



South African Intruder Detection
Services Association

BY-LAW NO. 25

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

VERSION 1.2 - MARCH 2004

1. GENERAL
2. DEFINITIONS
3. CONSTRUCTION
4. INSTALLATION AND DETECTION DEVICES
5. INSTALLATION AND EQUIPMENT SPECIFICATION
6. OPERATIONAL PROCEDURES
7. MAINTENANCE
8. RECORDS
9. ALARM COMPANY REPRESENTATIVE IDENTIFICATION
10. INSTALLATION CERTIFICATE
11. EQUIPMENT SPECIFICATIONS
12. INSTALLATION SPECIFICATION SCHEDULES



BY-LAW NO. 25

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

VERSION 1.2 - MARCH 2004

1. GENERAL

- 1.1 SAIDSA does not accept any liability and/or responsibility for any defect there may now or hereafter be in the installation and 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.
- 1.2 This specification lays down 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..
- 1.3 This specification does not purport to cover all the necessary requirements for a particular installation.

2. DEFINITIONS

2.1 *For the purposes of this specification the following definitions apply:*

- 2.1.1 **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.
- 2.1.2 **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.
- 2.1.3 **Risk area:** Offices, rooms and other areas within the Protected Premises, which either contain or give, access to disposable movable property.
- 2.1.4 **Subscriber:** A person or organisation utilising the services of a SAIDSA-approved alarm company for the installation and maintenance of an intruder alarm system.
- 2.1.5 **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.
- 2.1.6 **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.
- 2.1.7 **Alarm condition:** A condition whereby the alarm system, when armed, activates indicating a violation of any detection device.
- 2.1.8 **Tamper:** Any unauthorised entry into component parts of the alarm system,

detection devices or cabling.

- 2.1.9 **Trouble condition:** An abnormal condition in any part of an intruder alarm system, which must be eliminated to restore correct operation.
- 2.1.10 **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.
- 2.1.11 **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).
- 2.1.12 **Closed circuit:** A circuit within an intruder alarm system which when opened creates an alarm condition.
- 2.1.13 **Open circuit:** A circuit within an intruder alarm system which when closed creates an alarm condition.
- 2.1.14 **Closed circuit device:** A device arranged to create an alarm condition by opening a closed circuit.
- 2.1.15 **Open Circuit device:** A device arranged to create an alarm condition by closing an open circuit.
- 2.1.16 **A single pole circuit:** A circuit consisting of a conductor in the form of an electrical loop.
- 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 **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.
- 2.1.20 **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.
- 2.1.21 **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.
- 2.1.22 **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.
- 2.1.23 **Detection device - electronic** (passive, microwave, glass break detector): Apparatus or section of wiring intended to detect the entry or attempted entry of



an intruder.

- 2.1.24 **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.
- 2.1.25 **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.
- 2.1.26 a **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.
- 2.1.26 b **Back up battery:** Device responsible for ensuring power supply to the intruder alarm system in the event of a power failure.
- 2.1.27 **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.
- 2.1.28 **Signalling equipment:** Equipment used to communicate information to a Central Station e.g. communicator, radio, etc.
- 2.1.29 **Radio transmitter:** Equipment for the transmission of signals from the protected premises to a central station/control room by radio waves.
- 2.1.30 **Radio transceiver:** Bi-directional radio with acknowledgement capabilities.
- 2.1.31 **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.
- 2.1.32 **External sounder:** Signalling equipment consisting of a sound-producing device.
- 2.1.33 **Internal sounder:** Signalling equipment consisting of a sound-producing device so situated within the protected premises.
- 2.1.34 **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.
- 2.1.35 **Multi-Shot:** A circuit, which must be capable of multiple Alarm Conditions during any single arming.
- 2.1.36 **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.
- 2.1.37 **Instant Zone:** A Detection Circuit which when the control equipment is armed and subsequently violated, results in an instant alarm.
- 2.1.38 **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.

