

Contact Name:
Company Name:
Contact Phone Number:
Address:
Date sent to company:

CODE OF PRACTICE



Intruder Alarm Systems

FOREWORD

This Code of Practice defines the policies and procedures to be followed by members of the New Zealand Security Industry Association Inc involved in selling, installing and servicing intruder alarm systems.

The objectives in preparing this document are to ensure that high professional standards are maintained, false alarms are minimized, legal responsibilities are complied with and consequently that the industry's image and reputation is maintained.

Compliance with this code will also assist in minimising member's exposure to legal risk in the event of equipment failure or client loss.

The requirements of this Code are mandatory and compliance is a condition of membership of the New Zealand Security Industry Association Inc.

© NEW ZEALAND SECURITY ASSOCIATION (INC.)

First Print: November 2002

Revised: August 2004

Revised March 2007.

© COPYRIGHT *The copyright of this document is the property of the New Zealand Security Association. No part of it may be reproduced by photocopying or by any other means without the prior written permission of the executive Director of the New Zealand Security Association, unless the circumstances are covered by the exemption section (19 and 21) of the Copyright Act*

INDEX

1	GENERAL.....	8
1.1	Scope.....	8
1.2	Standards.....	8
1.3	Licensing.....	10
1.3.1	Companies.....	10
1.3.2	Employees.....	10
1.3.3	Sub-Contractors.....	10
1.3.4	Certificates of Approval.....	10
1.4	Insurances.....	11
1.5	Pre-employment Issues.....	11
1.5.1	Screening.....	11
1.5.2	Confidentiality.....	11
1.6	Staff Training.....	12
1.6.1	Minimum Qualification.....	12
1.6.2	Additional Training.....	12
1.7	Security of Information.....	12
1.8	Courteous Behaviour.....	12
1.9	Health and Safety.....	12
2	DESIGN OF SECURITY SYSTEMS.....	13
2.1	System Operational Requirement.....	13
2.2	Risk Assessment.....	13
2.3	Security Devices and Equipment.....	13
2.3.1	Approved Items.....	13
2.3.2	Environmental Requirements.....	13
2.3.3	Electrical Compatibility.....	13
2.3.4	Electromagnetic Compatibility (EMC).....	14
2.3.5	Connection of Detection Devices.....	14
2.4	Manufacturer's Specifications.....	14
2.5	Signalling.....	14

- 3 SYSTEM INSTALLATION AND COMMISSIONING.....14
 - 3.1 Installation.....14
 - 3.2 Neat and Tidy Work15
 - 3.3 Changes to the System.....15
 - 3.4 Commissioning15
 - 3.5 Client and Equipment Records17
 - 3.6 System Access Codes17
- 4 SYSTEM MAINTENANCE17
 - 4.1 Routine Maintenance Schedules17
 - 4.2 Routine Maintenance – Domestic Installations17
 - 4.3 Routine Maintenance - Non-Domestic Installations17
 - 4.4 Maintenance Visits.....18
 - 4.5 Remote Programming Access18
 - 4.6 Changes to System Configuration18
 - 4.6.1 Changes Made by the Alarm Company18
 - 4.6.2 Changes Made by Third Parties18
 - 4.7 Fault Reporting and Response18
- 5 FALSE ALARM MANAGEMENT19
 - 5.1 Reducing False Alarms19
- 6 DISPUTES PROCEDURE20
- 7 REPORTING BREACHES OF THIS CODE OF PRACTICE20

SECTION 1: GENERAL

	Evidence
Company Details	
Name	
Trading name(s)	
Locations – list all locations you operate from within New Zealand	
Company Registration details (date and registration number)	
Auditor to sight Company Registration Certificate	
Directors (list)	
Auditor to check against Companies Office records	
Staff Numbers	

