

**BY-LAW NO. 1**  
**SOUTH AFRICAN INTRUDER DETECTION SERVICES ASSOCIATION**  
**Requirements for a SAIDSA Approved Central Station**

**VERSION 1.6 - August 2023**

**PREAMBLE**

The construction of the Central Station is intended to prevent or delay unauthorized entry and to enable the occupants to raise an alarm in the event of an attack. These are categorized as follows, the requirements of each being dealt with under separate headings:-

1. Construction
2. Permitted Openings
3. Normal Entrance
4. Doors
5. Emergency Exits
6. Glazed Areas
7. Ablution Facilities
8. Ventilation Inlets and Outlets
9. Alarm Protection to the Central Station
10. Closed Circuit Television
11. Entry to Central Station
12. Communication Methods
13. Power Supply
14. Central Station Antenna
15. Relay Sites and Repeater Stations
16. Signals Received from Alarms Protected Premises
17. Records
18. Action Required
19. Supervisory Checks
20. Procedure Manual
21. Maintenance
22. Central Station Equipment
23. All Monitoring Receivers

**1. CONSTRUCTION**

**All parts of the fabric of the Central Station shall be of substantial construction. Substantial construction is taken to mean:**

**1. CONSTRUCTION**

**1.1 WALLS**

- 1.1.1 **Exterior Walls:** Must consist of at least 230mm of cement mortar brick work or 150mm reinforced concrete.
- 1.1.2 **Interior Walls:** can make use of other approved intrusion resistant materials such as but not limited to...Steel plating no less than 3.2mm in thickness or ballistic wall panels consisting of multi layered laminates (Fiberglass, Kevlar or materials of equivalent application and strength) which can be mounted on or between drywalling fixtures in accordance with manufacturers specifications and local building regulations. These materials must adhere to the US Ballistics specifications standard UL752 with a rating no lower than level 3. Certifications from the

manufacturer to be made available to SAIDSA on Inspection. Panels must be installed with no gaps.

## **1.2 ROOF/CEILING/FLOORS**

- 1.2.1 **Roof/Ceiling:** Will consist of suitably reinforced concrete at least 120mm thick, or steel to the equivalent strength.
- 1.2.2 **Floors:** in multi story constructions shall comply with the same specification referred to in 1.2.1
- 1.2.3 Where metal ceilings or floors are installed, the thickness of the sheet must be a minimum of 3mm. Sheets must be bolted or welded together. A Structural and Safety report must be provided to SAIDSA.
- 1.2.4 Ballistic panels \ alternate materials: consisting of multi layered laminates (Fiberglass, Kevlar or materials of equivalent application and strength) which can be mounted above existing fixed ceiling or attached directly to ceiling panels in accordance with manufacturers specifications and local building regulations. These materials must adhere to the US Ballistics specifications standard UL752 with a rating no lower than level 3. Certifications from the manufacturer to be made available to SAIDSA on Inspection. Panels must be installed with no gaps and a Structural and Safety report must be provided to SAIDSA.

## **2. PERMITTED OPENINGS**

- 2.1 Permitted openings only are allowed as specified herein.
  - 2.1.1 Normal entrance
  - 2.1.2 Emergency exits
  - 2.1.3 Glazed areas
  - 2.1.4 Ventilation inlets and outlets
  - 2.1.5 Service inlets and outlets

## **3. NORMAL ENTRANCE**

- 3.1 A normal entrance shall comprise of at least two interlocked doors separated by a lobby.
- 3.2 Two or more doors cannot be opened simultaneously.
- 3.3 All doors leading into the lobby must also be access controlled and make use of a Multi Interlock system.
- 3.4 The lobby shall be of the same construction as the Central Station.

## **4. DOORS**

- 4.1 The doors together with their hinges, frames and locking devices shall be of substantial construction.
  - 4.2.1 Where timber doors are used, both doors shall be at least 44mm thick, and of solid-core construction faced with mild steel metal sheets on both sides. Combined the total sheet thickness should be no less than 3.2mm.
  - 4.2.2 Alternate materials and ballistic panels consisting of multi layered laminates (Fiberglass, Kevlar or materials of equivalent application and strength) can also be used within the substantially constructed door in accordance with manufacturer's specifications. These materials must adhere to the US Ballistics specifications standard UL752 with a rating no lower than level 3.
- 4.3 On outward opening doors, bullet hinges or an equivalent of substantial construction must be used. The solution shall support the weight of the door. The door must not be removable whilst in a closed position.
- 4.4 All other hinges shall be internal and of substantial construction.
- 4.5 The locks securing the doors must have a minimum sudden impact resistance of 1000KG. The locking mechanism should be protected from tampering and show resistance to vibration. All locks must be installed to manufacturer's specifications.