- 2.1.39 **24-Hour Zone:** A zone that is permanently armed (Panic button, tamper switch).
- 2.1.40 **Swinger shutdown:** whereby a zone or zones are automatically bypassed/ shutdown by the system after a pre-programmed number of alarm conditions.
- 2.1.41 **Volumetric Detector:** A detector capable of sensing human movement in a volume such as a room.
- 2.1.42 **Communication:** (Also known as signalling) The transmission of information to the central station as per 3.8.1
- 2.1.43 **Domestic Monitoring Requirements:** (See Installation Specification Schedules)
- 2.1.44 **Commercial, Industrial and Retail Monitoring Requirements:**
(See Installation Specification Schedules)
- 2.1.45 **SAIA Approved** - South African Insurance Association Approved

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 ENVIRONMENTAL PRECAUTIONS

Appropriate precautions, by enclosure or otherwise, shall be taken to ensure that as far as practical no part of an intruder alarm system is adversely affected by the environmental conditions to which it is likely to be exposed. Special precautions shall be taken where parts are likely to be exposed to damage by weather, dampness, corrosion, rodents, insects, heat, oil, adverse industrial atmosphere or by mechanical means.

3.3 PRECAUTIONS AGAINST TAMPERING

- 3.3.1 When the intruder alarm system is disarmed, tampering with the enclosure of the control equipment or the signalling equipment shall cause a visible and/or audible alarm condition to be activated immediately. When the intruder alarm system is armed any such tampering shall create an alarm condition. The Radio Transmitter, Antenna, Control panel and power supply must be in a protected area.
- 3.3.2 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.

3.4 DETECTION CIRCUITS

- 3.4.1 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.

3.5 CONTROL EQUIPMENT

3.5.1 Due consideration shall be given to the following:-

3.5.1.1 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, in an area protected by a volumetric detector on an instant zone not visible from the outside. This will not apply in the stay mode. The door of the control panel must be tamper-proofed on a 24-hour zone.

3.5.1.2 System Control Facilities

Digital keypads are to be of the data transfer technology type. Remote arming/ disarming is only permissible if the code verification takes place within the control panel using a unique user/engineer identification. The use of a mechanical keyswitch alone, is prohibited. 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 system control point.

3.5.1.3 Disarming

When using a time delay on a zone protecting the disarming device, such entry delay shall not exceed 30 seconds. Any exceptions must be reflected on the certificate.

3.5.1.4 Arming

During the arming period procedure all isolated circuits or faulted circuits shall be clearly indicated.

3.5.1.5 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.

3.5.1.6 Bypass/Isolation

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

3.6 POWER SUPPLY EQUIPMENT

3.6.1 The mains transformer must be a minimum of 30VA, 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.

3.6.2 The control panel back-up battery must be a sealed battery and its requirements must be determined based on the power required to operate the alarm system for a minimum period of six hours in the standby condition whilst the system operates to its full capability. The control panel must provide a low battery cut-off of a minimum of 10.2v.

3.6.3 The use of car batteries is not permitted.



- 3.6.4 The battery charger shall be sufficient to recharge the battery to the required capacity within 24 hours whilst supplying the normal load of the system.
- 3.6.5 The transformer shall conform to SABS standards.
- 3.6.6 All transformers shall have internal PTC's and/or thermal fuses for protection against short circuits.

3.7 **AUDIBLE SOUNDERS**

- 3.7.1 An internal sounder rated at least 100dBa at 1 metre or an external sounder rated at least 120dBa at 1 metre, must be installed except in the case of a Personal Attack/Emergency Alarm. Such sounders must be audible throughout the protected premises.
- 3.7.2 The audible sounders shall be capable of sounding for a minimum period of three (3) minutes and must comply with the relevant Municipal Regulation.
- 3.7.3 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:

- " Digital communicator
- " Radio
- " GSM Communication - Bi-directional data transfer
- " SWIFTNET
- " TCP/IP

3.8.2 **Location and Protection**

The signalling equipment shall be positioned within the protected area (Refer 3.5.1.1)

3.8.3 **Telephones**

Where telephone lines are vulnerable, a second or alternate method of signalling must be installed.

3.8.4 **Delay of audible alarm**

If a siren delay is used, such delay shall not exceed 30 seconds.

3.8.5 **General Requirement**

Signalling circuit cabling 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.

