

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

CODE OF PRACTICE



Electronic Access Control CODE OF PRACTICE

Index

1	Company Information.....	4-6
2	<u>Glossary of terms</u>	7
3	<u>Information Dissemination</u>	9
4	<u>General</u>	9
4.1	<u>Staff Registration</u>	9
4.2	<u>Insurance</u>	9
4.3	<u>Staff Training</u>	9
4.4	<u>Courteous Behaviour</u>	10
4.5	<u>Related Standards and Legislation's</u>	10
4.6	<u>Manufacturers Specification</u>	10
4.7	<u>Security of Information</u>	10
5	<u>Access Control Objectives</u>	11
5.1	<u>Establishing the Clients Needs</u>	11
5.2	<u>Security Risk as a factor in "System Design"</u>	11
6	<u>System Design</u>	12
6.1	<u>Operational requirements</u>	12
6.2	<u>Operational Routine</u>	12
6.3	<u>Fire Alarm Interface</u>	12
6.4	<u>Lift Interface</u>	12
6.5	<u>System expansion</u>	13
6.6	<u>Scoping Paper for Client Direct Installations</u>	13
6.7	<u>Equipment Selection</u>	13
6.8	<u>Equipment Positioning</u>	14
7	<u>System Installation</u>	14

7.1	<u>Wiring</u>	14
7.2	<u>Equipment</u>	15
8	<u>Testing and Commissioning</u>	15
8.1	<u>Test Equipment</u>	15
8.2	<u>Commissioning Tests</u>	16
9	<u>Requirements for Regular Maintenance</u>	16
9.1	<u>The System</u>	16
10	<u>Audit Check List</u>	17

1: COMPANY INFORMATION

	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	
Total:	
Numbers required to hold CoAs:	

<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 2010 and 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 2010 and 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 current SG licence and COA as required under the Private Security Personnel and Private Investigators Act 2010 and amendments 	

<p>Customer Service Levels</p> <p>This Code of Practice is issued in order to ensure that persons and organisations operating in the Access Control 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 	
<p>Public Liability Insurance</p> <p>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.</p> <p>The Auditor is to:</p> <ul style="list-style-type: none"> • Sight a placement slip, insurers policy document or invoice from an insurer showing the Public Liability cover is in place and current. 	

2 Glossary of terms

Glossary of Terms and Meaning	
Electronic access control system	An electronic system specifically designed to operate electrically operated doors, automated gates and elevators or any combination thereof via the use of credential readers or biometric devices. For the purposes of this Code of Practice, the primary function of the system will be the electronic control of access doors/gates (more than 6 controlled doors/gates) and for multiple users (more than 20)
Integrated system	For the purpose of this Code of Practice an integrated system (intruder alarm + access control) will be considered as an access control system provided the system has at minimum (more than 6 controlled doors/gates) and for multiple users (more than 20)
Electronic keypad operated locks	For the purpose of this Code of Practice this form of control will not be considered as an electronic access control system.
REX	Request to exit device – May be free handle, push button, proximity switch, beam device or other such approved device to release the electric locking device.
EDR	Emergency door release device – Shall be an internationally recognised authority (UL, CE or equivalent) approved device to immediately release the electric lock under any circumstances when operated.
DHBR	Door hold back release device used to release magnetically held open doors. This device should be a different colour from the EDR and REX. Wording to clearly indicate function of “Hold Back Release”.
Fire alarm interface	An approved connection between the building fire alarm system and the access control system to immediately release electrically locked doors on building egress routes when the fire alarm system is operated.
Delay timer	An approved electronic timing device generally used in conjunction with an exit device (REX/EDR) to delay “lock release” by no more than 15 seconds under normal operation but provides instantaneous release under fire or other agreed emergency conditions
Electromagnetic clamp lock	An electric lock which relies on a magnetic bond between the lock body and its corresponding armature plate.
Electromagnetic shear lock	An electric lock that relies on a combination of magnetic bonding and a mechanical restraint to prevent lock shear.
Electric mortise lock	An electric lock mortised into the door and with a cable transfer mechanism to carry the signal/power cabling between the frame and the lock.
Electric strike lock	An Electric lock fitted into the door frame and which acts as an electrically operated door latch keeper.
Electric drop bolt	An electrically operated solenoid which extends or retracts a metal bolt to or from its