#### **4.6 Glass Interlock Doors**

- 4.6.1 Framework surround must match the equivalent minimum strength of 2mm Mild steel plate. Construction should be substantial and durable.
- 4.6.2 All glass sections shall consist of no less than 15mm three-ply laminated glass in sections not exceeding 1.5 Square Metres.  
Where glazed areas are larger than 1.5 square metres, they shall offer resistance to forced entry at least equivalent to that of European Standard EN1063 BR3-S (SANS1263-3 - 38mm). The member must be able to provide a certificate from a supplier confirming the standard of the glazed area installed.
- 4.6.3 Where Central Station operators are in direct view from outside the Central Station, one way vision laminate must be used on the exposed glass sections of the Glass Interlock Doors.
- 4.6.4 Roof of Interlocked Man Trap unit must be constructed of mild steel plate no less than 3mm thick or suitable equivalent, all relevant certifications of prebuilt units must be made available to SAIDSA on Inspection.
- 4.6.5 ALL Frames and Hinging required to be of substantial construction.

#### **5. EMERGENCY EXITS**

- 5.1 Emergency Exits shall comply with the requirements above, however, a single door is acceptable and no lobby is required.
- 5.2 The Emergency Exit door shall be easily opened from the inside. This shall comply with local fire regulations.
- 5.3 The Door must be alarmed on a 24 hour non-shutable zone and must be monitored by a SAIDSA approved Central Station.
- 5.4 Where a timber door is used, the door shall be at least 44mm thick, and of solid-core construction faced with mild steel metal sheets on both sides. Combined the total sheet thickness should be no less than 3mm.
- 5.5 The exit door shall offer resistance to forced entry from the outside.

#### **6. GLAZED AREAS**

- 6.1 Any glazed areas shall offer resistance to forced entry at least equivalent to that of three-ply laminated glass of 15mm thick, in sheets not larger in area than 1,5 square metres. Where glazed areas are larger than 1.5 square metres, they shall offer resistance to forced entry at least equivalent to that of European Standard EN1063 BR3-S (SANS1263-3 - 38mm) for internal glazed areas, and BR4-S (SANS1263-3 -52mm) for external glazed areas. The member must be able to provide a certificate from a supplier confirming the standard of the glazed area installed.
- 6.2 Frames and fixings must be of substantial construction and offer similar levels of protection as described in 6.1.
- 6.3 No opening sections are permitted in the external glazed areas.
- 6.4 Where external glazed areas are reachable from ground level, suitable Flatex or a minimum of 20mm diamond mesh of metal construction must be fitted.
- 6.5 It shall be ensured that the interior/staff of the Central Station are not within direct line of sight from the outside.

#### **7. ABLUTION FACILITIES**

- 7.1 Where only one Central Station operator is present, toilets and wash basins must be situated inside the Central Station. Where more than one operator is present, toilets and wash basins may be situated outside the Central Station but in close proximity. Exit may only be through the lobby doors.

#### **8. VENTILATION AND INLETS/OUTLETS**

- 8.1 The cross sectional area of the inlets and outlets shall not exceed 0,02 square metres.
- 8.3 Ventilation inlets and outlets shall be suitably protected against physical attack and not accessible from ground level.
- 8.5 Adequate ventilation to be supplied to cycle and replace the air within the Central Station

every 30 minutes.

- 8.6 Suitable air-conditioning compliant with building regulations to be provided in the Central Station.

## **9. ALARM PROTECTION TO THE CENTRAL STATION**

- 9.1 Wired/wireless emergency buttons shall be installed and easily accessed within the Central Station.
- 9.2 Signaling from the above emergency buttons will be directly to the Central Station of another SAIDSA approved Central Station. Such signaling must be tested weekly and records kept.