4. **INSTALLATION AND DETECTION DEVICES**

4.1 **Detection circuit restriction**

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



- " Five (5) electro-mechanical switching devices.
- " One (1) infrared beam or one pair of beams in parallel (dual beam units).
- " One (1) electronic detection device.
- " 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 SPECIFICATION

- 5.1 All detectors/devices must be installed to manufacturer's specification. 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 shuntlock (cut out switches) is not permitted.
- 5.5 All detectors must be fixed using wall plugs and/or screws. A minimum of two (2) screws shall be used. 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.
- 5.7 Where possible, terminations must be in accessible enclosures or detection devices only.
- 5.8 Where the use of multi-core cable is necessary, then cables 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.
- 5.9 Wiring of electronic detectors may not use a common negative cable.
- 5.10 All detection zones are to use end-of-line or double end-of-line monitoring. End-of-line resistors are to be installed within the last detector in the zone..
- 5.11 Each zone shall be 24-hour tamper protected with the ability to report a tamper to the central station. **(Commercial only)**
- 5.12 All user codes must be programmable by user including the master code and must be EPROM and not PROM based.
- 5.13 All zones must be multi-shot.
- 5.14 Magnetic reed switches must be the normally closed type, rhodium or gold-plated and hermetically sealed.
- 5.15 Mechanical Vibration switches are not permitted.
- 5.16 Additional security related devices connected to the intruder alarm system in addition to the requirements of Bylaw 25, shall not be governed by the requirements, provided that such additional devices do not adversely affect the correct operation of the intruder alarm system and installation as required by Bylaw 25.
- 5.17 The Installation Company shall sketch each area of the protected premises, detailing the position of each detector or device in relation to the doors and/or windows in that area at the date of installation or take-over. It is the responsibility of the contract holder to ensure that these records are kept confidential and may not be released without written consent from the client.

6. OPERATIONAL PROCEDURES

The installer shall issue an operating instruction manual for the panel to the client.



The subscriber shall receive a practical demonstration of the systems full functionality and shall be required to enter their own personal user code.

7. MAINTENANCE

- 7.1 A maintenance agreement must be entered into between the Installation/Service Company and the client. Service intervals shall be every twelve months.
- 7.2 ***This contractor shall be responsible for conducting the following during each maintenance service call:-***
 - 7.2.1 Inspect and test each detection device back to the control panel
 - 7.2.2 Inspect the inside of the alarm control panel and radio transmitter
 - 7.2.3 Measure the output of the transformer and charging circuit
 - 7.2.4 Inspect the antennae
 - 7.2.5 Inspect cables for visible damage
 - 7.2.6 Test all programmed signals from source to the central station/control room via radio transmitter and digital communicator where applicable
 - 7.2.7 Inspect the premises to confirm that the protection originally specified, is adequate.

8. RECORDS

- 8.1 The Alarm Company shall maintain accurate records relating to each intruder alarm system installed. These records shall include a sketch of the positioning of each piece of equipment as per 5.17.
- 8.2 It is recommended that the client be required to sign the sketch to confirm its accuracy.

9. ALARM COMPANY REPRESENTATIVE IDENTIFICATION

- 9.1 All representatives of the alarm company shall carry some positive means of identification such as an identification card bearing a photograph and identity number.
- 9.2 In addition, the employee shall be in possession of their SIRA identification card at all times.

10. INSTALLATION CERTIFICATE

- 10.1 An installation certificate must be issued when the intruder alarm system has been installed or in the event of a take-over or modification of the system as per 10.5
- 10.2 The Installation Company must keep duplicate certificates for the duration of the contract.
- 10.3 The issuing of certificates must be in accordance with SAIA Approved (Pty) Ltd). SAIDSA will be responsible for verifying that where exceptions are recorded, that these will be acceptable. In addition, these will be used to select random samples for inspection purposes.
- 10.4 Copies of the certificate shall be supplied to the client and the Installation Company.
- 10.5 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.
- 10.6 Only SAIDSA members who are approved for the installation of intruder alarm systems may be contracted to issue such certificates.



