Disaster, Emergency and School Security

Electronic security guidelines

Queensland Government

Contents

Introduction 4

General requirements 5

Procedures and standards 5

Quotations 6

Testing, commissioning and documentation 7

New school builds vs additional new facilities 9

Intruder detection systems 10

Intruder alarm monitoring 10

System requirements 10

Types of detection 16

Reed switches 20

Sirens 20

Duress buttons 20

System integration 21

Auxiliary inputs 21

System configuration and programming 22

CCTV 26

General requirements 26

Cameras 26

Recording and monitoring 27

Network and infrastructure 28

Physical installation 29

Electronic access control 31

General requirements 31

Cabled/integrated systems 31

Wireless systems 34

Occupant warning systems 35

General requirements 35
Network requirements 35
Speaker location/output 36
System capability 36
Components 37
Definitions 38
Appendix A: Intruder detection system commissioning checklist 40
Appendix B: School security site commissioning checklist 42

Introduction

This document has been developed by the Queensland Department of Education (DoE), to outline the minimum requirements for hardware and installation of the following at schools:

- Intruder detection systems;
- Closed circuit television (CCTV);
- Electronic access control; and
- Occupant warning systems (OWS).

The guidelines apply to the construction of new school sites and upgrades to electronic security systems at existing schools. They are designed to provide schools with security options that are:

- effective in mitigating the most commonly identified security risks at schools;
- suitable for normal operations;
- simple to use; and
- cost-efficient to install and maintain.

Schools with existing, functional security systems are not required to immediately replace or alter these in order to comply with these guidelines, except where they are in contravention of the conditions outlined in DoE's School security procedure or CCTV use in schools procedure.

Specifically, Concept 3000/4000 and Tecom Challenger v10 controllers are not suitable for new intruder detection systems installations and upgrades. These panels are currently installed at some schools and will continue to be eligible for monitoring until further notice. See Intruder detection systems below for more information.

Schools should include upgrading/replacement of electronic security systems to the standards noted in this document as part of their ongoing maintenance and network capacity planning.

For information about:

- requirements for general power outlets (GPOs) to support security systems; or
- fire alarm panels, emergency warning and intercommunication systems,

refer to the current Design standards for Department of Education facilities.

General requirements

Procedures and standards

Any installation of electronic security systems at schools must be undertaken by providers who can produce copies of current:

- Queensland electrical contractor licence;
- Queensland security provider licence: Individual class 2 (security equipment installers);
- Australian Cabler Registration Service Master cablers registration (open); and
- Technical certification for the security equipment being installed.

All works to install or maintain electronic security systems are to be completed to the relevant manufacturer requirements and compliant with:

- AS2201: Intruder alarm systems;
- AS3000: Electrical installations (wiring rules);
- AS/CA S008: Requirements for customer cabling;
- AS/CA S009: Installation requirements for customer cabling (wiring rules);
- AS62676: Video surveillance systems for use in security applications;
- Telecommunications cabling provider rules 2000;
- the latest version of the Design standards for Department of Education facilities;
- the latest version of the Departmental network infrastructure procedures and standards (DNIPS);
- requirements of Working on Department of Education facilities; and
- DoE's Asbestos management procedure and Asbestos incident management procedure.

Electronic access control may be integrated with an intruder detection system to achieve optimal operating outcomes, but CCTV and occupant warning systems must not be integrated to any other systems, and must operate independently.

Electronic security systems are not to be connected via an active network link to any other DoE equipment and shall not utilise the school's ethernet network connection to transmit or store data, or communicate with any source or destination (more information below).

Quotations

Quotations for electronic security systems are to include:

<table>
<tr><th>System</th><th>Quotation requirement</th></tr>
<tr><td>General</td><td>• Pre-start site meeting;
• Documentation of site-specific requirements;
• Handover documentation and user training ;
• Types and quantities of equipment; and
• Labour and travel as individual amounts.</td></tr>
<tr><td>CCTV</td><td>At least two options for system components from:
<table><tr><th>Cameras</th><th>NVRs</th></tr><tr><td>Vivotech;
Bosch;
Axis; or
equivalent as detailed in the Cameras section below.</td><td>Vivotech;
Bosch;
Axis;
Avigilon; or
equivalent as detailed in the Recording and monitoring section below.</td></tr></table></td></tr>
<tr><td>OWS</td><td>• Commissioning and initial sound check.</td></tr>
</table>

Testing, commissioning and documentation

On completion of installation works, the installer is to complete the tests, training, commissioning and documentation outlined below. Documentation is to be provided to the school and relevant project manager.

