security threat.
- Immediate dispatch of armed response upon detecting intrusion.
- Escalation to SABS Security Services and SAPS where appropriate.
- Electronic recording of activation, verification, dispatch and response information.

2.4 Roaming Panic Devices for Patrolling Security Officers

The service provider shall provide and integrate roaming/mobile panic devices for designated security officers conducting patrols.

The devices shall:

- Be portable or wearable and suitable for use during routine patrols.
- Allow discreet activation during an emergency, assault, threat or security incident.
- Transmit an immediate panic/duress signal to the central monitoring centre.
- Identify the relevant SABS site and device/location.
- Support location identification/tracking where technically feasible.
- Integrable to the central monitoring system.
- Generate a priority emergency alarm upon activation.
- Be regularly tested and maintained.

2.5 Static Panic Buttons at Guardhouses and Security Posts

The service provider shall provide, install, integrate and activate fixed panic buttons at designated guardhouses, security control points and other strategic locations identified by SABS.

Static panic devices shall:

- Be securely installed and readily accessible for activation by security personnel.
- Transmit an immediate panic signal to the services provider's monitoring centre.
- Clearly identify the SABS site and specific panic point/location.
- Initiate the required escalation and armed response procedure.
- Be protected against accidental or unauthorised activation where appropriate.
- Be tested regularly to confirm end-to-end functionality.

2.6 Data Communication Services

The service provider shall provide reliable and secure data communication services between SABS sites and the service provider's monitoring centre.

The service shall include:

- Provision of suitable communication links for alarm and panic signals.
- Transmission of visual verification information where applicable.
- Monitoring of communication link availability.
- Immediate identification and escalation of communication failures.
- Provision of backup communication paths where required.
- Maintenance and repair of communication equipment and links.
- Restoration of failed services within agreed SLA timeframes.

2.7 Installation, Integration and Commissioning

The service provider shall be responsible for all necessary:

- Site assessments.
- Technical surveys.
- Equipment supply.
- Installation.
- Configuration.
- Programming.
- Integration.
- Testing.
- Commissioning.
- Training.
- Documentation.

All alarm, visual verification and panic systems shall be fully integrated into the central monitoring platform.

The system shall not be considered commissioned until successful end-to-end testing has been completed and accepted by SABS Security Services.

2.8 Maintenance and Technical Support

Throughout the contract period, the service provider shall:

- Provide preventative and corrective maintenance.
- Maintain all supplied equipment and communication infrastructure.
- Attend to reported faults within agreed response times.
- Replace defective equipment where required.
- Monitor system health and communication status.
- Maintain complete maintenance and fault records.
- Provide technical support on a 24-hour basis for critical security system failures.

System Maintenance Schedules			
Corrective Maintenance	Costs per item	Preventative Maintenance	Costs
Replacement of VV batteries		Bi-annually	
Signal Booster			
Replacement of Panic Buttons			
Visual Verifier Unit (VV)			
VV Camera			
Passives			

Switch			
Port Expander			
IOE Board			
Door Contacts			
Keypad			

NB: If bidder does not submit quotation on official company letterhead, they will be disqualified.

3. TECHNICAL REQUIREMENTS

3.1 Central Monitoring Centre

The service provider shall have a continuously operational monitoring centre capable of:

- Monitoring all connected SABS alarm systems.
- Receiving visual verification signals.
- Receiving and processing static and roaming panic activations.
- Dispatching armed response personnel.
- Maintaining communication with response units.
- Recording all alarm and response events.
- Providing appropriate backup monitoring and business continuity arrangements.

3.2 Panic System Integration

- All roaming and static panic devices shall be integrated into the same central monitoring platform where technically feasible.
- Each activation shall provide, as a minimum:
- Date and time of activation → SABS site → device/location → type of activation → monitoring-centre action → armed response dispatch → arrival time → action taken → incident close-out.
- The service provider shall ensure that panic activations cannot be missed or treated as ordinary routine alarm events.

3.3 Mandatory Physical Verification of Monitoring Control Room and System Demonstration

A mandatory physical inspection shall be conducted at the preferred/winning bidder's monitoring control room before final appointment and/or contract award.

The preferred/winning bidder shall provide SABS with unrestricted reasonable access to the relevant operational areas required for verification and demonstration.

- The purpose of the visit shall be to verify, as a minimum:
- The physical existence and operational status of the bidder's monitoring/control room.
- The monitoring infrastructure, workstations and alarm management platform.
- Availability of appropriately staffed monitoring personnel on a 24-hour basis.
- Backup power and business continuity arrangements.
- Communication infrastructure and redundancy.
- Alarm receiving and processing capabilities.
- Visual verification monitoring capabilities.
- Panic alarm monitoring and escalation capabilities.

- Armed response dispatch and communication procedures.
- Incident logging, recording and reporting capabilities.
- Technical support and fault escalation arrangements.

The preferred/winning bidder shall be required to conduct a live technical demonstration to SABS representatives showing its ability to:

1. Receive an alarm signal from the existing client 's alarm system.
2. Receive and display a visual verification activation from the existing client 's alarm system.
3. Receive and identify a roaming panic activation.
4. Receive and identify a static panic activation from a guardhouse/security post.
5. Demonstrate the monitoring operator's verification and escalation process.
6. Demonstrate dispatch of the armed response unit.
7. Demonstrate event logging and retrieval of activation records.
8. Demonstrate the identification and reporting of communication failures.
9. Demonstrate the operation of backup communication and power arrangements, where applicable.

The bidder shall demonstrate its ability to integrate with the current SABS-installed visual verification intruder detection, alarm and panic systems and shall provide evidence that the proposed monitoring platform is technically compatible with the existing infrastructure.

