NZSA
NEW ZEALAND
SECURITY ASSOCIATION

CODE OF PRACTICE

SECURITY SYSTEMS:
ELECTRONIC AND PHYSICAL

Comprising:

- Camera Surveillance Systems
- Electronic Access Control
- Intruder Alarm Systems
- Physical Security Systems
- Security Integrators

Table of Contents

FOREWORD

This Code of Practice defines the policies and procedures to be followed by all members of the New Zealand Security Industry Association Incorporated involved in the provision of Security Services involving the use of Electronic and/or Physical Security Systems and including those who act as Security Integrators.

The objectives in preparing this document are to ensure that high professional standards are maintained, legal responsibilities are complied with and consequently that customers receive a quality service and the industry's image and reputation is maintained.

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

In this Code:
Sections 1 to 6 and 10 to 15 apply to all security technologies.

Sections 7, 8 and 9 are specific to each technology.

This document must be completed and sent to NZSA on application to undertake the NZSA Audit process as an Accredited Member. Where possible, supporting evidence should be provided or made available for review.

Members who are audited and deemed to be in compliance with this Code of Practice will not be required to undertake a further audit for a period of 5 years, subject to the satisfactory completion and return of the ACCREDITED MEMBER ANNUAL DECLARATION.

Section 1 - Company Information

DESCRIPTION	EVIDENCE
1.1 Company Name:	
1.2 Trading Name (if applicable):	
1.3 Senior Manager Details: - **Name** - **Position** - **Phone** - **Email**	

Section 2 – Training

DESCRIPTION	EVIDENCE
Induction Training Prior to the commencement of any duties Installers and Technicians must be trained and demonstrate competence in the following areas:	*NZSA to:* *- Sight standard induction training programme and staff records*
2.1.1 Occupational Health and Safety Prior to commencement of duties all new employees must undergo an Occupational Health and Safety Induction outlining the Companies Health and Safety Policy.	*NZSA to:* - *Sight no less than three examples of Health and Safety records for Member's staff* - *Sight records of Health and Safety Induction programmes completed for Members staff.*
2.1.2 Legal Rights, Powers and Obligations The Law as it applies to their role, relating to: - The Private Security Personnel and Private Investigators Act 2010 - Electricity Act 1992 - NZ Electrical Regulations 1997 and Associated Codes of Practice - Building Act 2004 - Health and Safety at Work Act 2015 - Privacy Act 1993	*NZSA to:* *- Sight standard induction training programme and staff records and verbally check knowledge with staff*
2.1.3 Administration Staff must have a clear understanding of the chain of control operated by the company. They should be trained to understand the differences and relationships between: - Standard Operating Procedures (SOP's) - Company Procedures - Site Procedures - Assignment Instructions	*NZSA to:* - *Confirm training and view examples.*

DESCRIPTION	EVIDENCE
2.1.4 Client, Customer and Public Relations Staff should be trained in the importance of building and maintaining relationships with the client and their customers. All staff represent their employer in the eyes of clients and the public and need to understand the impact their individual actions can have for the reputation of the company and of the industry in general.	*NZSA to:* - *Confirm training and view examples.*
2.2 Continuation Training **2.3** **2.3.1 Training towards National Qualifications** All staff (technicians and sales personnel) shall be adequately and properly trained, and competent, to do the work upon which they are engaged. The qualifications and training relevant to each position shall be a recognised NZQA qualification in the domain of Electronic Security or equal or equivalent through the process of "Recognition of Prior Learning/Current Competence". Ideally the member will have qualified Workplace Assessors on staff or available on a contract arrangement to complete assessment of any training completed. Ideally there will be an individual staff member plan for training to deliver a pathway for improvement of training knowledge and skills as he or she gains in experience. Files are to be maintained of training completed with the records clearly showing who met the standards required. Best practice is to also maintain individual staff member training files. This may not always be practical or possible given the resources available. As a minimum, major passes in training should be recorded in the staff member's personal file.	*NZSA TO:* - *Sight records of current, continuation and completed training.* - *Sight examples (where applicable) of credit registration for NZQA approved training.* - *Sight examples (where applicable) of workplace assessment by a trainer for current staff.*

DESCRIPTION	EVIDENCE
2.3.2 Maintaining Currency Security is constantly evolving through changes in approach, methods, technology, law and the nature of threats. Members must monitor these changes and incorporate them into their staff training as required.	*NZSA TO:* - *Sight any evidence that relevant changes in the law are advised to staff as soon as the change has been affected.* - *Sight any evidence that changes in technology are advised to staff as soon as practicable after such change of method becomes known.* - *Sight any evidence that refresher courses on the subjects previously instructed in are completed.*

