

## BY-LAW NO. 5

### Standard Installation Specification for Intruder Alarm Systems for Domestic, Commercial, Retail and Industrial Installations

Amended September 2011

#### 1. GENERAL

- 1.1 This specification lays down the minimum requirements for the construction, installation, operation and maintenance of intruder alarm systems in buildings. Specifications herein contain requirements to be applied in the aforesaid. Any deviation is to be indicated on the installation certificate and such deviation should not be seen as an acceptance of compliance.
- 1.2 SAIDSA does not accept any liability and/or responsibility for any defect there may be now or hereafter in the installation or any loss suffered by any party, due to its failure to operate at any time and no warranty or condition expressed or implied whether statutory or otherwise is given by SAIDSA in regard to the above installation either to the approved installer or to the customer.
- 1.3 This specification does not purport to cover all the necessary requirements for a particular installation and all efforts should be made to ensure correct risk assessment.
- 1.4 The client must be clearly informed that the installed equipment does not prevent intrusion but is intended to detect or deter intrusion.
- 1.5 This entire By-law must be read in conjunction with the appropriate annexures.
- 1.6 All equipment must be installed to manufacturer's specifications.

#### 2. DEFINITIONS

- 2.1 For the purposes of this specification the following definitions apply:
  - 2.1.1 **24-Hour Zone:** A zone that is permanently armed (Panic button, tamper switch).
  - 2.1.2 **Alarm condition:** A condition whereby the alarm system, when armed, activates indicating a violation of any detection device.
  - 2.1.3 **Alarm company:** A SAIDSA-approved installation organisation prepared to enter into a contract for the provision of the installation and/or monitoring, reaction and maintenance of an intruder alarm system.
  - 2.1.4 **Arming:** Putting an intruder alarm system or part of it (switching on of the alarm) into such a condition that an alarm condition created by any of the associated detection devices in the alarmed area is signalled.
  - 2.1.5 **Back up battery:** Device responsible for ensuring power supply to the intruder alarm system in the event of a power failure.
  - 2.1.6 **Balanced circuit:** A closed circuit so arranged that severance or shorting-out of any protective switch, detection device or wiring of the intruder alarm system will cause a detectable change in the resistance of the circuit.
  - 2.1.7 **Central station/control room:** Continually manned premises, equipped to receive and display signals from intruder alarm systems which complies with the requirements of By-Law 1 of SAIDSA and is prepared to enter into a contract for the provision of alarm monitoring.
  - 2.1.8 **Closed circuit:** A circuit within an intruder alarm system which when opened creates an alarm condition.
  - 2.1.9 **Closed circuit device:** A device arranged to create an alarm condition by opening a closed circuit.
  - 2.1.10 **Control equipment:** Equipment including switches, relays, indicators and other apparatus necessary for arming, disarming and/or programming intruder alarm system for activating signalling equipment and for indication of faults.
  - 2.1.11 **Delay Zone:** A Detection Circuit which when the control equipment is armed will provide a time delay for the purposes of entry and exit arming or disarming.
  - 2.1.12 **Deliberately operated device** (e.g. (panic button, glass break call point): A device permitting the subscriber or his staff to deliberately create an alarm condition.
  - 2.1.13 **Detection circuit:** Circuit by means of which one or more detection devices or deliberately operated devices are connected to the control or signalling equipment of an intruder alarm system.
  - 2.1.14 **Detection device – electronic** (e.g. passive infrared, microwave, glass break detector)  
: Apparatus or section of wiring intended to detect the entry or attempted entry of an intruder.
  - 2.1.15 **Digital communicator:** Equipment for the transmission of electronic signals through the telephone system to the central station/control room to a receiving device, which acknowledges receipt of the signal.
  - 2.1.16 **Disarming:** Putting an intruder alarm system or part of it into such a condition that an alarm condition created by any of the alarm conditions in the disarmed area, will not be registered in the central station (switching off of alarm).
  - 2.1.17 **Double pole circuit:** A closed circuit so arranged that throughout its length there are two or more adjacent conductors in different electrical states and such that an alarm and/or fault condition is generated if the two conductors are connected together or if either closed circuit is opened.