11. EQUIPMENT SPECIFICATIONS

11.1 Control Panels

- 11.1.1 The control panel shall be microprocessor controlled, keypad operated or where permissible controlled via remote control as defined in 3.5.1.2.
- 11.1.2 The control panel must be capable of accepting an audible listen-in device from the monitoring station. **(Commercial only)**

11.2 Keypad

- 11.2.1 The keypad shall have an internal sounder.
- 11.2.2 Keypads shall be of the data transfer type only.
- 11.3 Zones may not have a resistance tolerance greater than 30% of the lower and upper input threshold of the manufacturer's resistor value.

11.4 *Individual Zones shall have the following programming characteristics.*

- a. Bypass / no bypass.
- b. Supervision.
- c. Trouble reporting. **(Commercial only)**
- d. Restoral reporting. **(Commercial only)**
- e. If swinger shutdown is used, the control panel must have an auto swing reset function at least every 24-hours.

11.5 *The control panel shall be capable of reporting to the central station, the following diagnostic conditions:-*

- 11.5.1 Mains power failure/restoral
- 11.5.2 Keypad communication bus trouble
- 11.5.3 Low battery/restoral
- 11.5.4 Auxiliary supply trouble
- 11.5.5 Telephone line trouble
- 11.5.6 Communication failure
- 11.5.7 Wireless Supervisory zone trouble **(if applicable)**
- 11.5.8 Enclosure tamper
- 11.5.9 Wireless sensor low battery **(if applicable)**
- 11.5.10 Siren circuit trouble
- 11.5.11 Loss of clock time
- 11.5.12 Wireless RF blocking after 30 seconds. **(if applicable)**

- 11.6 Where a digital communicator is used, it must be ICASA approved.

11.7 *Where a digital communicator is used, it must be capable of sending the following signals to the central station*

- 11.7.1 Arm / Close with user ID. (Cell Phone number in the case of GSM operation)
- 11.7.2 Disarm / Open with user ID. (Cell Phone number in the case of GSM operation)
- 11.7.3 Alarm with zone identification.
- 11.7.4 Zone restoral
- 11.7.5 Partition numbers **(if applicable)**
- 11.7.6 Panic
- 11.7.7 Duress
- 11.7.8 Enclosure tamper
- 11.7.9 Zone tamper
- 11.7.10 Wrong code lockout.

- 11.7.11 Auto test
- 11.7.12 Main Fail
- 11.7.13 Mains Restore
- 11.7.14 Low battery
- 11.7.15 Low battery restore
- 11.7.16 Bypass with zone numbers
- 11.7.17 Siren Fault
- 11.7.18 Telephone line fault with Restoral
- 11.7.19 Wireless sensor supervision failure **(If applicable)**
- 11.7.20 Wireless sensor low battery **(If applicable)**
- 11.7.21 Wireless sensor tamper **(If applicable)**

11.8 **Control Room Functions**

- a. Auto test failure
- b. Zone restoral by exception
- c. Bypass with zone numbers and ID numbers
- d. Time scheduling for opening and closing

11.9 The test signal shall be programmable from 1 to 7 days or the equivalent in hours.

11.10 The control panel shall be capable of being programmed with different account codes, one for each partition when applicable.

11.11 The digital communicator shall be able to use a minimum of 2 phone numbers.

11.12 ***The digital communicator shall be capable of reporting at least one of the following formats:-***

11.12.1 Contact ID **(Commercial only)** or

11.12.2 SIA formats (any) **(Commercial only)**

11.13 The telephone communicator must operate with line seizure.

11.14 ***The minimum programmable outputs for connection to a long distance radio or any other form of communication shall be as follows:***

11.14.1 Domestic installations: 2 outputs.

11.14.2 Commercial installations: 4 outputs.

11.14.3 ***The programmable options for the outputs shall be the following.***

- a. Burglary
- b. 24 Hour alarm
- c. Fire
- d. Mains Failure/restoral
- e. Low Battery/restoral
- f. Duress
- g. Panic
- h. Auto Test
- i. Armed
- j. Disarmed
- k. Telephone line or GSM communications failure
- l. System trouble
- m. Tamper



11.15 **User Codes**

11.15.1 The control panel shall be capable of being programmed with different user codes.

11.15.2 User codes must be able to be reprogrammed using a user master code, separate from the installer code.

11.16 **Memory.**

11.16.1 The control panel shall have a minimum 128 event log.

11.16.2 All events shall be time and date referenced in the control panel.

11.16.3 The event log must be downloadable and capable of being read on-site.

11.16.4 The event log must use the control panel's internal clock to determine the event time and date stamp.

11.16.5 The event log must not be erasable via downloading. The Event Log must be an integral part of the control panel and must be permanently mounted.