Section 3 – Policy and Procedure

DESCRIPTION	EVIDENCE
3.1 Objectives The primary objectives of Electronic and Physical Security Systems should be to: 3.1.1 Act as a deterrent against undesirable activities, criminal or otherwise 3.1.2 Provide assurance, security and safety to people occupying the spaces covered 3.1.3 Detect unauthorised entry (Intruder Alarms) 3.1.4 Regulate entry into or from an area by: (a) mechanical key, keypad, electronic token or (b) biometric means (Electronic Access Control) (c) means of fences, gates bollards or other physical means (Physical Security)	
3.2 Manufacturers Installation Instructions 3.2.1 All Electronic and Physical Security Systems and associated equipment shall be installed within the limits of the manufacturer's stated installation instructions and conform to, at minimum, the relevant Standards as listed in Section 14 and this Code of Practice. 3.2.2 A copy of manufacturer's installation instructions for each product installed shall be kept on hand at the installer's premises. This may be in hard or soft copy formats.	*NZSA TO:* - *Check that copies of manufacturer's installation instructions are readily available and staff know where to access them.* - *Check that copies of this Code of Practice are readily available* - *Check that the member has copies of all the Standards specified in Appendix 1 readily available.*
3.3 Security Information All members shall recognise that information on security systems is confidential and should be protected. Details of security systems shall not be divulged to anyone unless that person has been authorised on a need to know basis. Those with a need to know may include the client's insurers and the Police.	*NZSA TO:* *- Check that there are procedures for secure storage and disposal of client information.*

DESCRIPTION		EVIDENCE
3.4	**Courteous Behaviour** In the context of this Code of Practice, all staff visiting Client's premises for whatever reason shall be courteous and respectful to the client and their employees/visitors. Each visiting staff member shall recognise that their performance and attitude will determine the Client's image of his/her company and the security industry at large.	*NZSA TO:* *- Check by observation and feedback from clients.*
3.5	**Occupational Health and Safety** The Member company must have an occupational health and safety policy suitable to the duties performed by their staff	*NZSA TO:* *- Verify mandatory Health and Safety Capability Audit undertaken.*
3.6	**Communications Equipment** Staff are required to be competent in the use of communications equipment and the appropriate protocols to be followed when using equipment to communicate with other parties. Communications equipment includes the following where applicable: - Radios (RT's) - Land line - Mobile telephone (calls) - Mobile telephone (text) - Computers	*NZSA TO:* *- Sight/observe/listen to not less than three staff using each form of communication equipment as applicable to the members operations*

Section 4 - System Operational Requirement

DESCRIPTION		EVIDENCE
4.1	**Establishing the Client's Needs** It is essential to establish what the client expects from the security system and how it is to be used. It is also essential that the client is made aware of the cost and human resource requirements for system management and maintenance. The client must be made aware of any proposed system limitations in the course of determining needs in order that they can make an informed decision. Members should have a system's limitations checklist that they discuss with clients and all limitations should be documented and signed off by the client as acceptable risks.	*NZSA TO:* *- Check that a documented process has been followed for at least two recent installations.*
4.2	**Establishing the Nature of the Risk** The nature of the risk shall be the prime consideration in the design of the system. The risk from criminal attack should be established at an early stage to determine the correct selection of equipment and for Camera Surveillance Systems, the positioning and degree of surveillance required. Protection of property and, personal safety and vandalism each require to be considered in the perspective according to the level of risk involved. In establishing the nature of risk, members must be cognisant of PSR (if applicable) and AS/NZS ISO 31000:2009: Risk Management. The Risk Assessment must be available before any design commences, to enable the correct selection of systems.	*NZSA TO:* *- Sight Risk Assessments process for at least two recent installations.*
4.3	**System Operational Requirement** When preparing a system proposal the specifier shall draw up a System Operational Requirement (SOR) sufficiently detailed to enable the client to fully understand the extent of the protection that 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.	*NZSA TO:* *- Check that a documented process has been followed for at least two recent installations.*

Section 5 – System Specification and Design

DESCRIPTION	EVIDENCE
5.1 Security Risk as a factor in "System Design" 5.1.1 "Security Risk" shall be a major influencing factor in the overall design of any security system. The risk should be established at an early stage to determine the performance needs, type and positioning of equipment and the degree of control required. Protection of brand (reputation), property, personal safety and information each need to be considered in determining overall risk. Refer: AS/NZS ISO 31000:2009 Risk Management 5.1.2 NZSA members' solutions shall not overstate the "Security Risks" in order to gain more sales or support excessive system solutions. 5.1.3 The client must be involved in determining system operational requirements and agree the areas to be controlled and at what times. 5.1.4 Clients shall be advised of system defaults under power loss, communications loss with field controllers, fire alarm activation and any other condition that has an impact on system performance. 5.1.5 Where integrated security systems are offered, care must be taken to ensure that all requirements within this Code of Practice and as applicable to each component of the security system are complied with.	*NZSA TO:* *- Check for evidence of compliance including evidence of a design process having been followed for at least two recent installations.*
5.2 Scoping Paper for Client Direct Installations 5.2.1 For new installations, a scoping paper /proposal which clearly reflects the clients operational requirements shall be produced and be made available to the client for sign off before any system is promoted. 5.2.2 The client maintains the right to have the Scoping Paper/Proposal peer reviewed before sign off. 5.2.3 The Scoping Paper/Proposal shall clearly state that although signed off by the client, the onus and responsibility for system design and operation rests with the designer and not the client. There will be exceptions to this and these exceptions shall be clearly listed and signed off by the client. 5.2.4 The Scoping Paper/Proposal shall clearly set out a complete scope of works including any items tagged out as the responsibility of others. The list of tagged items shall be signed off by the client in acknowledgement of works that the client will have to arrange for and pay separately. 5.2.5 The Scoping Paper/Proposal shall clearly set out a	

