

Australian/New Zealand Standard™

Intruder alarm systems

Part 1: Client's premises—Design, installation, commissioning and maintenance



AS/NZS 2201.1:2007

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee EL-031, Intruder Alarm Equipment and Installation. It was approved on behalf of the Council of Standards Australia on 6 December 2006 and on behalf of the Council of Standards New Zealand on 15 December 2006.
This Standard was published on 12 April 2007.

The following are represented on Committee EL-031:

Australian Industry Group
Australian Security Industry Association
Australian Security Intelligence Organization
Engineers Australia
Insurance Council of Australia
Insurance Council of New Zealand
NSW Police Service
National Security Association of Australia
New Zealand Security Association
Victoria Police
Victorian Security Institute

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 05500.

Australian/New Zealand Standard™

Intruder alarm systems

Part 1: Client's premises—Design, installation, commissioning and maintenance

Originated as AS 2201.1—1978.
Previous edition 1998.
Jointly revised and redesignated as AS/NZS 2201.1:2007.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 8160 8

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee EL-031, Intruder Alarm Equipment and Installations, to supersede AS 2201.1—1998.

The objective of this Standard is to assist insurers, alarm companies, equipment manufacturers, clients and the police in achieving a complete and accurate statement for an intruder alarm system required in particular premises.

This Standard is Part 1 of a series of Standards, the parts of which are as follows:

AS

2201 Intruder alarm systems

2201.1 Part 1: Client's premises—Design, installation, commissioning and maintenance (this part)

2201.2 Part 2: Monitoring centres

2201.3 Part 3: Detection devices for internal use

2201.5 Part 5: Alarm transmission systems

This Standard includes mandatory, optional and advisory specifications applicable to all parties concerned with intruder alarm systems.

Statements expressed in mandatory terms in notes to tables are deemed to be requirements of this Standard.

The term 'informative' has been used in this Standard to define the application of the appendix to which it applies. An 'informative' appendix is only for information and guidance.

CONTENTS

	<i>Page</i>
SECTION 1 SCOPE AND GENERAL	
1.1 SCOPE	5
1.2 APPLICATION	5
1.3 RISK ASSESSMENT	5
1.4 REFERENCED DOCUMENTS	5
1.5 DEFINITIONS	6
SECTION 2 SYSTEM INSTALLATION REQUIREMENTS	
2.1 GENERAL REQUIREMENTS	9
2.2 INSTALLATION	9
2.3 DETECTION DEVICES	10
2.4 AUDIBLE WARNING DEVICES	10
2.5 ENVIRONMENTAL CONDITIONS	10
2.6 WIRING	11
2.7 JOINTINGS.....	12
2.8 FLEXIBLE CONDUCTORS AND CONNECTIONS	13
2.9 TERMINATIONS	13
2.10 WIRE-FREE LINKS	14
2.11 COMMISSIONING.....	14
2.12 CLIENT TRAINING	14
SECTION 3 EQUIPMENT REQUIREMENTS	
3.1 GENERAL REQUIREMENTS	15
3.2 ADDITIONAL FUNCTIONALITY	15
3.3 ENVIRONMENTAL CONDITIONS	15
3.4 ELECTROMAGNETIC CONFORMANCE COMPATIBILITY (EMC).....	15
3.5 IMMUNITY	15
3.6 LOAD AND LINE CONDITIONS	15
3.7 ENCLOSURES.....	15
3.8 TERMINALS	15
3.9 MARKING OF CONTROL EQUIPMENT	16
3.10 INSTRUCTIONS	16
3.11 POWER SUPPLIES	16
3.12 POWER SUPPLY INDICATIONS.....	17
3.13 MARKING OF POWER SUPPLY EQUIPMENT.....	17
3.14 BATTERY REQUIREMENTS.....	18
3.15 WIRE-FREE SYSTEMS	19
3.16 EQUIPMENT CLASSIFICATION.....	21
SECTION 4 GENERAL OPERATIONAL PROCEDURES AND RESPONSIBILITIES	
4.1 GENERAL RESPONSIBILITIES	28
4.2 CLIENT'S RESPONSIBILITIES	28
SECTION 5 MAINTENANCE AND SERVICE	
5.1 SCOPE OF SECTION	29
5.2 MAINTENANCE	29