<p>Total:</p> <p>Numbers required to hold CoAs:</p>	
<p>Registration under the Private Security Personnel and Private Investigators Act 2010 (& Amdts and Replacements)</p> <p>All Directors, Staff and/or Contractors where there is a requirement to be licensed or hold a Certificate of Approval (COA) are registered under the Private Security Personnel and Private Investigators Act 2010and amendments.</p> <p>Auditor is to:</p> <ul style="list-style-type: none"> • Sight SG Licence issued by the Registrar • Check the COA for a range of not less than five staff. • Check at least three rosters for duty to ensure all staff working are licensed correctly. 	
<p>Contractors to the Member Company</p> <p>The primary contractor (the member) is responsible to ensure that all contract staff employed under any contractual arrangement are licensed or hold a Certificate of Approval as required under the Private Security Personnel and Private Investigators Act 2010and amendments.</p> <p>All contractors are to be required to show evidence to their principal that they have sufficient processes in place to ensure this requirement is always met.</p> <p>Auditor is to:</p> <ul style="list-style-type: none"> • Sight a declaration or a copy of the SG Licence issued by the Registrar to the Contractor • Check the member's staff for a current COA - not less than 10% of member's staff. • Check at least three rosters for duty to ensure all staff working are licensed correctly. • Check members' written evidence that all contracted staff hold a 	

<p>current SG licence and COA as required under the Private Security Personnel and Private Investigators Act 2010 and amendments</p>	
<p>Customer Service Levels This Code of Practice is issued in order to ensure that persons and organisations operating in the Security Guard field of the security industry provide a standard of service and quality of employee that meets the standard as defined in this Code of Practice as being the minimum level. Sufficient latitude is built into the Code to enable Security Companies to exercise initiative and individual expertise in the provision of service to a higher degree than that laid down in the Code.</p> <p>Auditor is to:</p> <ul style="list-style-type: none"> • Cite any examples of letters from clients praising individual staff or the company for provision of excellent standards of customer service. • Look for examples of training, posters, briefing notes, bonuses or recognition for staff to deliver excellent customer service 	

GENERAL

1.1 Scope

The requirements of this section apply to all members involved in any way with intruder alarm systems.

1.2 Standards

All security systems installed or maintained by members should comply with the requirements of the Standards listed below. Copies of the latest revisions of these Standards must be readily available to employees. If deviations from these Standards are necessary, for special reasons, the deviations shall be pointed out to the client and written confirmation obtained to the effect that the client understands and accepts the deviation.

NZS 4301:Part 1:1993	Intruder alarm systems – Systems installed in client’s premises
NZS/AS 2201.2:1992	Intruder alarm systems - Central stations
NZS 4301.3:1993 (AS2201.3:1991)	Intruder alarm systems - Detection devices for internal use
NZS/AS 2201.4:1990	Intruder alarm systems - Wire-free systems installed in client’s premises
AS/NZS 3000:2000	Electrical installations (known as the Australian/New Zealand Wiring Rules)
AS/NZS 3820:1998	Essential safety requirements for low voltage electrical equipment
AS/NZS 3100:2002	Approval and test specification -

General requirements for electrical
equipment

AS/NZS 4360:2004

Risk Management

1.3 Licensing

1.3.1 Companies

Companies, including sole traders, are required to be licensed according to the provisions of the Private Investigators and Security Guards Act 1974.

1.3.2 Employees

Employees and active Directors of licensed companies are required to possess a Certificate of Approval issued according to the provisions of the Private Investigators and Security Guards Act 1974.

1.3.3 Sub-Contractors

Companies are required to ensure that sub-contractor companies, including sole traders, are licensed and that their employees possess a Certificate of Approval issued according to the provisions of the Private Investigators and Security Guards Act 1974.

1.3.4 Certificates of Approval

In all cases, holders of Certificates of Approval must comply with Section 46 of the Private Investigators and Security Guards Act 1974 and:

- produce their Certificate of Approval to the police, or any other person they are dealing with, on demand
- provide the name and address of the Security Guard licence holder by whom they are employed to any other person, on demand
- ensure that their Certificate of Approval is valid
- not use the Certificate of Approval of another person

- use their Certificate of Approval only when working for the security guard licence holder (company) specified on the Certificate of Approval

1.4 Insurances

Members engaged in the design, installation and maintenance of security systems shall have appropriate cover in the following areas:

- Professional Indemnity Insurance
- Public Liability Insurance

Professional indemnity insurance and public liability insurance cover required of all NZSA members shall have due regard to the nature of the risk and the relevant standard but shall not be less than \$1,000,000.