	complete equipment schedule for the whole of works including client training and "As Built" documentation. 5.2.6 The Scope of Works shall clearly set out what is included in terms of: time schedules, user groups, door groups, alarm groups, password levels and associated operator authorisations. Client involvement with this process is mandatory. 5.2.7 All passwords on a client system remain the property of the client and the system shall be configured to ensure that the client password remains as the system master password with the client having the facility to cancel all other passwords. All manuals, keys, programmed credentials, card database and system configuration databases remain the property of the client and shall be handed over on request if kept off site by the installer.	
	5.3 Equipment Selection 5.3.1 Clients should be advised on what technologies are available, the pros and cons of the varying types and any specific site conditions or needs that would prohibit the choice of one technology over another. 5.3.2 Another driver for the system design is the resource requirement required for day-to-day system management. Clients must be made aware of resource requirements, training needs etc. so that they can make an informed decision on equipment choice. 5.3.3 System maintenance shall also be a major factor in equipment selection in terms of serviceability, spare parts availability and costs for support services. System serviceability should always be available from multiple vendors within a reasonable geographical area. Where this is not the case, the client should be made aware of the risk	
	5.4 Approved Items Only items which comply with the current Standards and legislation shall be specified. Standards currently recognised by the NZSA are: AS, NZS, UL, IEC and CE	
	5.5 Environmental Factors 5.5.1 Items shall be suitable for the environment in which they are to operate. In general all items shall be installed according to the manufacturers' installation instructions. Panels and switchboards shall be installed in a gas storage area. 5.5.2 All equipment being proposed for installation must be suitable for the application for which it is intended. 5.5.3 Wherever equipment is likely to be exposed to adverse environments such as wet, damp, hot, dusty or corrosive conditions, then all practicable steps must be taken to	

	eliminate or minimise the impact by use of suitably selected equipment and installation methods.	
5.6	**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.	
5.7	**Electromagnetic Compatibility (EMC)** Radio based alarm systems must comply with Radio communications Regulations 2001 in respect of 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 Radio communications (Compliance) Notice. The current Notice may be found on the Ministry of Economic Development's Radio Spectrum Management website	
5.8	**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 degree of protection being provided	
5.9	**Operational Routine** The normal business routine of the client and their staff shall be taken into account in bringing about good operational procedures and interaction between the staff and the system. User friendliness must be a prime consideration in system design and equipment selection	
5.10	**System Expansion** In designing a system, due consideration should be given to accommodate future extensions to the clients business and/or premises in the short to medium term forecasts. The client shall be made aware of recommended expansion options and all associated costs and benefits of early provision.	

Section 6 - Installation

DESCRIPTION		EVIDENCE
6.1	**Installation** All installations shall be carried out in accordance with appropriate Standards, Regulations, the manufacturer's instructions and this Code of Practice.	
6.2	**Neat and Tidy Work** All installations shall be carried out in a neat and tidy manner and the client's premises left clean and tidy during and upon completion of the installation.	
6.3	**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 received.	
6.4	**Equipment** (a) All equipment installations shall be in accordance with the manufacturer's installation instructions and shall comply with all safety aspects of the Electrical Regulations including safe earth and safe isolation. (b) All equipment shall have an "Ingress Protection" rating (IP rating) appropriate to the environment in which it is to operate. (c) All control units/power supplies shall be in lockable, tamper monitored enclosures. (d) All power supplies shall maintain the connected load for not less than 8 hours (2 hours if there is a site generator). (e) Power supplies shall have mains fail and battery abnormal voltage health check monitoring which should be remotely monitored where possible. (f) All batteries shall be legibly and durably labelled with the installation date.	*NZSA TO:* *- Inspect two recent installations to check compliance.*
6.5	**Equipment Positioning** (a) Due consideration should be given to the possible interference to the conduct of the clients business or activity (b) Equipment locations shall ensure a safe working environment for servicing personnel and shall further ensure easy access for servicing. (c) Locating equipment in areas with difficult access is strongly discouraged.	*NZSA TO:* *- Check for evidence of compliance*