SECTION 6 RECORDS AND REPORTS

6.1	CLIENT AND EQUIPMENT RECORDS	31
6.2	MAINTENANCE RECORD	31
6.3	AUTHORITY FOR DISCONNECTING.....	32
6.4	LOGBOOK.....	32

APPENDICES

A	APPLICATION GUIDE	33
B	INDUSTRY TERMS	34
C	STANDARDS RELATING TO BATTERIES AND BATTERY CHARGERS	35
D	OCCUPANCY RATIO CALCULATIONS	37

STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Australian/New Zealand Standard Intruder alarm systems

Part 1: Client's premises—Design, installation, commissioning and maintenance

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

This Standard specifies the minimum requirements for the design, installation, commissioning, installation and maintenance of intruder alarm systems.

It classifies equipment and systems interconnected by wire and wire-free links. Such systems consist of detection devices, control equipment, warning and signalling devices, and the necessary power supply equipment.

This Standard does not cover the transmission of signals from the client's premises to a remote centre. It does not specify the extent or degree of protection to be provided, nor does it necessarily cover all the requirements for a particular installation.

NOTES:

- 1 See AS 2201.2 for monitoring centres.
- 2 AS 2201.5 for alarm transmission systems between client's premises and monitoring centres.

1.2 APPLICATION

This Standard shall apply to intruder alarm systems in private premises, commercial premises and special installations.

1.3 RISK ASSESSMENT

Prior to installation, a risk assessment shall be conducted and documented in conjunction with the client. The classification of the intruder alarm system installation shall be selected in accordance with Appendix A with agreement from the client.

1.4 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS

1102	Graphical symbols for electrotechnical documentation
2201	Intruder alarm systems
2201.2	Part 2: Monitoring centres
2201.3	Part 3: Detection devices for internal use
2201.5	Part 5: Alarm transmission systems
4251	Electromagnetic compatibility (EMC)—Generic emission Standard
4251.1	Part 1: Residential, commercial and light industry

AS/NZS	
1125	Conductors in insulated electric cables and flexible cords
1768(Int)	Lightning protection
2053	Conduit and fittings for electrical installations
2053.1	Part 1: General requirements
3000	Electrical installations (known as the Australian/New Zealand Wiring Rules)
3191	Electric flexible cords
4383	Preparation of documents used in electrotechnology (all parts)
5000	Electric cables—Polymeric insulated
5000.1	Part 1: For working voltages up to and including 0.6/1 (1.2) kV
HB	
13	Electrical equipment for hazardous areas
EN	
50130	Alarm systems
50130-4	Part 4: Electromagnetic compatibility—Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
55024	Information technology equipment. Immunity characteristics. Limits and methods of measurement
FIPS PUB	Federal Information Processing Standards Publication (USA)
46-2	Data Encryption Standard (DES)
ACIF S009	Installation requirements for customer cabling (Wiring Rules)

1.5 DEFINITIONS

For the purpose of this Standard, the definitions below apply.

NOTE: See Appendix B for additional terms commonly used in industry.

1.5.1 Alarmed area

The total area to which detection is afforded by an intruder alarm system or any group of zones that can be collectively controlled.

NOTES:

- 1 This defined volume need not necessarily have physical boundaries such as walls, floor and ceiling.
- 2 A group of zones that can be collectively controlled is also known as a 'partition'.

1.5.2 Alarm condition

Status resulting from any one of the following:

- (a) Activation of a detection device.
- (b) Activation of a tamper-detection device or circuit.
- (c) Activation of a deliberately operated device.
- (d) Fault condition.
- (e) System alarms.

1.5.3 Alarm transmission equipment

The equipment used to transmit signals from a client's premises to a remote location such as a monitoring centre.

1.5.4 Alarm warning device

Any device at the alarmed premises used to audibly or visually annunciate an alarm condition.

1.5.5 Arming

Placing the control equipment into a state that will report pre-determined signals from devices within the protected area.

1.5.6 Arming station

A device for arming and disarming (or otherwise controlling) the control equipment. The arming station may be remote to or integral with the control equipment.