	corresponding keeper which is generally mounted on the controlled door.
Electric “V” bolt	A motor driven locking mechanism that drives or retracts the securing PIN to/from a V shaped keeper.
Fail safe lock	An electric lock which releases when power is removed.
Fail secure lock	An electric lock which locks when power is removed.
Magnetic Bond Sense-MBS	Electronic circuitry which monitors the magnetic bond between an electromagnetic lock and its corresponding armature when in the locked mode.
Lock position switch	An electronic component to monitor the operational status of the electric lock solenoid. (active/inactive) – Normally a micro-switch
Door position switch	An electronic component to monitor the door position. (Open/closed) – Normally a magnetic reed switch.
Latch position switch	An electronic component to monitor the lock latch position. (Engaged/Disengaged) – Normally a micro-switch or magnetic reed switch.
Tower bolt monitor switch	An electronic component to monitor the tower bolt position. (Engaged/Disengaged) – Normally a micro-switch or magnetic reed switch. Generally associated with the inactive leaf on a set of double doors.
Token/Credential	The user interface with the access point control mechanism – Card, FOB, finger print, eye pattern, hand geometry etc.
Token/Credential Technology	A wide variety of technologies exist including:- Weigand, magnet stripe, bar code, infrared barcode, RF proximity, Smart card, Biometric etc
Head end equipment	The system’s main intelligence source containing system set up configuration and database. (E.g.; System server, master controller). This is the equipment where all system programming is conducted.
Door controller	The panel containing all hardware, firmware and power & signal interfaces to the door access control system components
Lift controller	The panel containing all hardware, firmware and power & signal interfaces to the lift system to provide electronic access to operate lift control buttons (lift lobby call button, in car floor select button) either in isolation or combination.
Intelligent controller	A controller that performs all of its programmed functions in the absence of the head end.
Operator workstation	The operators interface to the head end.

3 Information Dissemination

This Code of Practice provides general guidelines to Clients and installers of Electronic Access Control Systems. All installations shall comply with applicable laws and regulations as listed in 3.5 – All NZSA Members are expected to have this documentation in hard copy form and to be able to explain how this information is disseminated to staff and contractors.

4 General

4.1 Staff Registration

All staff engaged in security work shall be licensed in accordance with the Private Security Personnel & Private Investigators Act 2010 (& Amendments & replacements) and shall carry such registration when on business and show it to clients when visiting them. NZSA Members are expected to have this documentation on hand for audit referral.

4.2 Insurance

The amount of Professional Indemnity Insurance cover required of all NZSA members, engaged in any part of the design of an Access Control System, shall have due regard to the nature of the risk and the relevant standard but shall not be less than \$1,000,000. The policy shall be kept current for 5 years following the system handover.

4.3 Staff Training

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:-

1. A recognised NZQA qualification in the domain of Electronic Security or equal and equivalent through the process of “Recognition of Prior Learning/Experience” or
2. For the product being offered to each client, a manufacturers factory training course certificate that confirms successful course completion to the competency level expected;

For the purposes of this COP, in-house training courses are not recognised as an acceptable form of training unless the training course has been endorsed in writing by the product manufacturer (not importer or distributor). NZSA Members are expected to have a staff records file with all staff information up to date and available for audit inspection.

4.4 Courteous Behaviour

In the context of this code of practice, all staff visiting Clients 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 that Clients image of his/her company and the security industry at large. NZSA Members are expected to explain their QA programme around this requirement.

4.5 Related Standards and Legislation's

- a)AS/NZS 3000 Electrical Installations
- b)New Zealand Electricity Act 1992
- c)NZ Wiring Regulations 1976
- d)NZ Building Act 2004 and in particular, means of escape from buildings
- e)NZSA Codes of Practice
- f) NZ Health & Safety in Employment Act 1992
- g)NZS 4121:2001 Design for Access and Mobility

All NZSA Members are expected to have hard copies of the above for reference purposes and an explanation as to how they disseminate this information to staff and contractors.

4.6 Manufacturers Specification

- 1.All Access Control systems and associated equipment shall be installed within the limits of the manufacturers specification and conform to at minimum related New Zealand and joint standards.
- 2.A copy of the Manufacturers specifications for each product installed shall be kept on hand at the installers premises.

4.7 Security of Information

All members shall recognise that information on security systems is confidential and should be protected. Details of Access Control system shall not be divulged to anyone else 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 Police. NZSA Members shall demonstrate their methods of information protection to the auditor.

5 Access Control Objectives

The primary objective of Access Control is to:-

- Regulate entry into or from an area by mechanical key, punch code, electronic token or biometric means. For the purposes of this Code of Practice, mechanical devices are excluded)

5.1 Establishing the Clients Needs

It is essential to establish what the client expects from the system and how it is to be used. It is also essential that the Client be made aware of the cost and human resource requirements for system management and maintenance.