1.5 Pre-employment Issues

1.5.1 Screening

Each applicant for employment shall be required to authorise pre-employment checks and provide a complete record of employment over the previous 7 years. References should be provided from not less than three sources including previous employers. The member is responsible for verifying these references and recording the outcome.

1.5.2 Confidentiality

Prior to employment, all applicants shall be required to sign a non-disclosure agreement that aims to maintain the confidentiality of both company and client information.

1.6 Staff Training

1.6.1 Minimum Qualification

All installation and maintenance technicians and supervisors employed by the company shall be adequately and properly trained and competent to do the work upon which they are engaged to the standards as set out in the relevant NZSA codes of practice. The minimum recommended qualification is Level 3 in the National Certificate in Electronic Security.

1.6.2 Additional Training

Additional training that is deemed necessary, including but not limited to, Health and Safety and product-specific training, is to be undertaken by all staff. The member is to maintain a record of current, continuing and completed training in respect of each staff member.

1.7 Security of Information

All members shall recognise that information related to client security systems is confidential and should be protected. Details of security systems shall not be divulged to anyone else unless that person has a legitimate need to know. Any documentation no longer required shall be disposed of securely.

1.8 Courteous Behaviour

All staff visiting clients' premises shall be courteous and respectful to the client and the client's staff and shall recognise that their performance and attitude will determine the client's image of his company and the security industry.

1.9 Health and Safety

All members and their staff are required to be familiar with and comply with current Health and Safety legislation and any other safety requirements. All members and their staff shall ensure compliance comply with client Health and Safety policy.

2 DESIGN OF SECURITY SYSTEMS

2.1 System Operational Requirement

When preparing a proposal for a security system the specifier shall draw up a System Operational Requirement sufficiently detailed to enable the client to fully understand the extent of the protection which is being offered. This shall have due regard to the nature of the risk, current and future operational requirements and any insurance cover required by the client.

2.2 Risk Assessment

The nature of the risk shall be the prime consideration in the design of the system. The risk from adversary attack should be established at an early stage to determine the correct layout of equipment and the degree of protection required. For example, protection of property and assets, personal safety and vandalism should be considered in perspective according to the level of risk involved. Risk should be assessed in accordance with AS/NZS 4360:2004.

2.3 Security Devices and Equipment

2.3.1 Approved Items

Only items, which comply with all current Standards and legislation, shall be used. Standards currently recognised by the NZSA are – AS, NZS, UL and CE with Telarc approval.

2.3.2 Environmental Requirements

Items shall be suitable for the environment in which they are to operate. In general all items shall be installed according to the manufacturers' specifications and instructions. No panel or switchboard shall be installed in a gas storage area.

2.3.3 Electrical Compatibility

Individual items shall be selected and interconnected in such a way to ensure satisfactory and continued reliable operation. In particular, consideration shall be given to ensuring that all electro-mechanical and solid state switching devices are conservatively operated in respect of voltage and current ratings.

2.3.4 Electromagnetic Compatibility (EMC)

Radio based alarm systems must comply with New Zealand's EMC standards for radio interference. Such equipment must display either the C-Tick (accompanied by the Supplier Code Number), or the Regulatory Compliance Mark (RCM) as specified in the current Radiocommunications (Compliance) Notice. The current Notice may be found on the Ministry of Economic Development's Radio Spectrum Management website.

2.3.5 Connection of Detection Devices

Not more than one detection device shall be connected to any detection circuit.

2.4 Manufacturer's Specifications

All security systems and associated equipment shall be used in accordance with the manufacturer's stated specification and should conform as a minimum to relevant New Zealand Standards.

2.5 Signalling

The method of signalling an alarm condition shall be fully considered. The merits of central alarm monitoring shall be pointed out to the client and a method of signalling must be adopted which is appropriate for the level of risk and the degree of protection being provided.