1.5.7 Client

Person or organization utilizing the service of a security alarm company.

1.5.8 Control equipment

The equipment that processes signals to provide appropriate outputs.

NOTE: This may take the form of the main control equipment, data gathering panel, or other equipment appropriate for the system design.

1.5.9 Deliberately operated device

A device that can be deliberately operated to generate an alarm condition.

NOTE: For example, duress/hold-up button, which may be wired or wireless.

1.5.10 Detection circuits

A circuit connecting one or more detection devices to the control equipment of an intruder alarm system.

1.5.11 Detection device

A device designed to generate an alarm condition in response to intrusion, an attempted intrusion, tampering or deliberate activation.

NOTE: It may also generate an alarm condition in response to a fault or tamper.

1.5.12 Disarming

Placing the control equipment into a state that will not report pre-determined signals from devices within the protected area.

1.5.13 Fault condition

A condition caused by malfunction of the equipment or circuit and indicated audibly, visually or both.

1.5.14 Indicating equipment

Audible and/or visual indication of the system status. The indicating equipment may be remote to or integral with the control equipment.

1.5.15 Intruder alarm system

Any system designed to detect and signal the presence, entry or attempted entry of an intruder into an alarmed area.

NOTE: Non-intruder alarm devices and functions, such as smoke detection, medical alarms, building services and similar, may be integrated into an intruder alarm system; however, these are not covered by this Standard.

1.5.16 Monitored circuit

A circuit arranged to provide an alarm condition in the event of interference to or failure of the circuit in addition to the intended alarm signal.

NOTE: Also known as 'supervised circuit'.

1.5.17 Monitoring centre

Facility that complies with AS 2201.2, which monitors intruder alarm systems and provides specific responses.

1.5.18 Partial arming/disarming

Arming/disarming discrete zone(s) or area(s) within the alarmed area (see Clause 1.5.1, Alarmed area).

1.5.19 Power supply equipment

Equipment that provides electrical power for the operation of any component of an intruder alarm system.

1.5.20 Remote access

Any access to the intruder alarm system that is not directly achieved through the system arming station(s).

1.5.21 Restricted key

A key system that is protected by patent. Individual keys require written authorization to be replicated.

1.5.22 Satellite siren

A self-contained audible alarm that incorporates a dedicated power supply, and is designed to operate in the event of—

- (a) an alarm signal from the control equipment;
- (b) activation of tamper-detection devices or circuits protecting the satellite; and
- (c) attack on or interference with the line connecting it to the control equipment.

1.5.23 Security alarm company

Person or organization having licences, where applicable, and providing one or more of the following: design, supply, installation, operation, servicing, monitoring or maintenance of an intruder alarm system.

1.5.24 Shell

The walls, floors, ceiling or roof of a building structure or compartments contained therein.

1.5.25 System alarm

An alarm generated by the control equipment in response to an abnormal system condition, excluding fault conditions.

1.5.26 Tamper-detection device

Any device designed to generate an alarm condition in response to unauthorized interference with a part of an intruder alarm system.

1.5.27 Zone

That part of an intruder alarm system to which at least one detection device is allotted and for which individual indication is provided.

SECTION 2 SYSTEM INSTALLATION REQUIREMENTS

2.1 GENERAL REQUIREMENTS

This Section specifies the installation and commissioning requirements for parts of an intruder alarm system consisting of the following elements:

- (a) Control equipment, indicating equipment and arming station(s) complying with the requirements of Section 3.
- (b) Power supply equipment complying with the requirements of Clauses 3.11 to 3.14.
- (c) Detection devices complying with AS 2201.3.
- (d) Audible alarm warning devices complying with the requirements of Clause 2.4 and/or remote alarm transmission equipment complying with the requirements of AS 2201.5.
- (e) Wiring, jointings and terminations or wire-free links complying with the requirements of Clauses 2.6 to 2.10.

2.2 INSTALLATION

2.2.1 General

All equipment shall be installed in accordance with the manufacturer's instructions.

2.2.2 Control equipment and power supply location

Except where otherwise approved by the client in writing, the control equipment and power supply equipment shall be located within the alarmed area and, where practicable, shall not be visible from outside the alarmed area.