DESCRIPTION	EVIDENCE
6.6 Wiring (a) Cable Installation and general wiring practice shall be in accordance with relevant clauses of the relevant Standards and Regulations. The Regulations apply to all installations connected with any source from which electricity is available, except for those exempted by the Regulations. (b) NZSA member companies are to ensure that responsible employees in their employ are familiar with the requirements of the Electrical Wiring Rules (AS/NZS 3000:2007) in terms of ELV installations. (c) With modern systems having IP addressable system components, it is essential that all cable runs be installed to meet the limit in networking cable distances. Where the client has an IT specialist/department, close liaison for network design/connectivity is strongly recommended. (d) All cabling shall be supported on appropriate cable reticulation systems (conduits, trays, ducting, catenary wire) and shall not be laid directly on false ceiling. (e) All cabling shall be installed in parallel to the main building axis and not in a direct point-to-point configuration. (f) All 230volt electrical works shall be carried out by a registered electrician and listed on a certificate of compliance with a copy given to the client. (g) All cabling shall be selected as appropriate to the environment in which it is to be installed. (h) Maintain a minimum separation distance between security system cables and mains voltage cabling. All cabling installed within 450mm of power cabling (230/440v) shall have an insulation rating of not less than 500volts as required under AS/NZS. (i) All cabling shall be legibly and durably labelled. (j) All video cable shall be selected to satisfy the transmission medium and to minimise video loss and interference. Installation and termination shall be in accordance with manufacturer's instructions. (k) Where interference is detected, the installation shall include all necessary forms of isolation to effect isolation of the source.	*NZSA TO:* - *Inspect two recent installations (preferably one domestic and one commercial) to ensure:* 1. *Cabling/wiring is tidy and conforms to best practice* 2. *An Electrical Certificate of Compliance has been issued when required* 3. *Mains and data circuits are segregated* 4. *Cables are correctly labelled.*

Section 7 – Access Control

DESCRIPTION	EVIDENCE
7.1 Operational requirements The access control system operational requirements shall take the following into account: 7.1.1 Determine which doors/gates/grills/barriers (access points) are to be controlled 7.1.2 Determine the appropriateness of the access point (in terms of practical application and operational reliability) to have an access control system fitted. (An example would be a door with a ceiling void above leading into the controlled space) 7.1.3 Determine the appropriateness of lock selection with regard to door swing, door usage and emergency egress. 7.1.4 Determine the potential traffic through each access point to ensure appropriate equipment selection. 7.1.5 Determine the operational requirements for each access point. 7.1.6 Identify need for door hold open devices and fire alarm release. 7.1.7 Determine emergency egress requirements 7.1.8 Identify the need for automatic door closers. 7.1.9 Identify the need for door closer coordinators. 7.1.10 Identify the needs for emergency override (emergency access and fire egress routes) 7.1.11 Identify the need for jemmy-bar protection devices and hinge bolts 7.1.12 Identify the resources needed for day-to-day systems management. 7.1.13 Ensure building code requirements are met (penetrations, fire ratings etc) 7.1.14 Fire Alarm Interface – Electronic Access Control (a) Ensure that all access controlled doors allow free egress from the building in the event of a fire or emergency. This does not mean that the locks must release on a fire dump. At minimum, on the secure side of the door there must be a means to release the lock. Mortise locks will have a free handle; electromagnetic locks will have a REX and EDR. It is not acceptable for a user to perform more than a single task to unlock a controlled door for egress unless approved in writing by a registered "Fire Engineer." (b) In some installations such as prisons, courts, forensic wards etc there is a requirement to have locks fail secure to facilitate a staged evacuation if necessary. These special circumstances will require compliance	*NZSA TO:* *- Inspect two recent installations and check that Operational Requirements have been met.*

certification from a registered "Fire Engineer".

(c) Ensure that the "Fire Alarm Interface" agrees with the fire evacuation plan for the building and if in doubt, discuss and agree a sensible solution with the "local fire service or Fire Engineer".

7.1.15 Lift Interface – Electronic Access Control

(a) There are various forms of access control for lifts and clients need to be aware of all basic forms.

(b) Floor selection without destination reporting (low level – generally one credential presentation allows multiple floor selection – associated risk of tail-gating)

(c) Floor selection with destination reporting (high level – one credential presentation, only one floor selected and reported – higher security but does not prevent tail-gating. This may be achieved either through a hardware/firmware solution or total software solution). Irrespective of which system is chosen, the lift emergency override has precedence over all security requirements.

7.2 Installation Requirements

7.2.1 All equipment other than access control point (lock cylinder, keypad and credential reader) shall be located within the secured area and in accordance with manufacturer's recommendations.

7.2.2 Determine where access readers will be positioned and whether they will be subject to weather conditions or vandalism and select equipment appropriately to mitigate the risk.

7.2.3 For safety reasons, card readers shall be positioned well beyond doors opening in the direction of the reader.

7.2.4 For safety reasons, REX and EDR devices shall be easily identified and located well beyond door opening in the direction of the REX/EDR.

7.2.5 REX and EDR devices shall be located in such a manner that they cannot be compromised from the unsecured side of the control point.