System	Testing and commissioning	Documentation	Training
Intruder detection systems	• Scheduling of testing and commissioning with PSG (48 hours notice required). • Testing and commissioning of each input and area with PSG.	• Validated commissioning report from onsite computer. • Validation from PSG. • PSG Client and Technical monitoring forms. • Signed, completed alarm system training certification form and Intruder detection commissioning checklist (see Appendix A).	• Authorised staff must be inducted to the system, complete training and certify that training has been received.
CCTV	• Ensure fields of view and focus are set correctly for each camera during day and night time conditions. • Test camera live view, playback and the export of footage functionality.	• Camera positions and images of view captured by each camera. • Networked Video Recorder (NVR) and monitoring station location. • User manuals. • Signed, completed CCTV training certification form.	• Training for appropriate school personnel demonstrating system operation, playback and transfer of footage to media storage. • Authorised staff must certify that training has been received.

System	Testing and commissioning	Documentation	Training
Electronic access control (where applicable)	• Walk through testing of site and approval of any programming by relevant staff and school security advisor.	• Signed, completed electronic access control training certification form. • User manuals.	• Authorised staff must be inducted to the system, complete training and certify that training has been received.
OWS	• Ensure all aspects of the systems are functioning correct. • Volume/sound check.	• Signed, completed certification form. • User manuals.	• Authorised staff must be inducted to the system, complete training and certify that training has been received.
General	• Ensure coverage of each system is to the satisfaction of the school's Business Manager/Principal. • A full commissioning of each system is to be carried out, attended by the installer, project manager and school representative.	• Documentation of site-specific requirements.	• As above.

New school builds vs additional new facilities

The following are to be installed for new school builds:

- Intruder detection system that covers all blocks/areas as outlined in Intruder detection systems below;
- CCTV that covers all areas of the campus as outlined in CCTV below;
- OWS that covers all areas of the campus as outlined in Occupant warning systems below; and
- Electronic access control if applicable (any proposed requirements to be determined in consultation with Disaster, Emergency and School Security (DESS).

The following are to be installed at new facilities or upgrades at existing schools:

- Intruder detection system with main controller installed in admin building which covers, at a minimum, the new facility and admin (if not already covered);
- CCTV with NVR, back up/redundancy NVR and monitoring station which covers, at a minimum, the new facility;
- Expansion of and connection to any pre-existing OWS; and
- OWS and electronic access control if applicable (any proposed requirements to be determined in consultation with DESS).

Upgrades should be considered from a holistic perspective, ensuring that new security infrastructure is capable of being integrated into existing security systems, noting that upgrades to controllers maybe required.

Intruder detection systems

Intruder alarm monitoring

As part of DoE's partnership with the Queensland Police Service, Protective Services Group (PSG), intruder alarm systems are to be connected to PSG for monitoring. Technical forms can be obtained from PSG. Client information and dispatch procedure forms can be found on OnePortal.

System requirements

Installation of a new or upgraded electronic intruder detection system must include provision of all necessary equipment, materials, installation and commissioning of the following:

- one single and unique controller, e.g T4000 (4G) with serial cabling;
- a local area network (LAN) communications system utilising the school's fibre optic network via fibre modems;
- power supply equipment including battery back-up for the entire system and surge protected GPOs;
- expander modules in each building as required for inputs to report to a single reporting system;
- internal keypads;
- external keypads;
- internal sirens;
- Intruder detection devices;
- fixed, non-latching, dual press duress buttons;
- fire hydrant and hose reel water flow switches, fire pump alarms and fire indicator panel connection. Systems are not to directly monitor smoke or fire detection devices. These devices must be monitored by a dedicated fire indicator panel (FIP), with two outputs from the FIP (alarm and fault status) being monitored by the intruder detection system;
- new workstation supplied and installed with system administration software e.g. Integriti Professional for Inner Range Integriti;
- site specific technical manuals;
- system logbook;
- manufacturer's operator manual;
- Ttaining of nominated personnel and enrolment for monitoring with PSG;

- UniBus UART with required cabling; and
- Hi-gain antenna if required for adequate communication. Communications, signal attenuation and propagation and processing delays are not to exceed the manufacturer's specifications.