The Client shall be made aware of any proposed system limitations in the course of determining needs in order that they can make an informed decision. (For example, the limited number of system codes in 26 bit Weigand format cards, the likelihood of forced door alarms when using electric strikes in association with standard door hardware). All NZSA Members are expected to have a system's limitations check list that they discuss with Clients.

All limitations shall be documented and signed off by the Client as acceptable risks.

5.2 Security Risk as a factor in "System Design"

- a) "Security Risk" shall be a major influencing factor in the overall design of the electronic access control 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, property, personal safety and information each require to be considered in determining overall risk. Refer AS/NZS 4360; 2004 Risk Management. NZSA Members offering electronic access control solutions shall not overstate the "Security Risks" in order to sell more products.
- b) The client must be involved in determining system operational requirements and agree the areas to be controlled and at what times.
- c) 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.
- d) Clients shall be informed as to the limitations of having electronic access control as the sole means of providing facility security. The merits of having complimentary systems such as intrusion detection and/or CCTV Surveillance should be overviewed.
- e) Where integrated systems (electronic access, intrusion detection, CCTV etc) are offered, then the related COP for each system shall be adhered to.

6 System Design

6.1 Operational requirements

Operational requirements of the access control system shall:

1. Determine which doors/gates/grilles/barriers (access points) are to be controlled.
2. Determine the appropriateness of the access point(in terms of practical application and operational reliability) to have an access control system fitted (Example would be a door with ceiling void above into the controlled space)
3. Determine the appropriateness of lock selection with regard to door swing; door usage and emergency egress.
4. Determine the potential traffic through each access point to ensure appropriate equipment selection.
5. Determine the operational requirements for each access point
6. Identify need for door hold open devices and fire alarm release.
7. Identify the need for automatic door closers.
8. Identify the need for door closer coordinators.
9. Identify the needs for emergency override (emergency access and fire egress routes).
10. Identify the need for jemmy-bar protection devices and hinge bolts.
11. Identify the resources necessary for day to day system management.

6.2 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.

6.3 Fire Alarm Interface

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”

In some installations such as prisons, courts, forensic wards etc there is a requirement to have the locks fail secure to facilitate a staged evacuation if necessary. These special circumstances will require compliance certification from a registered “Fire Engineer”

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”.

6.4 Lift Interface

There are various forms of access control for lifts and Clients need to be aware of all basic forms.

1. Floor selection without destination reporting (low level – generally one credential presentation allows multiple floor selection – possible tail-gating)
2. Floor selection with destination reporting (High level – one credential presentation, only one floor selectable and reported – higher security but tail gating still possible. This may be achieved either through a hardware/firmware solution or total software solution)
3. Irrespective of which system is chosen, the lift emergency override has precedence over all security requirements.

6.5 System expansion

When designing a system, due consideration should be given to accommodate future extensions to the clients business and/or premises in the short or medium forecasts. The Client shall be made aware of recommended expansion options and all associated costs and benefits of early provision.

6.6 Scoping Paper for Client Direct Installations

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.
2. The Client maintains the right to have the Scoping Paper/Proposal peer reviewed before sign off.
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.
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 for separately.
5. The Scoping Paper/Proposal shall clearly set out a complete equipment schedule for the whole of the works including Client training and “As Built” documentation
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 involved with this process is mandatory.
7. All passwords on a Clients 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.
8. 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.

6.7 Equipment Selection

1. The primary driver for system design and hence equipment selection will be the type of token/credential to be used. Clients should be advised on what technologies are available, the pros & cons of the varying types and any specific site conditions or needs that would prohibit the choice of one technology over another.
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.

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 service risk.

6.8 Equipment Positioning

1. All equipment other than the access control point (lock cylinder, keypad, credential reader,) shall be located within the secured area and in accordance with manufacturer's recommendations.
2. Equipment locations shall ensure a safe working environment for servicing personnel and shall further ensure easy access for servicing.
3. The locating of equipment in areas with difficult access is strongly discouraged.
4. 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.