7.2.6 Wherever possible, computer based equipment with hard drives shall be located in a secure controlled environment where the air temperature will be maintained between 19 and 21 degrees Celsius. Where this is not possible, the client should be made aware of potential operational risks.

7.2.7 Field equipment including door controllers, lift controllers and power supplies shall be located to ensure that operating temperatures are maintained within manufacturer's tolerances.

7.2.8 Blind bolts/Hex Bolts on the un-secure side of the door shall be the only acceptable fixing system for electromagnetic lock armatures and Z brackets.

7.2.9	All cables used are “fit for purpose”, taking into account: (a) Voltage drop (b) Data integrity	

Section 8 – Intruder Alarms

DESCRIPTION	EVIDENCE
8.1 Operational requirements The intruder alarm system operational requirements shall take the following into account: 8.1.1 Installation in accordance with appropriate sections of ASNZS 2201. 8.1.2 Determine which doors shall be the entry and egress doors. 8.1.3 Discuss the implications of furniture and other room contents in terms of masking the coverage. 8.1.4 Determine the areas of the premises to be covered and allocate zones accordingly. 8.1.5 Determine the most appropriate technology to provide each zone coverage. 8.1.6 Ensure the perimeter of the protected area is covered (external doors, windows trapdoors etc) 8.1.7 Determine the required response: (a) Sirens (b) Strobe lights (c) Off-site monitoring 8.1.8 Establish any special requirements including partial set/unset, pet ally etc.	*NZSA TO:* *- Inspect two recent installations and check that Operational Requirements have been met.*
8.2 Installation Requirements 8.2.1 All equipment shall be located within the secured area and in accordance with manufacturer's recommendations. 8.2.2 All cables installed in a secure and unobtrusive manner. 8.2.3 All cables used are "fit for purpose", taking into account: (a) Voltage drop (b) Data integrity (c) All penetrations back- filled with the required fire/vermin proof materials.	

Section 9 – Video Surveillance

9.1 Legal Limitations and Requirements Note: Guidance from the Privacy Commissioner on the impact of the Privacy Act on the use of Camera Surveillance Systems can be downloaded from: http://privacy.org.nz/assets/Files/Brochures-andpamphlets-andpubs/Privacy-and-CCTV-A-guide-October-2009.pdf. Where video surveillance is installed for external security purposes, signs should be prominently displayed so that casual visitors/customers will know of the surveillance. Determine in advance the period for which the recording will be kept and who will have access to it. Only disclose the contents of the recording for the purpose of which it was obtained and erase/delete as soon as possible, those parts of the recording, which are irrelevant to the investigation. Where stored images are likely to be required for evidential use, then all current legal requirements should be taken into account. These include but are not limited to: - Correct time and date; - Watermarking; - Export of original/complete images in the native file format without further compression; 9.1.5 Export/provision of a video player or similar device that will allow native file format images to be viewed using a standard Windows computer without requiring the installation of additional software to the computer.	*NZSA TO:* *- Inspect two recent installations and check that Operational Requirements are met.*
9.2 Operational Requirements 9.2.1 Schedule of Surveillance – When preparing a proposal for a Camera Surveillance System the specifier shall draw up a Schedule of Surveillance sufficiently detailed to enable the client to fully understand the extent of surveillance that is being offered. This shall have due regard to the nature of the risk and any insurance cover held by the client. 9.2.2 Equipment positioning – Due consideration should be given to possible interference of the field of view because area utilisation has been altered (signage, vegetation, racking, partitions etc.). No Camera Surveillance Camera should be deployed within toilet, change room facilities or other similar sensitive locations. 9.2.3 Due consideration should be taken to counter the effects of sunlight, glare and low light conditions when choosing cameras, lenses and the siting of such equipment.	

9.2.4 Where extreme low light conditions are encountered, use of additional lighting and/or infrared illuminators should be investigated. Colour rendering is an essential consideration.

9.2.5 The following factors must be considered:

(a) Detail to be observed. (This is affected by: - field of view, depth of field, distance from the camera and percentage of coverage.)
(b) Environmental conditions (natural light, artificial light, vegetation and weather.)
(c) All equipment shall have an "Ingress Protection" rating (IP rating) appropriate to the environment in which it is to operate.
(d) Camera equipment; including environmental housings, pan tilt and zoom (PTZ), or auto-pan, lenses, and other site specific equipment.
(e) Operational periods, and image placement of date and time references.
(f) Alarm interfaces and associated recording action.
(g) Equipment serviceability.

9.2.6 The following factors must be considered at each monitoring location:

(a) Staffed or un-staffed monitoring position.
(b) Video management software (VMS)
(c) Integration with automated access control and intruder detection systems.
(d) Time schedules where different monitoring parameters are required.
(e) Number of monitors and number of cameras per monitor
(f) Video imaging including; split screens, number of pictures to be displayed, and their relative positions on screen.
(g) Camera control systems including camera, lens (manual or automatic), camera position, washers and wipers, lighting, method of video and control transmission.
(h) Recording devices and media including; number of recorders, number of cameras per recorder and switching methods, recording duration per camera, requirements for recording rates, type of recorder and video management software.
(i) Alarm/Event driven interface to draw attention to an activity and/or record same, type of alarm detection method (intruder alarm system, video motion detection, intelligent scene monitoring.)
(j) OSH compliance requirements.