The contractor is to:

- connect a workstation with the control panel and ensure that the panel can be updated via the workstation and remotely by PSG;
- test communications with the Protective Services Central Operations Room. Contractor to ensure all technical and client forms are completed and submitted no less than 48 hours prior to commissioning with PSG;
- obtain a completed validation report from PSG is to be submitted as part of the commissioning process; and
- map any existing alarm system and update programming and firmware if required.

Cabling and power supply components are to be installed in accordance with the Design standards for Department of Education facilities.

System firmware

All security system components are to be supplied and fitted with the manufacturer's latest firmware version at the time of installation. System firmware is to be suitable for the purposes of:

- system operation as specified in this document;
- local administration using the software; and
- monitoring by PSG.

Optional functions

Where there exists a specific purpose or requirement to mitigate identified risks, an intruder detection system may also have equipment installed and programming to monitor:

- wireless, dual press duress pendants;
- audio sonic break glass detection;
- photoelectric beams; and
- wireless links (for remote intruder detection devices).

Where any of the above are proposed to be installed to mitigate specific identified risks, assistance should be sought from DESS before installation.

Network requirements

Controller expander modules are to utilise the school's optical fibre network for LAN for inter-building communications. Where access to the fibre network is not available, LAN isolator units and LAN transient protection should be included, as required.

Intruder detection equipment shall not be connected via an active network link to any other DoE equipment and shall not utilise the school's ethernet network connection to transmit or store data, or communicate with any source or destination. Fibre modems are recommended by system manufacturers must be installed for system communication.

Optical fibre modems shall be used to convert between suitable LAN communications media. The type of the optical fibre modem used shall suit the type of fibre installed. Only optical fibre modems which are produced by the alarm system manufacturer shall be used.

Power over ethernet (PoE) switches are not to be used for communication of the intruder detection system, unless required as part of a wireless link configuration.

Fibre modems can be wall mounted. Where blocks require new expander modules, the fibre modem is to be installed within the expander module enclosure, ensure the enclosure size is adequate to house 32 inputs, auxiliary equipment and fibre modem.

For new installations, no copper cabling is to be used between blocks. For existing site upgrades in buildings without fibre connection, assistance with evaluating copper and/or wireless connection options should be sought from the School Security Advisor at DESS.

Contractors are to investigate the school's current networking infrastructure to ensure there are adequate fibre pairs and communications cabinet space available in each block. The contractor is to liaise with ICT SS Design Services (formerly Network Design) network.design@qed.qld.gov.au for review if there are not adequate fibre cores or cabinet space, and include the include the costs of additional fibre or cabinet related works in quotes if determined by ICT Design Services to be required.

Main controller

To allow for alarm monitoring under DoE's agreement with PSG for security services, installations and system upgrades should have one of the following controllers:

- Inner Range Integriti;
- Tecom Challenger Plus (monitoring only, remote programming is not possible); or
- Paradox MG Series/SP6000+ (only to be considered for schools with a maximum of two blocks and 16 inputs) (monitoring only, remote programming is not possible).

Any school/Project Manager proposing to install an alternative system to those listed above should seek advice from DESS before installation.

Where possible, the controller is to be located in the same space as the school's Centre of Network (CoN). The controller must report via connection to a manufacturer approved general packet radio service (GPRS) unit. The GPRS unit is to be for the exclusive use of the alarm system and not shared with any other device. The GPRS unit is to have capacity for two 4G SIM cards, and be installed equipped with both Telstra and Optus connected 4G SIM cards.

Unless prior approval is gained from DESS, a single, unique controller is to be installed. The controller is to meet the following minimum requirements:

- Uniquely identifiable to the PSG Control Room by a single client code; and
- Capable of supporting the number of intruder detection inputs as detailed on the Scope of Works.

Each input shall be capable of being:

- individually identifiable as a number and name using the administration software or any system keypad;
- individually supervised and capable of monitoring and reporting SECURE, ALARM and TAMPER conditions;
- individually selected for testing using the administration software or any system keypad to display each of the above conditions;
- individually selected for isolation using the administration software, onsite keypad and remotely by PSG Central Operation Room so that secure alarm and tamper conditions can be excluded from processing by the system;
- Support the required number of intruder detection areas. Areas shall be capable of being:
    - Armed or disarmed under one instruction, individually or in a group;
    - Individually programmed for separate entry and exit delay times;
    - Individually programmed to allow any number of inputs to be grouped into the area;
- Support the required number of system keypads;
- Support the required number of access control doors. Each door is to be:
    - Individually identifiable as a number and name using the administration software or any system keypad;
    - Individually supervised and capable of reporting DOOR FORCED, DOOR AJAR (DOOR OPEN TOO LONG) and TAMPER conditions (as a minimum);
    - Capable of uniquely recognising and handling a suitable amount of individual PIN codes or access control cards, based on the operational requirements of the site, allowing for a contingency for future use;