SABS reserves the right to conduct additional technical verification at selected SABS sites to confirm the bidder's ability to integrate, activate and commission the proposed solution with the existing systems.

Failure by the preferred/winning bidder to satisfactorily demonstrate the required control room infrastructure, monitoring capability and integration with the existing SABS security systems may result in the bidder being deemed technically non-compliant and subject to further procurement evaluation in accordance with the applicable SABS procurement process.

3.3 Priority Response

Panic/duress activations shall be treated as high-priority emergency signals.

The monitoring centre shall immediately:

1. Receive the activation.
2. Identify the SABS site and device/location.
3. Initiate the approved verification/escalation procedure.
4. Dispatch armed response in accordance with the SLA.
5. Notify designated SABS personnel where required.
6. Contact SAPS/emergency services where the circumstances warrant.
7. Record the complete response process.

3.4 System Availability

The service provider shall maintain continuous service availability through appropriate:

- Backup power.
 - Redundant monitoring infrastructure.
-

- Backup communication channels.
- Network resilience.
- Disaster recovery arrangements.
- Business continuity procedures.

3.5 Communication Security

All alarm, panic and visual verification communication shall be transmitted through reliable and appropriately secured communication channels.

The service provider shall monitor communication links and promptly report failures that may compromise security monitoring.

3.6 Armed Response Resources

The service provider shall maintain sufficient armed response resources to service all SABS sites covered by the contract.

Response personnel shall be appropriately trained, authorised, licensed and equipped, and response vehicles shall be maintained in an operational and roadworthy condition.

3.7 Testing Requirements

The service provider shall conduct regular end-to-end testing of:

- Alarm signals.
- Visual verification activations.
- Roaming panic devices.
- Static guardhouse panic buttons.
- Communication links.
- Backup communication channels.
- Monitoring-centre receipt and processing.
- Armed response dispatch procedures.

Testing shall be coordinated with SABS Security Services to avoid unnecessary operational disruption, and all results shall be documented.

3.8 Monthly Reporting

The service provider shall submit a monthly performance report containing the following, as a minimum:

Report Item	Required Information
Alarm activations	Site, date, time, zone and outcome
Visual verification	Activations, verification results and response
Panic activations	Site, device, officer/location and response
Armed response	Dispatch and arrival times
False alarms	Frequency, causes and corrective actions
Communication faults	Outages, duration and resolution
Equipment faults	Fault, action taken and status

Maintenance	Preventative/corrective work completed
SLA performance	Response and resolution compliance
Incidents	Summary and recommendations
Outstanding actions	Responsible party and target completion date

4. COMPLIANCE REQUIREMENTS

- Valid Company & Director(s) PSIRA Certificates.
- Valid Company Armed Response Certificate.
- Valid PSIRA Letter of good standing
- Submission of minimum Three (3) contactable reference letters where the supplier is providing monitoring of virtual verifier intruder detection systems.
- Submission of minimum of Seven (7) valid Armed Response Vehicle Licences operating in SABS regions (Groenkloof, Olifantsfontein (NETFA), Secunda, Richards bay, Durban, Cape Town, and East London).
- Submission of minimum of Seven (7) valid 9mm firearms Licences.
- Emergency response plan demonstrating timelines to reach each of the above SABS 'site upon receiving alarm notification.
- Valid public liability insurance of minimum of R3 000 000.00
- Valid COIDA letter of good standing from department of labour only.
- Maintenance plan for virtual verifier intruder detection system
- Comprehensive CV(s) of technician(s) with qualifications and minimum of Five (5) years' experience of servicing Virtual Verifier Intruder Detection Systems.

5. TECHNICAL CAPABILITIES

The winning bidder should upon request demonstrate to SABS representatives the following in order to advance to the next level:

- 24-hour 365 Preattentional SAIDSA Compliance Control Room
- Handheld Two-way Radios
- Base Radio
- Virtual Verifier monitoring and receiving system
- Panic button receiving system
- Telecommunication (Telephone / Cell phone)

6. MINIMUM SERVICE LEVEL REQUIREMENTS

The service provider shall comply with the following minimum requirements:

Service	Minimum Requirement
Monitoring	24 hours / 365 days
Armed response	24 hours / 365 days
Visual verification monitoring	Continuous
Roaming panic monitoring	Continuous
Static panic monitoring	Continuous

Communication monitoring	Continuous
Alarm processing	Real-time
Panic activation	24 hours / 365 days
Armed response time	In accordance with site-specific SLA
Critical system fault response	In accordance with SLA
Fault restoration	In accordance with SLA
Testing	Weekly and documented
Monthly reporting	Mandatory

7. SERVICE PROVIDER RESPONSIBILITY

The appointed service provider shall be responsible for ensuring that the complete solution remains operational, integrated, monitored and supported for the full thirty-six (36) month contract period.

Any failure affecting the transmission of alarm, visual verification or panic signals shall be treated as a security-system deficiency and shall be immediately escalated to SABS Security Services, together with the corrective action and expected restoration time.

The service provider shall not deactivate, disconnect, relocate or materially alter any monitoring, alarm or panic device without prior approval from SABS Security Services, except where immediate action is required to protect life or prevent damage, in which case SABS shall be notified immediately.

8. KEY OBJECTIVE

The overall solution shall provide SABS with a single, integrated and reliable security monitoring and response capability covering:

Alarm Detection + Visual Verification + Roaming Guard Panic + Static Guardhouse Panic + Data Communication + Central Monitoring + Armed Response + Incident Reporting.