9.3	**Installation Requirements** 9.3.1 Video reticulation systems (fibre optic cable, coaxial cable, unshielded twisted pair, microwave link, RF link, wired or wireless network or other technology.) 9.3.2 Power supplies including power over Ethernet (PoE) switches.	
9.4	**Covert Operational Requirements** (a) Covert application of Camera Surveillance Systems is permissible for staff monitoring and surveillance for the purposes of an investigation. Its application should be limited to the time required to establish the cause of known or suspected criminal activity with monthly reviews up to a maximum deployment period of three months or as agreed with the client. (b) Staff should be informed of any CCTV use within their work areas (other than specific limited time covert operations)	

Section 10 – Testing and Commissioning

DESCRIPTION	EVIDENCE
10.1 Test Equipment All system test equipment shall be supplied by the installation company. Whilst equipment requirements will be dependent on the nature of the installation, the following items would be expected to be included: (a) Multi Meter (b) Pre-programmed valid card (c) Pre-programmed invalid card (d) Spare DPS magnet (e) Replacement EDR glass windows and reset tools (f) Laptop for programming (where required) (g) Printer or soft copy data capture device to off load system reports (h) Light Level or Lux Meter (camera surveillance system) (i) Calibrated camera target - preferably target should be representative of an average sized adult (camera surveillance system) (j) High resolution portable monitor (camera surveillance system)	
10.2 Commissioning Tests The primary outcome of commissioning tests shall be to satisfy the customer that they have been delivered a system that meets their expectations (as agreed under Section 4 Operational Requirement and Section 5 System Specification and Design). System functionality must be fully tested to demonstrate compliance with the System Operational Requirement and this is to be recorded on Commissioning Sheets. The Commissioning Sheets and test data shall form part of the client equipment records with a copy provided to the client. Commissioning documentation shall cover all functionality within the System Operational Requirements and include the following: 10.2.1 Camera Surveillance Systems (a) For all camera, tests conducted under a variety of lighting conditions ranging from darkness to bright sunlight (including direct sunshine where observed) to confirm overall acceptable performance. (b) For all internal cameras that face towards building perimeter windows, the same tests as per (a) should be applied. (c) The clarity of all video or recordings shall be such as	*NZSA TO:* *- Inspect two recent installations (preferably one domestic and one commercial) to check compliance with Commissioning Test requirements.*

to readily identify the target object both for direct viewing and from any playback device. (d) Provide the client with computer media/recording/photo's of test images for future reference along with a complete set of 'As Built" documentation, product information and user instructions. (e) Provide the client with all necessary training in the operation of the system and include telephone contact details for on-going support.	
10.2.2 Electronic Access Control and Physical Security Systems (a) Checks for all head end and field equipment (b) Local and remote monitoring (c) User training needs 10.2.3 Intruder Alarm Systems (a) Basic plan showing location of all devices (b) Zone listing (c) Test results for individual detectors sealed and activated (d) Test coverage of all detectors (e) Tampers connected and tested at all required devices (f) Sirens (and strobes) connected and tested (g) Mains power connected and labelled at both ends (h) Electrical Certificate of Compliance (where direct wired mains wiring has been used) (i) Batteries connected and legibly and durably dated (j) Standby voltage measured (k) Battery discharge current measured at full load (e.g. with sirens) with mains power off (l) Verification that all remote monitoring messages (voice, SMS, dialler etc.) are received correctly (m) Monitoring report faxed or emailed as per instructions (n) Check the wiring is tidy and correctly labelled. (o) Ancillary cabling is labelled/colour coded (p) Warning labels are in place (q) Name(s) of the technician(s) who performed the installation. (r) Adequate training shall be provided to the client on the correct procedure for operating the system (s) Equipment User Manuals and other information shall be provided in accordance with Section 4.1 of AS/NZSA 2201:2007. (t) Technical instructions shall be filed with the client and equipment records. (u) Client sign off that the system is operating	

	satisfactorily in accordance with the System Operational Requirement.	
10.3	**Client and Equipment Records** Initial records of equipment and system configuration shall be furnished to the client upon completion and commissioning as part of the operating and maintenance manual. The company shall securely maintain complete and accurate records relating to each of its security systems in accordance with Section 6.1 of AS/NZS 2201:2007 and ensure this information is available to the company's representative before every maintenance visit.	