3 SYSTEM INSTALLATION AND COMMISSIONING

3.1 Installation

All installation shall be carried out in accordance with the appropriate Standards, regulations and the manufacturer's specifications.

3.2 Neat and Tidy Work

All installations shall be carried out in a neat and tidy manner and the client's premises left cleaned and tidy during and upon completion of the installation.

3.3 Changes to the System

If any changes are made to the system during the course of the installation which causes it to differ from that specified these changes must be confirmed in writing to the client and the client's written confirmation obtained.

3.4 Commissioning

System functionality shall be tested to demonstrate compliance with the System Operational Requirement. Commissioning shall cover at least the items listed below and a copy of all test data shall be left on site with the client. The commissioning report shall form part of the client and equipment records.

1. Basic plan showing the location of all devices
2. Zone listing
3. Test results for individual detectors sealed and activated
4. Test coverage of all detectors
5. Tamperers connected and tested at all required devices
6. Sirens (and strobes) connected and tested
7. Mains power connected and labelled at both ends
8. Electrical Certificate of Compliance (where direct wired mains wiring has been used)

9. Batteries connected and legibly dated
10. Standby voltage measured
11. Battery discharge current measured at full load (e.g. with sirens) with mains power off
12. Verification that all remote monitoring messages (voice, SMS, dialler etc) are received correctly
13. Monitoring report faxed to workshop or client site
14. Check that wiring is tidy
15. Wiring is correctly labelled
16. Ancillary cabling is labelled / colour coded
17. Warning labels in place
18. Entry/Exit times recorded
19. Name(s) of the technician(s) who performed the installation
20. Adequate training shall be provided to the client on the correct procedure for operating the system
21. Equipment user manuals shall be provided to the client
22. Technical instructions shall be filed with the client and equipment records
23. Client sign off that the system is operating satisfactorily in accordance with the System Operational Requirement

3.5 Client and Equipment Records

The company shall securely maintain complete and accurate records relating to each of its intruder alarm systems in accordance with Section 9.3 of NZS 4301:Part 1:1993.

3.6 System Access Codes

All system access codes, including engineering codes, are the property of the client and shall be disclosed to the client upon request.

4 SYSTEM MAINTENANCE

4.1 Routine Maintenance Schedules

In all cases, clients shall be provided with a maintenance schedule that specifies the work to be carried out during each routine visit. The schedule shall be based upon Section 9.2.1.2 of NZS 4301:Part 1:1993. Completed schedules shall form part of the client and equipment records.

4.2 Routine Maintenance – Domestic Installations

Routine visits to ensure the maintenance of the alarm system installed in the client's premises shall be made annually by an authorised representative of the alarm company. The period between regular maintenance visits shall be no more than 13 months.

4.3 Routine Maintenance - Non-Domestic Installations

Routine visits to ensure the maintenance of the alarm system installed in the client's premises shall be made twice annually by an authorised representative of the alarm company. The period between regular maintenance visits shall be not more than 7 months.

4.4 Maintenance Visits

Prior to making the visit, the company or its representative shall contact the client, advise of the visit and arrange a mutually convenient date and time. The authorised representative shall wear an identification card and produce it to the client upon arrival. The identification card shall contain the name of the company, and the name and photograph of the authorised representative. Additionally, the authorised representative shall be in possession of a current Certificate of Approval issued by the company.

4.5 Remote Programming Access

Alarm companies are responsible for system configuration. Liability and security issues can therefore arise if remote access is available to third parties. Companies should therefore advise clients against permitting remote programming access to their security system by any third party. The decision to permit remote programming access rests solely with the client.

4.6 Changes to System Configuration

4.6.1 Changes Made by the Alarm Company

In all cases where changes are made to the system configuration by the alarm company, the alarm company must immediately notify the client's alarm monitoring company of the changes made, whether or not the monitoring company is a third party. Notification should normally be by email with the latest downloaded system configuration file attached.

4.6.2 Changes Made by Third Parties

Where a client permits remote programming access, the company granted such access shall immediately inform the alarm company of any changes made to the system configuration. Notification should normally be by email with the latest downloaded system configuration file attached.