11.17 **Wireless Systems**

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

11.17.2 The wireless system shall include 24 hour monitoring of zone supervision, low battery and tamper from each detector.

11.17.3 Wireless detectors must include a battery saving feature.

11.17.4 The control panel must be in a protected area which is protected by a wired PIR.

11.17.5 The wireless system shall contain at least one wired audible sounder.

11.17.6 All wireless receivers shall be installed within protected areas.

11.18 **Downloading.**

11.18.1 Downloading must require a security access CSID code different to the control panels operators or installer's code.

11.18.2 Each downloading operator shall access the downloading program with a unique user ID and password.

11.18.3 The downloading shall be capable of transferring individual or multiple programming locations to the control panel.

11.18.4 ***Downloading connections shall be capable of being made with any of the following options:-***

11.18.4.1 Direct auto answer after a programmable number of rings.

11.18.4.2 Call Back.

11.18.4.3 Direct link from P.C. to panel

11.18.5 ***The downloading operator shall have the following capabilities:-***

11.18.5.1 Arm.

11.18.5.2 Disarming may NOT be done by the central station except in specific circumstances where remote disarming is needed for controlled and verified access.

11.18.5.3 Isolate Zones

11.18.5.4 Turn off interior zones

11.18.5.5 Turn off entry delay

11.18.5.6 View system status

11.18.5.7 View alarm memory

11.18.5.8 View event Log

11.18.5.9 Clear alarm memory, but not event log

11.18.5.10 View trouble conditions



-
- 11.18.6 The downloading computer shall log all downloading activity with operator details. This information is to be stored in a file for future reference should this be so required.
- 11.18.7 Up/Down load must be security protected.

12. INSTALLATION SPECIFICATION SCHEDULES

Installations must be performed in accordance with the following Annexures:-

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

CATEGORY 1

Annexure A - Installation Specification Schedule - DOMESTIC WIRELESS SYSTEMS

~ Version 1.2 March 2004* ~

AREAS REQUIRING VOLUMETRIC DETECTION PROTECTION	PERIMETER PROTECTION REQUIRED	FIXED PANIC BUTTONS REQUIRED	SYSTEM OPERATION VIA	KEYPAD FUNCTIONS REQUIRED	REQUIRED AUDIBLE WARNING	MAXIMUM PERMISSIBLE SIREN DELAY	DETECTOR SPECIFICATION PERMISSIBLE
Main Bedroom, Passage Room containing Hi-Fi, VCR, DVD and TV. Subject to residence design. All other rooms containing valuable property	All perimeter doors to be protected	Main bedroom, passage. Within the vicinity of the entry/exit door	Remote arming and disarming or wired and/or Remote keypad (As per 3.5.1.2)	Arm, Disarm, Panic	Internal sounders rated at least 100 dba at 1 metre or external sounders rated at least 120 dba at 1 metre for a duration of not less than 3 minutes audible throughout the protected area, which must be tamper-proofed if not in a protected area	30 seconds	24 Hour tamper. Temperature compensated.
MONITORING AND REACTION	ALARMSIGNAL TRANSMISSION DELAY	MAXIMUM PERMISSIBLE ENTRY DELAY	MIN BATTERY BACKUP REQUIRED UNDER NORMAL CONDITIONS	DETECTOR BATTERY AND SYSTEM SUPERVISION REQUIREMENTS	GROUP 1 SIGNALS REQUIRED TO BE REPORTED TO THE CENTRAL STATION	LOG ONLY OF OPTIONAL SIGNALS REQUIRED	
Monitoring. (Dual monitoring Optional) Reaction where available	Not permitted	30 seconds	6 Hours	Detector Presence to be determined at least every 60 minutes. Detector low battery to be reported locally and to central station.	Panic and/or Duress. Alarm. Mains failure or Control panel low battery. Detector low battery.	Arm, disarm by user. Bypass by zone. System error. Troubled zones. Alarm by Zone.	

