

SOUTH AFRICAN INTRUDER DETECTION SERVICES ASSOCIATION
BY-LAW NO. 1
Requirements for a SAIDSA Approved Central Station
Revised 2017 Version 1.2

PREAMBLE

The construction of the Central station is intended to prevent or delay unauthorised entry and to enable the occupants to raise an alarm in the event of an attack. These are categorised 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. Ventilation Inlets and Outlets
8. Alarm Protection to the Central Station
9. Closed Circuit Television
10. Personnel Entry to Central Station
11. Telephone Lines
12. Power Supply
13. Central Station Antenna
14. Relay Sites and Repeater Stations
15. Signals Received from Alarms Protected Premises
16. Records
17. Action Required
18. Supervisory Checks
19. Procedure Manual
20. Maintenance
21. Central Station Equipment
22. Digital Telephone Monitoring Receiver

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:** At least 230mm of cement mortar brick work or 150mm reinforce concrete.
- 1.2 **Roof/Ceiling:** Suitably reinforced concrete at least 120mm thick, or steel to the equivalent strength.
- 1.3 Where metal ceilings 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.

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 at least two interlocked doors separated by a lobby.
- 3.2 Both doors cannot be opened simultaneously.
- 3.3 The area between interlocked doors may not have other openings unless into another control room of the same construction. (3-way interlock)
- 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 Where timber doors are used, both doors shall be at least 44mm thick, and of solid-core construction faced with a minimum 1,5mm mild steel metal sheet on both sides.

- 4.3 On an outward opening door, Bullet hinges must be used. All other hinges shall be internal.
- 4.4 The locks securing the doors shall be of a high security type. All locks must be installed to manufacturer's specifications and must resist a sudden impact.
- 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.
The Door must be alarmed on a 24 hour non-shutable zone and must be monitored by a SAIDSA approved Central Station.
- 5.3 Where timber doors are used, both doors shall be at least 44mm thick, and of solid-core construction faced with a mild steel sheet of a minimum thickness of 1,5mm on both sides.
- 5.4 The doors must be tamper proof 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 (SANS 1263-3 – 38mm Thickness) for internal glazed areas, and BR4-S (SANS 1263-3 - 52mm Thickness) for external glazed areas. Where the glazed area is larger than 1.5 square metres, 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.
- 6.3 No opening sections are permitted in the glazed areas.
- 6.4 Where windows are line-of-sight, suitable Flatex or a minimum of 20mm diamond mesh of metal construction must be fitted.
- 7. ABLUTION FACILITIES**
- 7.1 Where only one control room operator is present, toilets and wash basins must be situated inside the control room. Where more than one operator is present, toilets and wash basins may be situated outside the control room 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.
- 8.2 It shall be ensured that the interior/staff of the Central Station are not within direct line of sight from the outside. Ventilation piping/ducting must be protected by means of suitably constructed right angle elbows/bends.
- 8.3 Ventilation inlets and outlets shall be suitably protected against physical attack.
- 8.4 The inlets must be situated within a protected area or alternatively, be inaccessible.
- 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 is to be provided in the Central Station.
- 9. ALARM PROTECTION TO THE CENTRAL STATION**
- 9.1 Deliberately activated devices (emergency switches) shall be strategically sited within the Central Station.
- 9.2 Signalling from the above deliberately activated devices will be directly to the Central Station of another SAIDSA approved Central Station. Such signalling must be tested weekly.
- 10. CLOSED CIRCUIT TELEVISION**
- 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 9.1 above shall be provided at a minimum of 6 frames per second per camera with a history of at least 24 hours with time/date stamp.
- 11. ENTRY TO CENTRAL STATION**
- 11.1 Where 4 or more operators are utilised 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 authorised personnel shall require positive identification by the Central Station operators.
- 12. TELEPHONE LINES**
- 12.1 Where Telkom or other service provider regulations and techniques permit there should be a minimum of two exchange telephone lines for voice communication.
- 12.2 These telephone lines shall be routed separately from the building, underground or

- concealed.
- 12.3 One telephone line shall be barred from incoming calls.
- 12.4 Cellular communications are acceptable, but must be a fixture.
- 12.5 In all communications with the police and response companies, a reference number shall be obtained and recorded.
- 12.6 All records to be kept for a minimum of twelve (12) months

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 shall include batteries located within the Central Station, capable of sustaining the monitoring equipment for a period of not less than 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 control room vulnerable.
- 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 sited within close proximity to the Central Station. Where this is impracticable, then the aerial and any connecting cables should be suitably protected against any mechanical damage or unauthorised interference.
- 14.2 The antenna shall be protected by suitable electronic intruder detection devices to detect tampering.

15 RELAY SITES AND REPEATER STATIONS

- 15.1 Where the service provider permits, a comprehensive signal test shall be carried out every hour to ensure the efficient working order of all relay sites, repeater stations and receivers and all records of such tests shall be maintained.

16 SIGNALS RECEIVED FROM ALARM PROTECTED PREMISES

- 16.1 Receipt of an alarm signal from an alarm installation shall give a visible and audible warning with a hard copy printout available.
- 16.2 Where GSM or IP protocols are utilised, a backup receiver/decoder must be used. It is recommended that a second form of signal routing into the central station is used.

17 RECORDS

The following records should be kept in the Central Station

- 17.1 Hard copy printout, electronic or disc storage 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 computer based.
- 17.4 Back-up system may be PC based or manual card system.
- 17.5 Back-up records may not be older than 24 hours.
- 17.6 Electronic on-line back up equipment must be optically and electronically isolated. It can however remain unplugged and remain this way unless a back-up is being performed.
- 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 valid signal from an alarm system.
- 18.2 Signals received are grouped into three main categories. Namely; Life Threatening, Intruder Signals and Status/Maintenance signals. Each category should receive the minimum action as per the table below but not limited thereto.

	Life Threatening	Intruder	Status
Phone and Verify	No	Yes	No
Dispatch Police and/or Armed Response	Yes	Yes	No
Record	Yes	Yes	Yes

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 programme shall be instituted covering the Central Station receivers, power supplies, stand-by 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 Stand-by equipment is to be readily accessible in the company's premises.
- 22.3 The Stand-by equipment must be alarmed and protected if situated outside the Central Station.
- 22.4 Stand-by 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 Stand-by equipment shall be dedicated to the Alarm Central Station and shall remain unplugged until required.

23 DIGITAL TELEPHONE MONITORING RECEIVER

- 23.1 The receiver shall include a 256-event buffer on the control module.
- 23.2 The receiver shall include a line fault monitor for each line.
- 23.3 Surge suppressers and filters will be provided for the AC mains and the telephone lines.

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 1994-2018*