- Capable of uniquely identifying each PIN user or cardholder by both their first and last name in a 16-character (minimum) text string;
- Capable of reporting all the conditions detailed from all equipment and devices using the communications format specified in the supplied scope of works;
- Capable of allowing all programming to be performed and all system operations to be controlled both:
  - locally at the controller;
  - at any keypad; or
  - by using the manufacturer's specific administration software; and
  - remotely over the GPRS unit through the software package used by PSG (Integriti modules only).
- able of storing a retrievable event history;
- capable of temporarily isolating inputs. The system is to be programmed to default to automatically re-enable any isolated inputs on the opening of an associated area to avoid inputs to remaining isolated indefinitely;
- fitted with a 12V DC 7.5Ahr back-up battery to permit full system operation in the event of mains power failure for a minimum of 4 hours;
- supplied with a suitable firmware version;
- fitted with a dual port (minimum), FS232 interface for the connection of a system computer; and
- supplied with the maximum possible memory expansion option.

Expander modules

Manufacturer specific expander modules are to be installed as necessary to meet the requirements of the site being covered.

Only 16 or 32 input system expander modules are to be installed for school blocks. When upgrading an existing system that is expanding to established modular blocks an 8 input expander module may be considered (more information below).

The number and location of system expander modules is to allow for efficient cabling, connection and operation of the system with an absolute minimum of externally run detector cabling.

Expander module power supply is to be by separate surge protected GPOs with labelling as required by the Design standards for Department of Education facilities.

Locations of expander modules are to be assessed in accordance with any known future school developments and facilitate system expansion in the future, but should be installed in a secure data

room covered by intruder detection. In buildings where a data room is not present, the expander module should be installed in a closet, storeroom or withdrawal room ensuring it can be secured and safely accessed by service technicians.

Expander modules are to be wall mounted in accordance with the manufacturer's instructions and installed between 1500mm and 2100 above finished floor level (AFFL).

Where an expander module is installed adjacent to a main controller or another expander module, there is to be a minimum distance of 100mm between equipment.

Expander modules are to be fitted in a metal enclosure equipped with a 2amp power supply and 7.5Ahr battery.

Inner Range mini expander modules

Mini expander modules:

- can only be used in demountable buildings, grounds equipment storage and other sheds;
- are not be used in any building or shed where more than 5 detection inputs are required; and
- are to be capable of direct connection for onboard tamper input, low battery and AC programmable through systems inputs.

Tecom 4 input DGP

Tecom 4 input DGPs are not to be used.

Keypads

Manufacturer specific LCD keypads are to be installed for onsite arming and disarming of the intruder detection system.

All keypads should be identical in appearance and function.

Each keypad is to be equipped with an internal tamper to detect attempts to forcefully open a keypad or remove a keypad from its mounting surface.

System design should aim to have no more than 8 keypads in total over a standard state school/high school campus, or 16 at P-12 colleges.

At a minimum, keypads should typically be installed in the following locations:

- Internal administration – adjacent to the main entry (mandatory);
- External administration (mandatory);
- External hall or performing arts block;
- External facilities shed;

- External canteen; and
- Staff rooms.

Where additional keypads are required for normal school operations, assistance should be sought from DESS.

Internal keypads

Internal keypads are to be installed within 5 metres of the main entry, mounted at a height of 1200mm AFFL, securely fixed to a flat surface.

Internal keypads should feature a programmed exit delay of 30 seconds when armed in the area in which the keypad is located.

External keypads

External keypads should be installed at the administration block and the hall. Additional external keypads are to be installed as required for normal school operations.

External keypads are to be installed in a steel protective enclosure wall box, with the following features as a minimum:

- IP66 protection rated enclosure fitted with a cylinder lock or secure latch to allow for a padlock, keyed to the school's master key system. All keypad enclosures on site are to be keyed alike; and
- a tamper switch must be installed to detect attempts to remove the enclosure from its mounting surface via extension of the keypad's integral tamper switch.