## **10. VIDEO SURVEILLANCE (CCTV)**

- 10.1 All permitted openings to the Central Station shall be suitably monitored by vandal resistant closed circuit television cameras.
- 10.2 Recording of the cameras as per 10.1 above shall be provided with a searchable time/date stamped history of at least 48 hours.

## **11. ENTRY TO CENTRAL STATION**

- 11.1 Where 4 or more operators are utilized in the Central Station, access control should be provided which includes a time event log.
- 11.2 Entry to the Central Station other than by authorized personnel shall require positive identification by the Central Station operators.
- 11.3 Staff entry to the central station should be via biometric, facial recognition, tag, card system or access granted by Central Station operators upon positive verification.

## **12. COMMUNICATION METHODS**

- 12.1 Where land lines or other alternate communication services are used, there should be a minimum of two voice communication lines.
- 12.2 Wire based or fiber communication lines to the Central station should be underground or securely concealed and physically protected from tampering.
- 12.3 Backup voice communication should be in place, utilizing an alternate technology.
- 12.4 Cellular router communications with fixed desktop handsets are permitted when linked to voice recording system.
- 12.5 In all communications with the police, emergency services and response companies, a reference number shall be obtained and recorded.
- 12.6 All communication records to be kept for a minimum of twelve (12) months whilst compliance with the POPIA act must be maintained.

## **13. POWER SUPPLY**

- 13.1 The electricity supply may be either from external mains or from a battery standby.
- 13.2 In the event of a disruption of the external electricity supply, the stand-by power supply shall automatically be brought into use without interruption.
- 13.3 The stand-by supply including inverters and batteries must be located within the Central Station or an adjacent secure room. The solutions must be capable of sustaining the monitoring equipment for a period of at least 24 hours or not less than 50 minutes if a standby generator is installed.
- 13.4 The standby generator shall have an independent means of starting without leaving the Central Station vulnerable.
- 13.5 The standby generator must be housed in a secured protected area.
- 13.5 The amp hour capacity of the standby power supply shall be calculated on the basis of the average hourly current drain multiplied by the factor 1.5.
- 13.6 Any recharging facility of the standby power supply shall be sufficient to provide the maximum load requirements and to simultaneously recharge the battery from that discharged state to the required capacity within 24 hours.
- 13.7 In the event of an interruption in the mains power supply, all equipment essential to the operation of the Central Station shall continue to operate without loss of security or degradation of performance.

#### **14. CENTRAL STATION ANTENNA**

##### **(including any antenna receiving/transmitting RF signals)**

- 14.1 The antenna must be situated within close proximity to the Central Station. Where this is not possible, the antenna and any connecting cables should be suitably protected against any mechanical damage or unauthorized interference.
- 14.2 Where the antenna is not situated within close proximity to Central Station, the antenna shall be protected by suitable electronic intruder detection devices to detect tampering.

#### **15. RELAY SITES AND REPEATER STATIONS**

- 15.1 Auto hour tests from repeater or routing equipment shall be monitored to ensure the efficient working order of all relay sites, repeater stations and receivers and all records of such tests shall be recorded by the Central Station monitoring software.

#### **16. SIGNALS RECEIVED FROM ALARM PROTECTED PREMISES**

- 16.1 Receipt of an alarm signal from an alarm installation shall give suitable visual notification to Central Station operators on receipt with a hard copy printout option available should it be requested.
- 16.2 The use of 2G/3G technology is not recommended, but if used client should be informed of imminent sunset of this technology with risk/cost involved.
  - 16.2.1 Dual communication path is compulsory on all systems. If not accepted by the customer, this must be noted on the certificate as non-compliant.
  - 16.2.2 On low risk installations the dual communication may be in a single device – ie: sim card and fibre, provided that the router back up battery is the same as the alarm system.
  - 16.2.3 On high risk and commercial installations two separate communication devices must be used.
  - 16.2.4 The following methods are considered acceptable. One or more of the following:

Dual monitoring using different technologies or carrier mediums is recommended.