* To be read in conjunction with Bylaw 25

CATEGORY 2

Annexure A - Installation Specification Schedule - DOMESTIC WIRELESS SYSTEMS ~ Version 1.2 March 2004* ~

AREAS REQUIRING VOLUMETRIC DETECTION PROTECTION	PERIMETER PROTECTION REQUIRED	FIXED PANIC BUTTONS REQUIRED	SYSTEM OPERATION VIA	KEYPAD FUNCTIONS REQUIRED	REQUIRED AUDIBLE WARNING	MAXIMUM PERMISSIBLE SIREN DELAY	DETECTOR SPECIFICATION PERMISSIBLE
Main Bedroom, Passage, TV Room, Lounge. All other rooms containing valuable property. All defined risk areas.	All perimeter doors to be protected	Main bedroom, passage. Within the vicinity of the entry/exit door	Remote arming and disarming or wired and/or Remote keypad (As per 3.5.1.2)	Arm, Disarm, Panic	Internal sounders rated at least 100 dba at 1 metre or external sounders rated at least 120 dba at 1 metre for a duration of not less than 3 minutes audible throughout the protected area, which must be tamper-proofed if not in a protected area	30 seconds	24-Hour tamper. Temperature compensated.
MONITORING AND REACTION	ALARM SIGNAL TRANSMISSION DELAY	MAXIMUM PERMISSIBLE ENTRY DELAY	MIN BATTERY BACKUP REQUIRED UNDER NORMAL CONDITIONS	DETECTOR BATTERY AND SYSTEM SUPERVISION REQUIREMENTS	GROUP 1 SIGNALS REQUIRED TO BE REPORTED TO THE CENTRAL STATION	GROUP 1 SIGNALS REQUIRED TO BE REPORTED TO THE CENTRAL STATION	GROUP 2 SIGNALS.
DUAL MONITORING Reaction where available	Not permitted	30 seconds	6 Hours	Detector Presence to be determined at least every 60 minutes. Detector low battery to be reported locally and to central station.	Panic and/or Duress. Alarm. Mains failure or Control panel low battery. Detector low battery.		Arm, disarm by user. Bypass by zone. System error. Troubled zones. Supervision. Alarm by Zone. RF Jamming.

*** To be read in conjunction with Bylaw 25**

CATEGORY 1

Annexure B - Installation Specification Schedule - DOMESTIC WIRED SYSTEMS ~ Version 1.2 March 2004 * ~

AREAS REQUIRING VOLUMETRIC DETECTION PROTECTION	PERIMETER PROTECTION REQUIRED	FIXED PANIC BUTTONS REQUIRED	SYSTEM OPERATION VIA	KEYPAD FUNCTIONS REQUIRED	REQUIRED AUDIBLE WARNING	SYSTEM REQUIREMENTS	DETECTOR SPECIFICATION PERMISSIBLE
Main Bedroom, Passage, Room containing Hi-Fi, VCR, DVD and TV. Subject to residence design. e.g. open plan	All perimeter doors to be protected	Main bedroom, passage. Within the vicinity of the entry/exit door	Data Transfer keypad or Remote (As per 3.5.1.2)	Arm, Disarm, Duress/Panic	Internal sounders rated at least 100 dBa at 1 metre or external sounders rated at least 120 dBa at 1 metre for a duration of not less than 3 minutes audible throughout the protected area, which must be tamper-protected if not in a protected area	128 Event Log	24Hour tamper. EOL Resistor Temperature compensated.
MONITORING AND REACTION	ALARM SIGNAL TRANSMISSION DELAY	MAXIMUM PERMISSIBLE ENTRY DELAY	MIN BATTERY BACKUP REQUIRED UNDER NORMAL CONDITIONS	MAXIMUM PERMISSIBLE SIREN DELAY	GROUP 1 SIGNALS REQUIRED TO BE REPORTED TO THE CENTRAL STATION	LOG ONLY OF OPTIONAL SIGNALS REQUIRED	
Monitoring. Reaction where available	Not permitted	30 seconds	6 Hours	30 Seconds	Panic and/or Duress. Alarm. Mains failure or low battery		Arm, disarm by user. Bypass by zone. System error. Troubled zones. Alarm by Zone.