In high-risk locations, a tamper switch (connected to a dedicated input so that each device can be individually addressed in system programming) may be required for external enclosures. Advice should be sought from DESS before installation.

Types of detection

The table below outlines the standard for detection devices based on room or area type. Assistance for proposed exceptions to the below should be sought from DESS.

Block	Room/area type	Device
Administration	Resource and photocopy rooms, meeting rooms, interview rooms, offices, staff room, store rooms (with windows).	Motion detection
	Data rooms, secure store rooms (no windows).	Reed switch Motion detection
	Reception, cash counter.	Motion detection

Block	Room/area type	Device
		Duress button/s
Prep	General learning areas, practical learning areas, store rooms (with windows), preparation areas, withdrawal rooms, offices, staff rooms.	Motion detector
	Storage area (no windows) external doors.	Reed switch
General teaching and special education	All offices, classrooms, staff rooms, teacher preparation areas, resource stores, computer room, withdrawal rooms, wet/dry areas.	Motion detection
	Secure store rooms, AV equipment storage.	Reed switch
Music	Offices, classrooms, preparation areas.	Motion detector
	Instrument store rooms.	Reed switch
Resource/library	Reading areas, book shelving, resource stores, computer areas, audio/visual rooms, loans desk area, teacher preparation areas, all offices, staff rooms, work rooms.	Motion detector
	Secure store rooms.	Reed switch
Canteen	Serving areas, preparation areas, uniform storage and sales, stationery storage and sales.	Motion detector
	Servery counter shutters.	Dual reed switch
	Money handling areas.	Motion detector Duress button
Hall	Staff rooms, sports equipment storage, AV equipment storage, lighting equipment, kitchens.	Motion detector
	Fire doors and roller doors.	Dual reed switch
Manual arts	All offices, classroom, staff rooms and workshops.	Motion detector
	Secure stores, spray paint booths, flammable liquid stores.	Reed switch
Performing arts	All offices, classrooms, staff rooms, AV equipment storage, preparation areas, lighting equipment.	Motion detector
	Box office, money handling areas.	Duress button
Home economics	All offices, classrooms, staff rooms, kitchens, food and equipment storage areas.	Motion detection

Block	Room/area type	Device
Commerce	All offices, classrooms, staff rooms, computer rooms.	Motion detector
	Secure stores.	Reed switch
Art	All offices, classrooms, staff rooms, paint and equipment storage, media/graphics rooms, darkrooms.	Motion detector
Sciences	All offices, classrooms, staff rooms, AV equipment storage, preparation rooms, chemical storage.	Motion detector
Staff rooms	All offices, classrooms, staff rooms.	Motion detector
Ancillary staff	All offices, store rooms, workshops.	Motion detector
	Chemical/fuel stores.	Reed switch
Agricultural unit	Staff rooms workshops.	Motion detector
	Grounds equipment sheds and chemical/fuel stores.	Reed switch
Swimming pool	Canteens.	Motion detection
	Plant room, chemical stores.	Reed switch
Shed (facilities)	Equipment/storage area.	Motion detector
	Shed entry/roller doors.	Reed switch
Shed (general use)*[1]	Physical education storage, grounds equipment storage, prep storage.	Reed switch

Motion detectors

Minimum requirements:

- Wide angle 12m range;
- Dual element mirror optic;
- Mounting height capacity up to 4.9m.

Motion detectors are to be programmed with LED indicator lights activated.

Dualtech detectors

Minimum requirements:

[1] Motion detection may be required in sheds where there are windows or items of high value stored in the area. Advice should be sought from DESS before installation.