- 2.1.18 **End of line resistance:** A closed circuit so arranged that at severance or shorting-out of any part of the wiring will cause a detectable change in the resistance of the circuit.
- 2.1.19 **External sounder:** Signalling equipment consisting of a sound-producing device.
- 2.1.20 **Fullower zone:** A Detection Circuit which when the control equipment is armed and subsequently violated, prior to a Delay Zone being violated, results in an instant alarm. Should a delay zone be triggered first, this zone will be treated as a delay zone.
- 2.1.21 **Instant Zone:** A Detection Circuit which when the control equipment is armed and subsequently violated, results in an instant alarm.
- 2.1.22 **Internal sounder:** Signalling equipment consisting of a sound-producing device so situated within the protected premises.
- 2.1.23 **Intruder alarm system:** A means of detecting and signalling the presence, entry or attempted entry of an intruder into a protected premises. For the purposes of this By-law, it is specifically noted that the use of wireless/wirefree systems is permitted.
- 2.1.24 **Isolate (bypass):** A deliberate action whereby part (circuit) of the alarm system is disabled during a single alarm state and does not have the ability to signal an alarm condition.
- 2.1.25 **Multiplex circuit:** A multiple detection device circuit arranged in such a way that operation of a single detection device will signal the identity of that device to the control equipment. The multiplex cabling must be tamper protected.
- 2.1.26 **Multi-Shot:** A circuit capable of multiple Alarm Conditions during a single arming period. The number of alarm conditions is determined by the value of the swinger shutdown.
- 2.1.27 **Open circuit:** A circuit within an intruder alarm system which when closed creates an alarm condition.
- 2.1.28 **Open Circuit device:** A device arranged to create an alarm condition by closing an open circuit.
- 2.1.29 **Power supply equipment:** Equipment providing power for the retaining of the battery in a good state of charge and for the operation of any component part of an intruder detection system, either independently or through the control equipment.
- 2.1.30 **Protected premises:** That part of the premises under the control of one or more subscriber, to which protection is afforded by an intruder alarm system.
- 2.1.31 **Protective switch - mechanical** (e.g. magnetic switches, pressure mats): Apparatus or section of wiring intended to detect the entry or attempted entry of an intruder.
- 2.1.32 **Radio transceiver:** Bi-directional radio with acknowledgement capabilities.
- 2.1.33 **Radio transmitter:** Equipment for the transmission of signals from the protected premises to a central station/control room by radio waves.
- 2.1.34 **Risk area: (Protected area)** Offices, rooms and other areas within the Protected Premises, which either contain or give, access to disposable movable property.
- 2.1.35 **Signalling circuit:** Circuit within an intruder alarm system operated by the control equipment, which communicates a signal from the control equipment to the signalling equipment.
- 2.1.36 **Signalling equipment:** Equipment used to communication information to a Central Station e.g. communicator, radio, etc.
- 2.1.37 **Single pole circuit:** A circuit consisting of a conductor in the form of an electrical loop.
- 2.1.38 **Subscriber:** A person or organisation utilising the services of a SAIDSA-approved alarm company for the installation and maintenance of an intruder alarm system.
- 2.1.39 **Swinger shutdown:** whereby a zone or zones are automatically bypassed/shutdown by the system after a pre-programmed number of alarm conditions. (see Multi-Shot)
- 2.1.40 **Tamper:** Any unauthorised entry into component parts of the alarm system and detection devices.
- 2.1.41 **Trouble condition:** An abnormal condition in any part of an intruder alarm system, which must be eliminated to restore correct operation.
- 2.1.42 **Volumetric Detector:** A detector capable of sensing human movement in a volume such as a room.

### 3. CONSTRUCTION:

#### 3.1 Intruder alarm system

The intruder alarm system shall consist of detection circuits, various detection devices, control equipment, one or more signalling circuits, signalling equipment and the necessary power supply equipment.

#### 3.2 Precautions against tampering

- 3.2.1 The control panel housing cover and electronic detection devices e.g. PIR, glassbreak, etc, must be tamper protected on a 24 hour zone in retail, commercial, industrial and high risk domestic installations.
- 3.2.2 The communication devices, antenna, control panel and power supply must be in a protected area.
- 3.2.3 Wiring of electronic detectors may not use a common negative.
- 3.2.4 The detection devices and other parts of the alarm system shall be so mounted and located that the possibility of interference by mechanical or magnetic means is reduced to a minimum. Where the frame of a protected door, window or other entry exit point can be readily displaced, this displacement must create an alarm condition.

#### 3.3 Detection circuits

- 3.3.1 Every detection circuit forming part of the intruder alarm system shall be so arranged that failure of the power supply to the circuit displays a fault condition during arming.

### **3.4 Control equipment**

#### **3.4.1. Location and Enclosure**

Where ceiling access is possible, the control panel, radio and antenna shall be installed a minimum of 1,5m below the ceiling, or in an area that is not vulnerable to tampering from within the ceiling void. These devices must be protected by a volumetric detector on an instant zone and must not be visible from the outside of the premises. This will not apply in the stay mode.