*** To be read in conjunction with Bylaw 25**

CATEGORY 2

Annexure B - Installation Specification Schedule - DOMESTIC WIRED SYSTEMS ~ Version 1.2 March 2004* ~

AREAS REQUIRING VOLUMETRIC DETECTION PROTECTION	PERIMETER PROTECTION REQUIRED	FIXED PANIC BUTTONS REQUIRED	SYSTEM OPERATION VIA	KEYPAD FUNCTIONS REQUIRED	REQUIRED AUDIBLE WARNING	SYSTEM REQUIREMENTS	DETECTOR SPECIFICATION PERMISSIBLE
Main Bedroom, Passage, TV Room, Lounge. All defined risk areas	All perimeter doors to be protected	Main bedroom, passage. Within the vicinity of the entry/exit door	Data Transfer keypad or Remote (As per 3.5.1.2)	Arm, Disarm, Duress/Panic	Internal sounders rated at least 100 dBa at 1 metre or external sounders rated at least 120 dBa at 1 metre for a duration of not less than 3 minutes audible throughout the protected area, which must be tamper-proofed if not in a protected area	128 Event Log	24Hour tamper. EOL Resistor Temperature compensated.
MONITORING AND REACTION	ALARM SIGNAL TRANSMISSION DELAY	MAXIMUM PERMISSIBLE ENTRY DELAY	MIN BATTERY BACKUP REQUIRED UNDER NORMAL CONDITIONS	MAXIMUM PERMISSIBLE SIREN DELAY	GROUP 1 SIGNALS	GROUP 2 SIGNALS	
DUAL MONITORING Reaction where available	Not permitted	30 seconds	6 Hours	30 Seconds	Alarm. Panic and/or Duress. Arm, disarm. System error. Mains failure with restore. Battery low with restore. Radio Power-up (if applicable)	Panic and/or duress. Arm,disarm by user. Bypass by zone. System error by type. Alarm by zone. Tamper by zone. Mains failure with restore. Battery low with restore.	

* To be read in conjunction with Bylaw 25

Annexure C - Installation Specification for Commercial, Retail and Industrial Security ~ Version 1.2 March 2004* ~

PROTECTION REQUIRED	SYSTEM REQUIREMENTS	MONITORING AND REACTION	PANIC BUTTONS REQUIRED	SYSTEM OPERATION VIA	KEYPAD FUNCTIONS REQUIRED	REQUIRED AUDIBLE WARNING	DETECTOR SPECIFICATIONS	GROUP1 SIGNALS	MIN BATTERY BACKUP REQUIRED UNDER NORMAL CONDITIONS	GROUP2 SIGNALS
All defined risk areas must be protected. All perimeter doors to be protected. Any display window must be protected with either glass break detectors or curtain passive detectors.	128 Event log. Each user shall be allocated a separate user code	Dual monitoring Reaction where available	Keypad, Reception areas, Pay points. Encrypted Code Hopping on remotes	Data Transfer Keypad or remote as per 3.5.1.2	Arm/Disarm Duress/ Panic	Internal sounders rated at least 100 dBa at 1 metre or external sounders rated at least 120 dBa at 1 metre for a duration of not less than 3 minutes audible throughout the protected area, which must be tamper-proofed if not in a protected area	24Hour tamper. High RF immunity. EOL resistor. Temperature compensated. Anti masking on PIRS where required. 75% of manufacturers specification. Same for glass break detectors.	Alarm. Panic and/or Duress. Arm,disarm. System error. Mains failure with restore. Battery low with restore. Radio Power-up (if applicable)	6 Hours	Panic and/or duress. Arm,disarm by user. Bypass by zone. System error by type. Alarm by zone. Tamper by zone. Mains failure with restore. Battery low with restore.

*** To be read in conjunction with Bylaw 25**