4.7 Fault Reporting and Response

The client shall at all times be kept informed of the current address and telephone number of the alarm company's emergency service facility. Under normal conditions the time taken for the company's representative to attend the client's premises, following notification of a fault, shall not exceed 8 hours.

5 FALSE ALARM MANAGEMENT

5.1 Reducing False Alarms

Every effort should be made to minimise the number of false alarms reported from the system. This will be substantially achieved if the above requirements plus those specified in the Standards are followed. The following additional points will also assist clients in this regard:

1. The alarm system should only be operated by persons who have been properly trained.
2. All doors and windows should be carefully closed and secured.
3. Moving objects should not be allowed within the range of the internal space detectors.
4. The agreed entry/exit procedure should always be followed.
5. The alarm system should always be treated with care and respect.
6. The alarm company should be advised of any changes in the building and contents which might affect the operation of the system.
7. Regular maintenance checks should be carried out in accordance with the requirements of Section 4 of this Code of Practice.
8. Check all equipment has been installed according to the manufacturer's recommendations.

6 DISPUTES PROCEDURE

In the event of any dispute arising between an NZSA member and their client concerning the operation of the system, the following procedures shall be followed:

1. The system shall be immediately inspected by at least 2 members of the company's staff, one of whom shall be a member of senior management. In the event that a second member of staff is unavailable, a senior member of another NZSA company or the technical support person for the distributor of the equipment can act as a substitute.
2. No admission of liability shall be made to the client, the client's insurers or any other persons.
3. Full and complete records of the results of the inspection shall be kept in a clear and tidy format. These shall include any chart recordings or other such documentation as appropriate. This information shall be retained for a minimum period of 7 years after the event.
4. Copies of the documentation referred to above shall be forwarded to the NZSA Executive Director immediately after the inspection. If necessary the Executive Director will then refer the matter to the NZSA disputes committee.

7 REPORTING BREACHES OF THIS CODE OF PRACTICE

Should NZSA members find clear evidence of breaches of this Code of Practice, they shall report their findings to the NZSA Complaints committee, in writing, via the NZSA Executive Director.

New Zealand Security Association Inc
 Audit Check List
 Intruder Alarm Systems (Domestic and Commercial)

(This Audit requires that one Domestic System and one Commercial System are audited)

Company Name: _____ System: _____ Auditor Name: _____ Date: _____

	<u>Check List for Compliance</u>	<u>Reference</u>	<u>Evidence</u>
1	GENERAL		
1.1	The Company is licensed under the PI&SG Act 1974.	COP 1.3.1	
1.2	All Directors, Staff and/or Sub-Contractors where, there is a requirement to be licensed or hold a certificate of Approval, are registered under the PI&SG Act 1974.	COP 1.3.2 COP 1.3.3	
1.3	The Company holds Professional Indemnity and Public Liability insurances with the latter being not less than \$1million.	COP 1.4	
1.4	Each applicant for employment has authorised pre-employment checks and provided a complete record of employment over the last 7 years. References to be provided from not less than three sources, including previous employers.	COP 1.5.1	
1.5	Prior to employment all applicants are to sign a non-disclosure agreement, maintaining confidentiality of client and company information.	COP 1.5.2	
1.6	Technicians are properly trained and competent to do the work upon which they are engaged.	COP 1.6.1	

	<u>Check List for Compliance</u>	<u>Reference</u>	<u>Evidence</u>
1.7	Additional training is provided and individual records are maintained.	COP 1.6.2	
1.8	There is a procedure for secure disposal of client information.	COP 1.7	
1.9	The company has copies of all the Standards specified in COP 1.2 readily available.	COP 1.2	
2	SYSTEM DOCUMENTATION		
2.1	Commissioning and Test Data is available on the client site.	COP 3.4	
2.2	A plan of the installation, showing placement of equipment and zones, is available.	COP 3.4	
2.3	The equipment complies with recognised standards (UL, AS/ NZS, CE, C-Tick, RMC) as appropriate.	COP 2.3	
2.4	An Electrical Certificate of compliance has been issued where appropriate.	COP 3.4	
2.5	Technical instructions are filed with Client and Equipment records.	COP 3.4	
2.6	Client and Equipment records are complete and accurate.	COP 3.5	