2.2.3 Mounting

All components shall be securely fixed in such a position to minimize the risk of interference or damage.

All components mounted to masonry shall be fixed in position using corrosion-resistant plugs or masonry anchors.

All components mounted to plaster board shall be fixed in position using purpose-designed corrosion-resistant wall anchors suitable for the weight loading. Where possible, at least two fixings should be into one or more timber or steel studs.

Bolts or machine screws, washers and anti-vibration devices shall be used where necessary for fixing into metal.

Corrosion-resistant bolts, screws and washers suitable for the environment shall be used.

2.2.4 Tamper detection

Tamper-detection devices shall be fitted in accordance with the system classifications specified in Section 3, as applicable.

2.2.5 Power supply equipment

Power supply equipment and indicators, excluding AC step-down transformers or solar cells which may be mounted remotely, shall be housed integrally with the control equipment or in separate enclosures(s) conforming to the requirements of Clause 3.7.

2.2.6 Battery marking

Each battery shall be legibly and durably marked with the month and year of installation.

2.2.7 Alarm transmission equipment

Where the alarm transmission equipment is housed in a separate enclosure, the enclosure shall comply with Clause 3.7.

2.3 DETECTION DEVICES

2.3.1 General

Detection devices shall be installed in accordance with the manufacturer's requirements and AS 2201.3. The number and type of detection devices shall be selected to mitigate the agreed risk profile selected in accordance with Clause 1.3.

The security alarm company shall make every reasonable effort to locate detection devices in order to optimize the balance between intruder detection and the risk of detecting unwanted signals and interference.

2.3.2 Zoning

Individual or addressable zones shall be provided for each powered electronic detection device (e.g., devices such as movement detectors, etc.).

Individual or addressable zones shall also be provided for each unpowered detection device (e.g., electromechanical devices such as reed switches etc.), except where identical multiple devices are installed on common adjacent detection points (e.g., double doors or multiple windows within the same frame).

2.3.3 End-of-line supervision

End-of-line supervision devices shall be terminated within detection devices where possible. Where this is not possible, they shall be terminated within a junction box fitted with tamper-detection devices meeting the requirements of Clause 3.16.3.5. The junction box shall be located immediately adjacent to the detection devices and interconnecting cables shall not be visible.

2.4 AUDIBLE WARNING DEVICES

Audible alarms shall meet the requirements of Clause 3.16.2.9 and shall sound as required in response to an audible alarm output being generated by the control equipment.

Class 1 and Class 2 intruder alarm systems shall incorporate at least two audible alarm warning devices.

NOTE: Legislation may impose bans or limits on the duration or sound level of audible alarms different from those specified herein.

2.5 ENVIRONMENTAL CONDITIONS

2.5.1 General environmental conditions

All equipment and materials shall be chosen to suit the expected environmental conditions at the installed location.

2.5.2 Special environmental conditions

If any equipment, material or wiring is located in a position where it may be exposed to dampness, corrosion or other special conditions, the design and construction shall ensure that the reliability of the system is not prejudiced by such a condition.

Any equipment installed where flammable or explosive gas or dust are reasonably expected to be present shall comply with the requirements of the appropriate Australian/New Zealand Standard(s) for equipment for use in such hazardous locations (see Notes 1 and 2).

NOTES:

- 1 Further guidance is given in HB 13.
- 2 For example, AS/NZS 3000 may require equipment installed in hazardous locations to comply with other relevant Standards.

2.6 WIRING

2.6.1 General

Any circuit wiring incorporated in an intruder alarm system shall be installed and connected in accordance with ACIF S009 or requirements of the relevant regulatory authorities. Where equipment is required to interface with low voltage circuits, the wiring shall comply with AS/NZS 3000. Wiring shall be arranged to minimize risk of attack or damage.

NOTE: Where practicable, wiring should be concealed, to reduce the risk of attack or damage.

The wiring specified in this Clause refers to copper conductors; however, it does not exclude the use of other conductors, fibre optics or radio waves for the transmission of signals.