#### **3.4.2 System Control Facilities**

3.4.2.1 Digital keypads are to be of the data transfer technology type.

3.4.2.2 The use of a mechanical keyswitch alone, is prohibited.

3.4.2.3 In the case of an intruder alarm system having a keypad as an integral part of the enclosure, this keypad may not be used as the primary control point. The keypad must be in a protected area and must not be vulnerable to tampering.

##### **3.4.2.4 Remote Arming**

All remote arming transmitters must be of the Encrypted Rolling code type.

In commercial installations, remote arming is only permissible if the code verification takes place within the control panel using a unique user/engineer identification.

3.4.2.5 The client must be clearly informed of any possible risks associated with the use of remote arming.

#### **3.4.3 Disarming**

When using a time delay on a zone protecting the keypad, such entry delay shall not exceed 30 seconds.

#### **3.4.4 Arming**

During the arming period procedure the status of all isolated circuits or faulted circuits shall be easily accessible.

##### **3.4.4.1 Circuit Identification**

Where more than one detection circuit is used, the control equipment shall be capable of indicating immediately the individual circuit in which the alarm condition occurred, on disarming the control panel.

##### **3.4.4.2 Bypass/Isolation**

Once armed, no bypassed zones shall be indicated on the keypad.

### **3.5 Power Supply Equipment**

3.5.4 The mains transformer must be a minimum of 40VA, fused, surge protected and should not be less than the control panel manufacturer's specification. Due consideration must be given to the current draw of all devices connected to the control panel. All transformers shall have internal PTC's and/or thermal fuses for protection against short circuits.

3.5.2 The control panel back-up battery must have a minimum capacity of 7.0aH and be of the sealed type or have a minimum standby time of six hours for any part of the system. The control panel must provide a low battery cut-off of a minimum of 10.2v. (Exclusive of wireless systems)

3.5.2 The battery charger shall be sufficient to recharge the battery to the required capacity within 24 hours.

3.5.3 The use of car batteries is not permitted.

3.5.4 A mains failure or low battery signal shall be transmitted to the central station.

3.5.5 The cable from the transformer to the control panel must have a minimum core diameter of 0.5mm (Cabletyre)

3.5.6 All power supply equipment shall be correctly earthed using an electrical earth.

### **3.7 Audible sounders**

3.7.1 The audible sounders shall be capable of sounding for a minimum period of three (3) minutes and must comply with the relevant Municipal Regulation.

3.7.2 All sounders must be audible unless agreed to in writing between the client and the installation company.

3.7.3 External sounders shall have their cables monitored for tamper by the control panel.

### **3.8 Signalling Equipment Systems**

#### **3.8.1 To Central Stations/Control rooms.**

The following methods are considered acceptable. Use can be made of one or more of the following. Dual monitoring is recommended:

- ◆ PSTN
- ◆ Radio

- ◆ GSM Communication
  - ◆ SWIFTNET
  - ◆ TCP/IP
  - ◆ Spread Spectrum
- 3.8.2 The radio transmitter and antenna must be correctly installed to manufacturers 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).
- 3.8.3 Minimum signals i.e. burglary and panic must be monitored separately.
- 3.8.4 Where required, all communication equipment shall be ICASA approved.
- 3.8.5 Where any communication mediums are vulnerable or unreliable, a second or alternate method of signalling must be used.
- 3.8.6 **GSM Requirements**
- 3.8.6.1 Where GSM transmitters are used, the GPRS should revert to another network or to SMS signals where signals are weak or high volumes of traffic exist on the network.
- 3.8.6.2 No pre-paid SIM cards will be permitted.
- 3.8.6.3 Only Private Networks (APNs) may be used.
- 3.8.6.4 GSM Clients should 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.
- 3.8.7 Commercial, Retail, Industrial and high risk domestic installations must have Dual monitoring.
- 3.8.8 **General Requirement**
- 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.

#### 4. INSTALLATION AND DETECTION DEVICES

##### 4.1 Detection circuit restriction

A detection circuit/zone must consist of only one of the following combination:

- ◆ Five (5) Magnetic contacts (Except in Zone doubling, then 1 magnetic contact only on each zone.)
- ◆ One (1) infrared beam or one pair of beams in parallel (dual beam units).
- ◆ Two (2) electronic detection devices. (Except in Zone doubling, then 1 electronic detector only on each zone.)
- ◆ Two (2) audio detection devices.
- ◆ Five (5) electronic shock sensors.
- ◆ Ten (10) anti-tamper detection devices.
- ◆ Five (5) sealed magnetic pull switches with an end-of-line resistor