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

5. For safety reasons, REX and EDR devices shall be easily identified and located well beyond door opening in the direction of the REX/EDR
6. 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. Wherever possible, computer based equipment with hard drives shall be located in a controlled environment where the air temperature will be maintained between 19° C and 21°C. Where this is not possible, the Client should be made aware of operational risks.
8. Field equipment including door controllers, lift controllers and power supplies shall be located to ensure that operating temperatures are maintained within manufacturer's tolerances.
9. 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 System Installation

7.1 Wiring

1. Cable Installation and general wiring practice shall be in accordance with relevant clauses of the relevant Standards and Regulations. These Regulations apply to all installations connected with any source from which electricity is available, except for those exempted by the Regulations.
2. 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 in terms of ELV installations.
3. With modern systems having IP addressable system components, it is essential that all cable runs be installed to meet the limitation in networking cable distances. Where the Client has an IT specialist/department, close liaison for network design/connectivity is strongly recommended.
4. All cabling shall be supported on appropriate cable reticulation systems (conduits, trays, ducting, catenary wire) and shall not be laid directly on false ceiling.
5. All cabling shall be installed in parallel to the main building axis and not in a direct point to point configuration.

6. 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.
7. All cabling shall be selected as appropriate to the environment in which it is to be installed.
8. 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.

7.2 Equipment

1. All equipment installation shall be in accordance with the manufacturer's recommendation and shall comply with all safety aspects of the Electrical Regulations including safe earthing and safe isolation.
2. All equipment shall have an "Ingress Protection" rating (IP rating) appropriate to the environment in which it is to operate.
3. All control units/power supplies shall be in lockable, tamper monitored enclosures.
4. All power supplies shall maintain the connected load for not less than 8 hours (2 hours if there is a site generator) and.
5. Power supplies shall have mains fail and battery abnormal voltage health check monitoring which should be remotely monitored where possible.

8 Testing and Commissioning

8.1 Test Equipment

All systems test equipment shall be supplied by the installation company and shall include:-

1. Multi-meter
2. Pre-programmed valid card
3. Pre-programmed invalid card
4. Spare DPS magnet
5. Replacement EDR glass windows and reset tools
6. Laptop for programming (where required)
7. Printer or soft copy data capture device to off load system reports.

8.2 Commissioning Tests

The primary outcome of commissioning tests shall be to satisfy the customer that they have been delivered a system which meets their expectations as agreed under Section 4.

Provide a detailed set of commissioning sheets which covers all aspects of the system tests including head end equipment checks, all field equipment checks, local and remote monitoring checks and user training needs.

9 Requirements for Regular Maintenance

9.1 The System

- a) Make an inventory check of the system to ensure all components are present and 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) Note any environmental changes and the effects they have on the system.
- e) Using a valid card prove access granted. (all doors & lifts)
- f) Using an invalid card, prove access denied (all doors & lifts)
- g) For systems with intelligent controllers, interrupt the comms line and prove access granted/denied as above.
- h) Check that the automatic door closers operate 100% from both part open position and full open position (All doors)
- i) Prove that the DOTL (door open too long alarm) is fully functional (all doors).
- j) Confirm that there are no obstacles to emergency egress at any controlled access point (all doors)
- k) Confirm day-light savings is set to auto-update and has been programmed accordingly.
- l) Confirm that door forced alarms are generated under the forced door condition (all doors).
- m) Confirm that there is a **mechanical** means to access the system controllers to manually operate doors in the event of a serious system malfunction.
- n) 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 updated at the agreed frequency of the back-ups. Confirm with the Client a system back-up schedule.
- o) Confirm that all time controlled schedules are automatically updated for programmed holidays.
- p) 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.
- q) 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 tests performed.
- r) 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.
- s) For all installed systems, the Client should be offered a maintenance contract option either as fully comprehensive (all parts and labour included) or preventative & response (fixed portion plus response & parts). It is the Clients prerogative to decline but declination has risk factors that should be discussed with the Client.

10 Audit Check List

Clause	Topic Summary	Mandatory	Recommended	Evidence
1	Glossary of Terms	-	Yes	
2	Information Dissemination to staff	Yes		
3	General	-	-	
3.1	Staff registration under Private Security Personnel & Private Investigators Act 2010 (& Amendments & replacements)	Yes		
3.2	PI Insurance – Systems design requirement	Yes		
3.3 (1)	Staff training – NZQA qualifications	-	Yes	
3.3 (2)	Staff training –Manufacturer’s training	Yes		
3.4	Courteous Behaviour and checking	Yes		
3.5 (a)	AS/NZS3000 wiring rules – Related sections	Yes		
3.5 (b)	NZ Electricity Act	-	Yes	
3.5 (c)	NZ Wiring Regulations	-	Yes	
3.5 (d)	Building Act – Egress compliance	Yes		
3.5 (e)	NZSA – COP’s compliance	Yes		
3.5 (f)	Health & Safety; Obligations/responsibilities	Yes		
3.5 (g)	Access & Mobility-Related sections	Yes		
3.6	Manufacturers Specification	-	-	
3.6(a)	Compliance with manufacturers instructions	Yes		
3.6(b)	Manufacturers instructions available	Yes		
4	Objectives	Yes		
4.1	Client needs are established	Yes		
	System limitations are explained	Yes		
4.2(a)	Security Risk factored as design basis	Yes		
4.2(b)	Operational needs set with Client	-	Yes	
4.2(c)	System defaults explained to Client	Yes		
4.2(d)	System limitations explained to Client	Yes		
4.2(e)	COP adherence for each integrated element	Yes		
5	System Design	-	-	