Section 11 – Requirements for Regular Maintenance

DESCRIPTION	EVIDENCE
11.1 Routine Maintenance Procedures In all cases, clients shall be provided with a maintenance schedule that specifies the work to be carried out during each routine visit.	*NZSA TO:* *- Check that a suitable maintenance schedule is used by the company and that maintenance records are being maintained.*
11.2 Routine Maintenance Clients should be made aware of the advisability of having in place a routine maintenance programme. Routine visits to ensure the maintenance of the alarm system installed in the client's premises should be made by an authorised representative of the Member Company. The maximum time between maintenance visits should not exceed: - 24 months in the case of domestic installations - 12 months in the case of commercial installations.	
11.3 Maintenance Visits Prior to making the visit, the Member 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 Member company, and the name and photograph of the authorised representative. Additionally, the authorised representative shall visibly wear or display a valid Security Personnel Badge issued by the Licensing Authority.	

DESCRIPTION		EVIDENCE
11.4	**The System** Maintenance checks should be as per manufacturer instruction but include the following for all systems: (a) Make an inventory of the system to ensure all components are present in their correct location. Equipment serial numbers should be checked against the original installation record. (b) Check ventilation and security of all components. (c) Check the condition and the security of cables and connections. Pay particular attention to connectors and ensure they are soundly fixed to the cable with no internal shorts or open circuits. (d) Check condition of batteries (e) Note any environmental changes and the effects they have on the system.	
11.5	**Access control systems** Maintenance checks specific to Access Control and Physical Control Systems should include the following: (a) Use a valid card to prove access granted (all doors and lifts) (b) Use an invalid card to prove access denied (all doors and lifts) (c) For systems with intelligent controllers, interrupt the communications line and prove access granted/denied as above (d) Check that the automatic door closers operate 100% from both part open position and full open position (all doors) (e) Prove that the DOTL (Door Open to Long alarm) is functional (all doors) (f) Confirm that there are no obstacles to emergency egress at any controlled access point (all doors) (g) Confirm day-light savings is set to auto-update and has been programmed accordingly (h) Confirm that door forced alarms are generated under the forced door condition (all doors) (i) Confirm that there is a mechanical means to access the system controllers to manually operate doors in the event of a serious system malfunction. (j) System and card databases are to be backed up (daily/weekly/monthly/bi-monthly/annually or annually) with a backup file stored off site and	*NZSA TO:* *- Sight completed maintenance schedules in respect of at least two recent Camera Surveillance System installations*

updated at the agreed frequency of the back-ups. Confirm with the client a system back-up schedule.

(k) Confirm that all time controlled schedules are automatically updated for programmed holidays.

(l) Confirm the operation of all fire and emergency system interfaces and at least annually carry out a complete emergency egress test in conjunction with the fire alarm system provider where IQP certification is required.

(m) Provide the client with the necessary service documentation to facilitate his/her building Warrant of Fitness. Documentation should cover at minimum the service checks required to achieve building compliance under the local body IQP regime. The client should be advised of the risks associated with not having such checks performed.

(n) After each agreed service check, provide the client with a detailed system status report including any items that require immediate or short term remedial works to keep the system compliant. Items not covered under a maintenance agreement should have estimated costs on an item per item basis.

(o) For all installed systems, the client should be offered a maintenance contract option either as fully comprehensive (all parts and labour included) or preventative and response (fixed portion plus response and parts). It is the client's prerogative to decline but declination has risk factors that should be discussed with the client

(p) Carry out manufacturer specified maintenance including:

- Door position switches
- Lock operation
- Door closer operation
- Reader functionality
- REX operation
- Emergency egress operation

11.6 Intruder Alarm Systems

The schedule shall be based upon Section 5.2.1.2 of AS/NZS 2201:2007. Maintenance records shall be maintained in accordance with Section 6.2 of AS/NZS 2201:2007 and shall form part of the client and equipment records.

- Ensure correct functioning of:
- Keypads

- Door position switches
- Detectors
- Sirens
- Off-site monitoring

11.7 Camera Surveillance Systems

Maintenance checks specific to Camera Surveillance Systems should include the following:

(a) For all systems make a comparison of the current recorded image quality with the original recording made at the time of commissioning (Original recordings should be held on site in a secure location)

(b) For Cameras:

- Reassess camera locations. Is the field of view still clear; is the camera vulnerable to interference?
- Check for image burn and missing pixels on cameras and assess the expected service life until replacement will be required
- Make a visual inspection for any physical damage
- Check camera mountings for position, corrosion and rigidity
- Check lens focus, including back plane focus, aperture, scene illumination and optimum picture quality
- Clean all camera housings, windows, lenses etc.
- Ensure lenses and their connecting cables are correctly attached to the camera.
- At the monitor, manually select each camera and note the clarity of picture.