#### 5. INSTALLATION AND EQUIPMENT

- 5.1 All LED's within detectors are to be disabled after installation set-up. **(Commercial only)**
- 5.2 Magnetic contacts may be installed at the hinge side of a window to permit partial opening when the alarm is armed in domestic applications.
- 5.3 Two stage magnetic contacts can be fitted to windows to allow for partial opening of the window when the alarm is armed, providing the gap does not exceed 75mm. Unless recessed reed switches are used, these contacts must be installed at the top of the window. These contacts are not to be placed on an entry/exit zone.
- 5.4 The use of car batteries, mechanical keyswitches, mechanical vibration switches and shuntlocks (cut out switches) is not permitted.
- 5.5 All detectors must be fixed using wall plugs and screws. The use of double sided tape or glue is not permitted.
- 5.6 Cables must run neatly in such a manner so as to avoid physical damage. All cables that are vulnerable to corrosion and damage as well as external wiring must be suitably protected or placed in conduit.
- 5.7 All joints must be soldered and insulated or in a junction box containing screw terminal blocks.
- 5.8 The use of a cigarette lighter or any other flame-producing device for the purpose of soldering, is not permitted.
- 5.9 Detector lenses must be suitably fixed in such a way as to prohibit their easy removal from the outside of the housing.
- 5.10 Cables within the control panel must be marked and terminated in an enclosure, using solder, crimping ferrules or strip connectors (chocolate blocks). Cables must be identified either by marking, labelling or colour coding.
- 5.11 All detection zones are to use single end-of-line or double end-of-line monitoring. End-of-line resistors are to be installed at the detector end of the line, i.e. within the detector.
- 5.12 Each zone shall be 24-hour tamper protected with the ability to report a tamper to the central station. **(Commercial only)**
- 5.13 All user codes must be programmable by the user including the master code and must be EPROM and not PROM based.

- 5.14 The event log must be an integral part of the control panel and must not be physically removable.
- 5.15 All equipment must be installed to manufacturers specifications.

**6. OPERATIONAL PROCEDURES**

When the system is installed, the subscriber shall receive a practical demonstration of the systems full functionality and shall be required to enter alarm user code. An operating instruction manual for the control panel must be available on request.

**7. RECORDS**

The Alarm Company shall maintain accurate records relating to each intruder alarm system installed.

**8. ALARM COMPANY REPRESENTATIVE IDENTIFICATION**

All representatives of the alarm company shall carry an identification card bearing the company name, PSIRA number, photograph and identity number.

**9. CERTIFICATE OF COMPLIANCE**

- 9.1 A SAIDSA certificate of compliance must be issued to the client when the intruder alarm system has been installed. The Installation Company must keep duplicate certificates for the duration of the contract.
- 9.2 All certificates and/or guarantees provided by the installer will be null and void if any third party, including the user, tampers, adds, removes or replaces any equipment in the installation. SAIDSA must be informed by the installer of any such occurrence.
- 9.3 Any non-compliance exceptions are to be clearly noted on the certificate.

**10. EQUIPMENT SPECIFICATIONS**

**10.1 Control Panels**

- 10.1.1 The control panel shall be microprocessor controlled, keypad operated.
- 10.1.2 Where permissible the system may be controlled via remote control as defined in 3.4.2.
- 10.1.3 The control panel must have a minimum 128 event log.
- 10.1.4 All zones must be multi-shot as defined in 2.1.26 and 2.9.39. The recommended minimum number of swingers is 3 (three). There is no prescribed maximum, but where used, the client must be informed of this function being enabled and any possible risks associated with the automatic shutdown of any affected zone(s).
- 10.1.5 The event log must not be erasable via downloading.

**10.2 Keypad**

- 10.2.1 The keypad shall have an internal sounder.
- 10.2.2 Keypads shall be of the data transfer type only.

**11. WIRELESS SYSTEMS.**

- 11.1 The wireless system shall operate on a South African ICASA approved frequency.
- 11.2 The wireless system shall include 24 hour monitoring of zone supervision, low battery and tamper from each detector.
- 11.3 Wireless detectors must include a battery saving feature.
- 11.4 The control panel must be in a protected area which is protected by a hard-wired PIR.
- 11.5 All wireless receivers/repeaters shall be installed within a protected area.

**12. INSTALLATION SPECIFICATION SCHEDULES**

**This entire By-law must be read in conjunction with the following Annexures.**

- i. Annexure A - Domestic Wireless Systems**
- ii. Annexure B - Domestic Wired Systems**
- iii. Annexure C - Commercial, Retail, Industrial and High Risk domestic Systems**

*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 1994-2011*