VHF/ UHF Radio  
GSM 4G Communication  
TCP/IP  
Spread Spectrum

- 16.3 In the event that a Radio transmitter and antenna is used, they must be correctly installed according to manufacturer's specifications. The DC power cable from the Radio transmitter to the control panel must have a minimum core diameter of 0.5mm (Cabtyre or Ripcord).
- 16.4 Minimum signals i.e. burglary and panic must be monitored separately.
- 16.5 Where required, all communication equipment shall be ICASA approved.
- 16.6 It is recommended that where possible, GSM/IP communication is not used as a single communication medium or as a primary means of communication.
- 16.7 No pre-paid SIM cards will be permitted.
- 16.8 In the event that a GSM transmitter is used, the customer must be clearly informed that they are being monitored by GSM technology as well as any risks associated with the connection of this equipment to the cellular network.
- 16.9 Communication cable shall not form part of main wiring harness and shall be run in such a manner as to protect them from tampering or physical damage. Cables to the communications devices must be wired below the ceiling.

## 17. RECORDS

The following records should be kept in the Central Station:

- 17.1 Electronic backups of alarm signals received.
- 17.2 Record of alarm calls received giving details of action taken and response.
- 17.3 Primary monitoring system must be electronic database technology based.
- 17.4 All back-up systems must be PC based
- 17.5 Back-up records may not be older than 24 hours.
- 17.6 Electronic backup equipment must be electronically isolated and updated weekly.
- 17.7 All reported incidents shall be available for a period of 36 months.

## 18. ACTION REQUIRED

- 18.1 The following action shall be taken by the Central Station on receipt of a signal from an intruder detection system and/or emergency call from the customer.
- 18.2 Signals/calls received are grouped into the following main categories. Each category should receive the minimum action below but not limited thereto:

Life threatening : eg. duress, confirmed incidents in progress  
Emergency signals : eg. panic signals  
Intruder signals : eg. alarm/burglary, visual verification.  
Status signals : eg. power, arm/disarm, communication/detector loss or tamper  
Maintenance signals : eg. alarm system battery condition, RF jamming

	<b>Life Threatening</b>	<b>Emergency</b>	<b>Intruder</b>	<b>Status</b>	<b>Maintenance</b>
<b>Phone and Verify</b>	No	Yes	Yes	No	No
<b>Dispatch Police / Armed Reaction (if contractually required)</b>	Yes	Yes, if requested or not canceled	Yes, if requested or not canceled	No	No
<b>Notify customer (text or app)</b>	No	No	No	No	No
<b>Log / record</b>	Yes	Yes	Yes	Yes	Yes

- 18.3 On dispatching armed reaction to a premises/customer, as much information as possible must be relayed to the reaction officer with regards to the exact location, means of access if any, where the activation has arisen from, what type of signal was received and any possible threat reported.

## **19. SUPERVISORY CHECKS**

- 19.1 When the Central Station is manned by one operator, provision shall be made for physical or electronic supervisory checks on the operator at intervals not exceeding 30 minutes.
- 19.2 Failure of the operator to respond to the checks shall result in an alarm being transmitted.

## **20. PROCEDURE MANUAL**

There shall be a Central Station procedure manual. Compliance with this manual should be checked at regular intervals.

## **21. MAINTENANCE**

An effective preventative maintenance program shall be instituted covering the Central Station receivers, power supplies, backup equipment, relay sites and repeater stations. Tests must be carried out once a week and documented.

## **22. CENTRAL STATION EQUIPMENT**

- 22.1 All primary communication equipment must be situated within the Central Station.
- 22.2 Backup equipment is to be readily accessible in the company's premises.
- 22.3 The backup equipment must be alarmed and protected if situated outside the Central Station.
- 22.4 Backup equipment shall be directly interchangeable and all reasonable precautions shall be taken to ensure that normal uninterrupted Central Station service is provided in the event of essential equipment being faulty or damaged.
- 22.5 Backup equipment shall be dedicated to the Alarm Central Station and shall remain unplugged until required.

## **23. AII MONITORING RECEIVERS**

- 23.1 The receiver shall include a 256-event buffer on the control module.
- 23.2 The receiver shall include a line, channel, network data connection or general error\fault monitor.
- 23.3 Surge suppressors and filters will be provided and used for the AC mains and communication data line connections.

*All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage or retrieval system, without permission in writing from the publishers. Every effort has been made to ensure accuracy of information at the time of going to print. However, the authors and publishers cannot be held responsible for errors or omissions for any reason whatsoever.*

*Copyright - South African Intruder Detection Services Association (SAIDSA) –  
All rights reserved 1994-2023*