2.6.2 Type of wiring

Wiring shall comply with the following requirements:

- (a) *Minimum rating* Wiring shall have a total cross-sectional area not less than 0.20 mm² and an outer sheath insulation rating not less than 300 V RMS. Except for coaxial cable which may have a solid core, conductors shall be stranded.

The following applies to Class 1 and 2 systems:

- (i) For single core and figure-eight cables, conductors shall have a minimum of 14 strands of diameter 0.20 mm.
- (ii) For multi-core cables (three or more conductors), conductors shall have a minimum of seven strands of diameter 0.20 mm.

The following applies to Class 3 systems and above:

- (A) For single core and figure-eight cables, conductors shall have a minimum of 24 strands of diameter 0.20 mm.
- (B) For multi-core shielded cables (three or more conductors), conductors shall have a minimum of seven strands of diameter 0.20 mm.
- (C) For multi-core non-shielded cables (three or more conductors), conductors shall have 14 strands of diameter 0.20 mm.
- (b) *Load sizing* Wiring shall be suitably rated for the intended load and sized such that, under all expected load and source voltage conditions, the voltage drop in the wiring shall not be sufficient to reduce the terminal voltage at the devices to 10% above the lower limit stated by the manufacturer.
- (c) *Open wiring* Wiring run as open wiring, such as along walls, shall be supported by clips at distances not exceeding 500 mm. Where additional support is necessary to avoid contact with the building structure, pipework or other features, to provide clearance or for any other purpose, additional supporting saddles, cleats, clips or insulators shall be provided.

- (d) *Wiring within ceilings and under floors* Wiring within ceilings including suspended ceilings, under floors and the like shall be neat and tidy and, where practicable, shall be clipped or stapled at distances not exceeding 1 m or run in conduit. Care shall be taken to avoid hazards such as hot-water pipes, and wiring shall be segregated from other wiring and electrical cables as specified in ACIF S009 or relevant requirements of the New Zealand Ministry of Economic Development (Radio Spectrum Management (RSM) Division).
- (e) *Flexible wiring* Where circuit wiring is required to be attached to hinged or movable doors or windows, conductors shall be insulated, flexible conductors complying with Clause 2.8.

2.6.3 Stress on conductors and terminals

Conductors shall be supported and arranged so that there will be no undue mechanical stress on either the conductors or the terminals to which they are connected.

2.6.4 Protection of wiring

The type of wiring shall be such that it is not adversely affected by environmental conditions to which it may be exposed (e.g., corrosion, heat, weather, mechanical damage, fumes and the like). Where liable to damage, or exposed to weather, wiring shall be adequately protected by conduits, piping, ducts or cover strips, in accordance with ACIF S009 or the requirements of the relevant regulatory authority.

Wiring shall be protected as follows:

- (a) *Wiring to control equipment and external alarms* Except where allowed below, wiring spaces for connection to control equipment and external alarms shall be arranged so that the wiring passes directly through the wall into the rear of the enclosure. Where such an arrangement is impracticable, the wiring from control equipment and external alarms to ceiling or floor space shall—
 - (i) contain or incorporate a monitored circuit with a level of supervision in accordance with the classification of the system (e.g., Class 1 systems shall meet the requirements of Clause 3.16.2); and
 - (ii) be encased by conduit complying with AS/NZS 2053.1, piping or one-piece duct.
- (b) *Wiring between buildings* Aerial, underground and surface wiring between buildings and to external detection devices shall be installed in accordance with the appropriate provisions of ACIF S009 or relevant regulatory authority, and shall meet the requirements of Items (a)(i) and (a)(ii) above. In addition, aerial cables shall have surge protection devices in accordance with AS/NZS 1768(Int).

2.7 JOINTINGS

Joints in wiring shall be concealed or contained within a junction box to reduce the possibility of tampering, and those between fixed wiring and flexible connections shall be mechanically supported to prevent acute bending or breakage of the conductors.

All joints shall be mechanically and electrically sound, and shall be of one of the following forms:

- (a) *Soldered joints* The conductors shall be mechanically connected and soldered. The finished joint shall be covered with a suitable insulating material.
- (b) *Clamped joints* The conductor shall be secured in accordance with Clause 2.9.