5.1.1	Control points logically determined	Yes		
5.1.2	Control points deemed appropriate	Yes		
Clause	Topic Summary	Mandatory	Recommended	Evidence
5.1.3	Lock selection appropriate to application	Yes		
5.1.4	Lock selection fit for purpose	Yes		
5.1.5	Operational requirements determined	Yes		
5.1.6	Door hold open devices considered		Yes	
5.1.7	Auto-closers fitted		Yes	
5.1.8	Door co-ordinators considered		Yes	
5.1.9	Emergency access/egress override included	Yes		
5.1.10	Anti-Jemmy bar plates/hinge bolts included		Yes	
5.1.11	System Management resources defined	Yes		
5.2	Day to day business operations unhindered	Yes		
5.3	Compliant Fire alarm interface in place	Yes		
5.4	Client advised on lift control options	Yes		
5.5	Allowances made for system expansion		Yes	
5.6	Scoping paper for Client Direct Install	-	-	
5.6.1	Scoping paper defines operational needs		Yes	
5.6.2	Peer review of scoping paper accepted		Yes	
5.6.3	Responsibility remains with designer	Yes		
5.6.4	Scope of works defined	Yes		
5.6.5	Equipment schedule defined	Yes		
5.6.6	Client engaged in defining parameters	Yes		
5.6.7	Client in control of system password		Yes	
5.6.8	System components are Client property	Yes		
5.7	Equipment Selection	-	-	
5.7.1	Credential options are explained		Yes	
5.7.2	Resource requirements are explained	Yes		
5.7.3	Service options are explained	Yes		
5.8	Equipment positioning	-	-	
5.8.1	Head end equipment in secure location		Yes	
5.8.2	H&S a factor in location selection		Yes	
5.8.3	Difficult access to equipment is avoided		Yes	
5.8.4	Access readers appropriate to environment		Yes	
5.8.5	Equipment location avoids possible injury	Yes		
5.8.6	Equipment on secure side not compromised	Yes		
5.8.7	Operating environment appropriate to risk		Yes	

5.8.8	Operating temperatures are controlled		Yes	
5.8.9	Locks not compromised from unsecured side	Yes		
Clause	Topic Summary	Mandatory	Recommended	Evidence
6	System Installation – Wiring & Equipment	-	-	
6.1	Wiring	-	-	
6.1.1	Compliance with rules and regulations	Yes		
6.1.2	Familiarisation with AS/NZS 3000	Yes		
6.1.3	Network cabling installed to best practice	Yes		
6.1.4	Reticulation systems appropriate to need		Yes	
6.1.5	Cable routes parallel to building axis		Yes	
6.1.6	C of C issued for 230v connection	Yes		
6.1.7	Cable selection appropriate to environment	Yes		
6.1.8	Circuit segregation - AS/NZS 3000 comply	Yes		
6.2	Equipment	-	-	
6.2.1	Manufacturers guidelines followed	Yes		
6.2.2	Appropriate Ingress protection applied	Yes		
6.2.3	Tampered enclosures used		Yes	
6.2.4	8 hour standby power provided		Yes	
6.2.5	Power supply health check monitored		Yes	
7	Testing and Commissioning	-	-	
7.1	Test equipment	-	-	
7.1.1	Multi-Meter		Yes	
7.1.2	Pre-programmed valid card		Yes	
7.1.3	Pre-programmed invalid card		Yes	
7.1.4	Spare DPS magnet		Yes	
7.1.5	Replacement EDR glass & reset tool		Yes	
7.1.6	Laptop		Yes	
7.1.7	Printer/Flash drive		Yes	
7.2	Commissioning Tests	-	-	
7.1.1	Detailed commissioning sheets are available	Yes		
8	System maintenance	-	-	
8.1	Maintenance check list reflects all items as listed under this section of the COP	Yes		

Additional Remarks:

Auditor Signature: _____

Date: _____

For the Company:

Name: _____ **Signature:** _____ **Date:** _____