South African Intruder Detection Services Association

BY-LAW NO. 5

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

JANUARY 2020 – Version 1.3

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 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 **APP (smartphone application):** A **mobile app** (application software) is a computer program designed to run on smartphones, tablet computers and other devices. Apps can be used for the view or control of remote systems, including alarm or video security equipment. The APP should be sufficiently secure to prevent its misuse by third party. It is recommended that upon arming/disarming and bypass, the user ID is recorded in the control panel event log or server.

2.1.5 **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. This can be initiated via a keypad, keyfob, App or another suitable user interface.

2.1.6 **Back up battery:** Device responsible for ensuring a constant supply of backup power to the intruder alarm system in the event of a power failure.

2.1.7 **Bi-directional (2 way) Wireless transmission:** Allows the control panel and remote devices to both transmit and receive wireless signals. This allows the panel to monitor and control the device and the device to monitor the panels status and wireless connection.

2.1.8 **Bypass (Isolate):** 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.

2.1.9 **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.

2.1.10 **Cloaking:** The deliberate covering of an intruder using infrared blocking materials with the intent of hiding the infrared emission of the human body.
Anti-cloaking: A specific detector used to detect the deliberate covering of an intruder with infrared blocking materials.

2.1.11 **Closed circuit:** A circuit within an intruder alarm system which when opened creates an alarm condition.

2.1.12 **Closed circuit device:** A device arranged to create an alarm condition by opening a closed circuit.

2.1.13 **Code hopping:** A rolling code (Also called a **hopping code**) used in keyless entry systems to prevent the capture and recording of the code for duplication purposes. Such systems are typical in alarms, garage door openers and keyless car entry systems.

2.1.14 **Control equipment (Unit/Hub):** 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.

2.1.15 **Control room Transmissions:** The transmission of alarm events from a control panel alarm device to a control room. This can be done through a number of cable or wireless transmission methods including RF, GSM, GPRS, IP, PSTN, DSSS.

2.1.65 **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.

2.1.17 **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.

2.1.18 **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.

2.1.19 **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.

2.1.20 **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).

2.1.21 **End of line resistance (EOL)**: 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.
Double End of Line Resistance (DEOL): A closed circuit so arranged and programmed that the control panel will register an alarm or tamper condition from a detection device when the system is armed or disarmed.

2.1.22 **External sounder:** Signalling equipment consisting of a sound-producing device.

2.1.23 **Follower 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.

2.1.24 **Hybrid system:** Intruder alarm System comprising of wireless as well as hardwired components.

2.1.25 **Instant Zone:** A Detection Circuit which when the control equipment is armed and subsequently violated, results in an instant alarm.

2.1.26 **Internal sounder:** Signalling equipment consisting of a sound-producing device so situated within the protected premises.

2.1.27 **Intruder alarm system:** A means of detecting and signalling the presence, entry or attempted entry of an intruder into a protected premise. For the purposes of this By-law, it is specifically noted that the use of wireless/wirefree systems is permitted.

2.1.28 **Jamming:** The transmission of radio signals with the purpose of interfering with the correct operation of wireless networks to disrupt information flow, including alarm, GSM, Radio and CCTV equipment in a security installation.

2.1.29 **Keypad**: A control device used for arming, disarming, programming and status reports

2.1.30 **Masking:** The deliberate or accidental covering or blocking of a detector where the detector is unable to detect infrared.
Anti-masking: A detector specifically designed to detect the covering or blocking of a detector.

2.1.31 **Multi-Shot:** A circuit capable of multiple Alarm Conditions during a single arming period.

2.1.32 **Open circuit:** A circuit within an intruder alarm system which when closed creates an alarm condition.

2.1.33 **Open Circuit device:** A device arranged to create an alarm condition by closing an open circuit.

2.1.34 **Partition:** A programmable feature within a control panel allowing a zone or group of zones to be operated independently from the rest of the system, each partition having its own keypad functions, access codes, account codes, and reporting functions and can be armed/disarmed independently.

2.1.35 **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.

2.1.36 **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.

2.1.37 **Radio transceiver:** Bi-directional radio with acknowledgement capabilities.

2.1.38 **Radio transmitter:** Equipment for the transmission of signals from the protected premises to a central station/control room by radio waves.

2.1.39 **Remote:** (also known as a keyfob). A wireless handheld transmitting device used for the purpose of remotely arming and disarming a control panel and other auxiliary functions.

2.1.40 **Risk area: (Protected area)** Offices, rooms and other areas within the Protected Premises, which either contain or give, access to disposable movable property.

2.1.39 **Signalling Equipment & devices:** Equipment used to communicate information to a Central Station e.g. communicator, radio, etc.

2.1.40 **Spread Spectrum:** In radio communication, spread-spectrum techniques are methods by which a signal generated is deliberately spread over a number of frequencies, resulting in a signal that provides more secure communications including increasing resistance to natural interference, noise and jamming.

2.1.41 **Subscriber:** A person or organisation utilising the services of a SAIDSA-approved alarm company for the installation and maintenance of an intruder alarm system.