DESCRIPTION	EVIDENCE
(c) Check outdoor camera housings to ensure that - all cable entry points are adequately bushed - there are no signs of condensation on the face plate of the housing - the mounting is rigid, corrosion free and adequate to support the camera and housing, etc. without movement - the front of the lens is as far as practicable 20mm to 50mm from front of the housing - the camera is operating within specified temperature range - that all housing ventilation systems are operational and free from obstruction - No insects have taken up residence (d) Controls - Check that all controls, manual and automatic, perform to manufacturer's specifications - Ensure that auto-sequencing times meet the sire's needs and that the process is clean and without picture roll. (e) Monitors - Check for image quality on the monitors. Provide an assessment as to when replacement will be required. - Make a visual check for physical damage - Check cabling and connectors - Check operation of all control settings - Clean monitor screen (f) Recorder / Video Archive - Check (correct) the date/time settings on the DVR/NVR/Video Management system software. - Check the clarity of recorded images on playback and compare these with the original images recorded at commissioning. - Check that all equipment functions operate correctly (STOP; PAUSE; SEARCH; FF, RW, video and player export etc.) (g) General - Provide a general assessment of the system - Check with those responsible for daily operation that they are sufficiently familiar with its operation. If there is any doubt, arrange for training - Provide new computer media/recording/photos of test images of the systems current performance.	

Section 12 – Programming

DESCRIPTION		EVIDENCE
12.1	**Remote Programming Access**	
12.2	Written advice should be provided to clients where a system has been configured to allow authorised remote access for maintenance and/or operational purposes.	
12.3	Member companies are responsible for system configuration. Liability and security issues can therefore arise if remote access is available to thirds parties. Member companies should therefore advise clients against permitting remote access programming to their security system by any third party. The decision to permit remote access does however rest with the client.	
12.4	**Changes to System Configuration**	
12.5	Changes made by the Install (Member) company In all cases where changes are made to the system configuration by the install company, the Member 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.	
12.6	Changes made by a third party Where a client permits third party remote access, the company granted such access shall immediately inform the Member company of any changes made to the system configuration. Notification should normally be by email with the latest downloaded system configuration attached.	
12.7	**Fault Reporting and Response** The client shall at all times be kept informed of the current 24-hour contact details of the Member 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, should not exceed 8 hours	

DESCRIPTION	EVIDENCE
12.8 System Access Codes All system access codes, except installer engineering codes, are the property of the client and shall be disclosed to the client on request. Should a client wish to engage a different service provider, the installer engineering code should be changed by the current service provider and the new code supplied to the client along with a copy of the system installation manual. Clients should not be expected to pay any more than a standard call-out fee for this service. Clients should be advised to pass the code and installation manual to the new service provider without delay. The new service provider should then change the installer engineering code as soon as possible.	

Section 13 – False Alarm Management (guidance for clients)

DESCRIPTION	EVIDENCE
13.1 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 within the Standards are followed. The following additional points will also assist clients in this regard. (a) The alarm system should only be operated by persons who have been properly trained. (b) All doors and windows should be carefully closed and secured. (c) Moving objects should not be allowed within the range of the internal space detectors (including curtains, photo copiers which may overflow during after-hours etc.) (d) The agreed entry/exit procedures should always be followed. (e) The alarm system should always be treated with care and respect. (f) The alarm company should be advised of any changes in the building and contents which might effect the operation of the system. (g) Regular maintenance checks should be carried out in accordance with the requirements of Section 9 of this Code of Practice. (h) Check all equipment has been installed according to the manufacturer's recommendations.	

Section 14 – Standards and Legislation

All security systems installed or maintained by members should comply with the requirements of the Standards listed below. Copies of the latest revisions of those Standards relevant to the services provided by the member must be readily available to employees (online access for NZ standards is free to NZSA members) . 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.

Risk Management

AS/NZS ISO 31000:2009	Risk Management - Principles and guidelines

Access Control

AS/NZS 4121:2001	Design for Access and Mobility

Fences

AS/NZS 3016:2002	Electrical installations - Electric security fences

Doors/Gates/windows

AS/NZS 60335.2.103:2011	Household and similar electrical appliances - Safety - Part 2.103: Particular requirements for drives for gates, doors and windows
AS/NZS 2343:1997	Bullet-resistant panels and elements
AS/NZS 2803.1:1994	Doors - Security Screen - Hinged
AS/NZS 2804.1:1995	Installation of security screen doors - Hinged
AS/NZS 2803.2:1995	Doors - Security Screen - Sliding
AS/NZS 4483.1:1999	Security screen doors and security window grilles - Methods of test - Method 1: Dynamic impact test
AS/NZS 4604:1999	Security window grilles

Guarding

ASNZS4421-2011-	Guard & Patrol Security Services

Electronic Security (General)

AS/NZS 3000:2007	Electrical Installations (Australia / New Zealand Wiring Rules)

Alarms

AS/NZS 2201.1:2007	Intruder Alarm Systems - Client's premises - design, installation, commissioning and maintenance
NZS 4301.3.1993	Intruder Alarm Systems - Detection devices for internal use (AS 2201.3:1991

Legislation

Private Security Personnel and Private Investigators Act 2010
NZ Building Act 1991 and in particular, means of escape from buildings
The Health and Safety at Work Act 2015
Privacy Act 1993
Electricity Act 1992