	<u>Check List for Compliance</u>	<u>Reference</u>	<u>Evidence</u>
3	CONTROL EQUIPMENT		
3.1	Each control panel / remote panel complies with NZS4301.1:1993 in respect of control and indication facilities, including labelling.	NZS 4301.1:1993 4.1	
3.2	Each control panel / remote panel is appropriately located.	NZS 4301.1:1993 4.2	
3.3	The control equipment is legibly and indelibly marked.	NZS 4301.1:1993 4.2 AS/NZS 3100:2002	
3.4	Each control panel / remote panel housing is correctly fitted with tamper detection.	NZS 4301.1:1993 4.3	
3.5	Each battery container is legibly and durably marked.	NZS 4301.1:1993 5.4.7	
3.6	Mains power is connected to the power supply equipment and properly marked.	NZS 4301.1:1993 5.6.3 & 5.8	
3.7	With the mains power off and the system under full load, voltage levels at each standby battery or power supply is not less than 95% of the rated voltage.	NZS 4301.1:1993 9.2.1.2.e	

	<u>Check List for Compliance</u>	<u>Reference</u>	<u>Evidence</u>
4	INSTALLATION & COMMISSIONING		
4.1	The overall installation is neat and tidy.	COP 3.2	
4.2	Wiring and cabling is tidy and correctly labelled.	COP 3.4	
4.3	All wiring has suitable physical protection.	NZS 4301.1:1993 7.2.4	
4.4	All terminals are of the correct type and secure.	NZS 4301.1:1993 7.5	
4.5	All cable sizes are correct.	NZS 4301.1:1993 7.2.1 & 7.4	
4.6	Detector coverage, regardless of the type used, meets or exceeds the System Operational Requirement.	COP 2.3.2	
4.7	Not more than one detection device is connected to any detection circuit.	COP 2.3.4	
4.8	Tampers are connected to all detectors needing them.	NZS 4301.3:1993 2.5	
4.9	All detectors are adequately protected from vibration (i.e., securely fixed).	NZS 4301.3:1993 2.7	

	<u>Check List for Compliance</u>	<u>Reference</u>	<u>Evidence</u>
4.10	Each detector is fitted with walk-test facilities.	NZS 4301.3:1993 2.12	
4.11	The walk-test facility can be disabled on each detector.	NZS 4301.3:1993 2.12	
4.12	Each detector is appropriately marked.	NZS 4301.3:1993 2.13	
4.13	Audible alarms are enclosed in protective housings.	NZS 4301.1:1993 6.2.1.2.1	
4.14	Audible alarm housings are protected by tamper detection devices.	NZS 4301.1:1993 6.2.1.2.3	
4.15	Audible alarms are appropriately located.	NZS 4301.1:1993 6.2.1.3 & 6.2.1.4.b	
4.16	Audible alarms comply with TA regulations on duration of sound.	NZS 4301.1:1993 6.2.1.5.1	
4.17	Automatic dialling equipment is appropriately located and protected.	NZS 4301.1:1993 6.2.4.2	

	<u>Check List for Compliance</u>	<u>Reference</u>	<u>Evidence</u>
5	OPERATION AND MAINTENANCE		
5.1	The system is undertaking its function in accordance with the System Operational Requirement.	COP 3.4 NZS 4301.1:1993 8.2.7	
5.2	There is provision for a 24/7 service for on call maintenance.	COP 4.7 NZS 4301.1:1993 9.2.3	
5.3	A Routine Maintenance Schedule is available.	COP 4.1	
5.4	A properly completed Client's Log Book is located inside the alarm control panel or other secure location.	NZS 4301.1:1993 9.3.6	
5.5	All tests undertaken during the audit are compared with, either on-site system print out, or, print out from a monitoring facility.	Audit Requirement	

Additional Remarks:

Auditor Signature: _____

Date: _____

For the Company:

Name: _____

Signature: _____

Date: _____