2.1.42 **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)

2.1.43 **Tamper:** Any unauthorised entry into component parts of the alarm system and detection devices.

2.1.44 **Trouble condition:** An abnormal condition in any part of an intruder alarm system, which must be eliminated to restore correct operation.

2.1.45 **Visual Verification:** Visual Verification is the management by exception of an Intruder Alarm Activation at any site being monitored, providing a mean of visually verifying the intruder alarm activation.
The purpose of Visual Verification is to quickly discriminate a positive alarm that requires urgent attention from any other event that should not be considered as a positive alarm.
The purpose of Visual Verification is to provide a minimum level of visual information to verify an Intruder Alarm Activation and respond to it accordingly.

2.1.46 **Volumetric Detector:** A detector capable of sensing human movement in a volume such as a room.

2.1.47 **Web Interface:** A user interface which allow users to control and interact with their security installation through a web browser. This can be used for a remote control, system management, visual feedback, and many other functions.

2.1.48 **Wireless Transmissions:** The transmissions of alarm information from a transmitting device (i.e. detector, magnetic contact or transceiver to a receiving device or console within an approved ICASA RF band.

2.1.49 **Zone (Circuit):** See closed and open circuit.

3. CONSTRUCTION:

3.1 Intruder Detection system

The intruder detection system may consist of various detection devices, control equipment, signalling equipment and the necessary power backup equipment for detecting and verifying unwanted intrusion

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 residential 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 to reduce the possibility of interference by mechanical or magnetic means.

3.3 Detection circuits

3.3.1 Every detection circuit forming part of the intruder detection system shall be monitored for fault, trouble, status conditions and display 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.
In the case of an intruder alarm system having a keypad as an integral part of the enclosure, it may not be part of the entry/exit area. In the armed state, a person must not be able to gain access to the control panel within the entry delay period. The control panel and battery must not be in an entry/exit delay zone. It is recommended that remote arming or a second keypad be used.

3.4.2.4 **Remote Arming**

All remote arming devices and/or software applications must be encrypted.
In commercial installations, remote arming is only permissible if the code verification takes place within the control panel using a unique user 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.

4. EQUIPMENT SPECIFICATIONS

4.1 Control Panels

4.1.1 The control panel shall be microprocessor controlled; keypad operated.
4.1.2 Where permissible the system may be controlled via remote control as defined in 3.4.2.4
4.1.3 The control panel must have the capability of storing the last 500 events.
4.1.4 The event log must not be erasable and/or via downloading

4.2 Keypad

4.2.1 The keypad shall have an internal sounder.
4.2.2 Keypads shall be of the data transfer type only.

4.3 Power Supply Equipment

4.3.1 The mains transformer must be in accordance with the electrical and manufacturers specifications and as per the design of the system and charging capacity.
4.3.2 It is recommended that all transformers are fused and surge protected.
4.3.3 The control panel must provide a low battery cut-off of a minimum of 10.2v. (Exclusive of wireless systems)
4.3.4 The use of liquid electrolyte lead acid type or car batteries is not permitted.
4.3.5 It is recommended that a mains failure or low battery signal is transmitted to the central station.
4.3.6 The cable from the transformer to the control panel must have a minimum core diameter of 0.5mm (Cabtyre)
4.3.7 The transformer shall be correctly earthed according to the manufacturer's instructions using an electrical earth.

4.4 Audible sounders

4.4.1 The audible sounders shall be capable of sounding for a minimum period of three (3) minutes and must comply with the relevant Municipal Regulation.
4.4.2 All sounders must be audible unless agreed to in writing between the client and the installation company.
4.4.3 External sounders shall have their cables monitored for tamper by the control panel.

4.5 Signalling Equipment Systems

4.5.1 **To Central Stations/Control rooms.**

The following methods are considered acceptable. Use can be made of one or more of the following. Dual monitoring using different technologies or carrier mediums is recommended.

- PSTN
- Radio
- GSM Communication
- TCP/IP
- Spread Spectrum

4.5.2 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).
4.5.3 Minimum signals i.e. burglary and panic must be monitored separately.
4.5.4 Where required, all communication equipment shall be ICASA approved.
4.5.5 Where any communication mediums are vulnerable or unreliable, a second or alternate method of signalling must be used.
4.5.6 It is recommended that where possible, GSM/GPRS communication is not used as a single communication medium or as a primary means of communication.

4.6 GSM Requirements

4.6.1 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.
4.6.2 No pre-paid SIM cards will be permitted.

4.6.3 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.

4.6.4 Commercial, Retail, Industrial and high-risk residential installations must have Dual monitoring, using different carrier mediums.

4.7 General Requirement

4.7.1 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.

5. INSTALLATION AND DETECTION DEVICES

5.1 Detection zone restrictions

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

- 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. (eg. Passive infrared detectors, PIR/MW detectors) (Except in Zone doubling, then 1 electronic detector only on each zone.)
- Two (2) audio detection devices. (eg. Glassbreak detectors)
- Five (5) electronic shock sensors.
- Ten (10) anti-tamper detection devices.
- Five (5) sealed magnetic pull switches with an end-of-line resistor

6. INSTALLATION AND EQUIPMENT

6.1 All LED's within detectors are to be disabled after installation set-up. (*Voluntary for residential, compulsory for Commercial installations.)*

6.2 All external doors must be protected by a magnetic, electromagnetic, electromechanical or wireless door contact.

6.3 Magnetic contacts may be installed at the hinge side of a window to permit partial opening when the alarm is armed in domestic applications.

6.4 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.

6.5 The use of car batteries, mechanical keyswitches, mechanical vibration switches and shuntlocks (cut out switches) is not permitted.

6.6 All detectors must be fixed using wall plugs and screws in mortar bricks, concrete, wood or dry walling. In the case of glass, aluminium, or treated surfaces, a secure attachment method must be used. The use of double-sided tape, cable glue or glue guns are not permitted. 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.

6.7 All joints must be soldered and insulated or in a junction box containing screw terminal blocks.

6.8 The use of a cigarette lighter or any other flame-producing device for the purpose of soldering, is not permitted.

Where Radio or GSM units are used, the power cables must be terminated at the battery via a radio battery connection pc board.

6.9 Detector lenses must be suitably fixed in such a way as to prohibit their easy removal from the outside of the housing.

6.10 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.

6.11 All detector zones must be supervised. Where single end-of-line or double end-of-line monitoring are used, the resistors must to be installed at the detector end of the line, i.e. within the detector.

6.12 Each zone shall be 24-hour tamper protected with the ability to report a tamper to the central station. **(Commercial only)**

6.13 The event log must be an integral part of the control panel and must not be physically removable.

6.14 All equipment must be installed to manufacturer's specifications.

7. FALSE ALARM MANAGEMENT

7.1 All zones must be multi-shot. It is recommended that the swinger shutdown is disabled or set to maximum in respect of each zone. Where the client requests a lower number of alarm conditions to be set in the swinger shutdown, this must be marked as an exception on the Certificate of Compliance.

7.2 It is recommended that outdoor detectors are set to a maximum of 5 alarm conditions on the swinger shutdown within a 24-hour cycle. However, this must be at the discretion of the client and in accordance with the contractual obligation.

7.3 It is not recommended that electric fences be connected to alarm system zones, but if done it should be optically isolated from the system or by means of a relay. Standard automation transmitters and receivers are not permitted.

8. WIRELESS SYSTEMS

8.1 Wireless Installation Considerations

8.1.1 When wireless connections are selected, careful consideration should be given to the influence of intentional or unintentional transmissions using the same frequency and/or means of signal modulation as those of the transmitting device. Such transmissions may result in receiver units generating tamper or fault conditions or prevent the interconnections from functioning correctly.

8.1.2 Consideration should be taken of electrical and or mechanical devices within close proximity to wireless devices.

8.2 Low Battery

When the transmitting device or detector has a low battery condition indicating battery close to end of life cycle and due for replacement, it is recommended that the devices lost from the system due to battery failure, low or dead should be visible, by zone, either at keypad and/or each device.

8.3 Environmental considerations

8.3.1 Wireless device tampers must raise immediate tamper events at the keypad and/or offsite monitoring. It is recommended that the device ID should be available with all reporting.

8.3.2 It is recommended that the signal strength should be tested at the point of installation.

8.3.3 it is the responsibility of the installer to assess these environmental factors and plan the installation appropriately. Where environments are not suitable for a reliable wireless installation, wired detectors should be used.

8.3.4 The client must be clearly informed that natural or manmade environmental changes could affect the operation of the system.

8.3.5 It is recommended that the installer tests the environment for interference by means of a frequency analyser.

8.4 Supervision

8.4.1 All wireless alarm systems installed must have the ability to report specific activations such as supervision, low battery, and tamper.

8.4.2 The system must have the ability to monitor and communicate RF jamming.

8.4.3 Outdoor detectors must have front and mounting tampers for monitored supervision. **(Commercial and High Risk Residential installations)**

8.4.4 All devices must be bi-directional. **(Commercial and High Risk Residential installations)**

8.4.5 Detector & transceiver must have a common battery for reporting purposes.

8.5 Management of RF jamming

8.5.1 The receiving device used should continually monitor the area for any signals that could cause signals from enrolled detectors to be compromised.

8.5.2 It is recommended that the system sends RF jamming or any other signal such as low battery on detectors, more than once to the control room.

8.5.3 It is recommended that the system uses a second form of communication to send RF Jamming signals or any other signals such as low battery on detectors.

8.6 Hybrid system

8.6.1 It is recommended that at least 30% in Residential and at least 50% in commercial and Industrial to be hardwired, except where bi-directional systems are installed.

8.7 General

8.7.1 The wireless system shall operate on a South African ICASA approved frequency.

8.7.2 Wireless detectors must include a battery saving feature.

8.7.3 All wireless receivers/repeaters shall be installed within a protected area and protected by a hard-wired or two-way supervised wireless detector.

9. 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.

10. RECORDS

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

11. 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.

12. CERTIFICATE OF COMPLIANCE

12.1 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.

12.2 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.

12.3 Any non-compliance exceptions are to be clearly noted on the certificate.