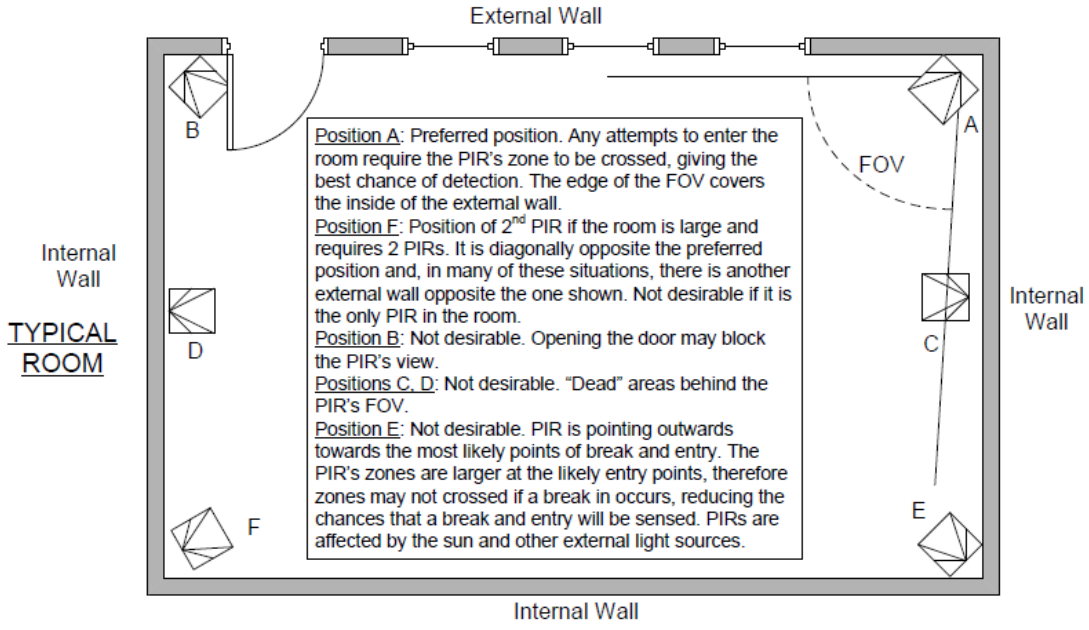
- Tritech, PIR and microwave movement detector;
- Microwave noise adaptive processing;
- 90-degree field of view;
- 12m coverage area; and
- Mounting height capacity up to 4.9m.

Position of detectors in offices, classrooms

Detectors must be positioned so that optimal protection is provided for the specified location with full coverage of all possible entry and egress points while causing minimum interference to activities within the location.

In general, detectors should not be installed within:

- 30cm of any window which can be opened;
- 40 cm of any air-conditioning or forced air ventilation supply or return opening; or
- 40cm from the blades of any ceiling fans.



Where ceilings:

- are angled/curved etc., PIR are to be mounted horizontally with a wall mount or angled bracket from the ceiling;
- have low strength/stability, PIRs are to be mounted to a steel/aluminium plate, which is to be fixed to the ceiling support frame;
- have external support trusses and beams, PIR to be installed below.

Reed switches

Minimum requirements:

- Contact: NC, SPST;
- Rating (max):10W;
- Voltage (max): 100V DC;
- Current (max): 500mA;
- Reed: epoxy sealed.

Sirens

Minimum requirements:

- Sound level: 105dB/m;
- Voltage: 12V DC;
- Current: 110mA;
- Sirens are to be installed internally ceiling mounted and centrally located within the room;
- Sirens are not to be installed adjacent to motion detectors;
- Sirens are not to be secured to suspended ceiling T-Bar frames. Where the ceiling is suspended tiles, the siren is to be screw fixed to the centre of the tile (in accordance with DoE requirements for ACM management);
- Each siren is to be connected to an individual relay, with the relay connected to a separate and individual output on the controller or expander module;
- Sirens are to be configured to operate for no more than 2 minutes on each alarm activation;
- Piezo top hat sirens should be installed;
- External sirens should not be installed as part of a standard intruder detection system. Where a specific purpose for external sirens is identified, advice should be sought from DESS before installation.

Duress buttons

Fixed, non-latching dual press duress buttons must be located to minimise the likelihood of false alarms and to ensure ease of use.

Duress buttons must be installed at reception desks in a school's administration area and any location where money is stored or handled. This may include canteens, multi-purpose hall kiosks or uniform shop points of sale.

In each building containing a duress button where staff areas lead to a public facing foyer area, a single dedicated, silent internal strobe must be installed and positioned to:

- alert staff in other areas of a duress activation allowing them to either shelter in place or provide assistance; and
- avoid escalating incidents by advertising the duress activation to an aggressor.

The strobe shall operate for a set period of 5 minutes.

System integration

Where lighting, air-conditioning management, or high temperature alarms are to be integrated with the intruder detection system:

- the controller and each expander module are to be fitted with 1 relay for each interfacing system;
- the relay shall switch either a “dry contact” or 12V DC output, programmed to change states when the alarm area associated with the respective building/block is area or disarmed; and
- the contractor is to provide cabling from this relay to the relevant service control panel or relay.

Auxiliary inputs

Fire indication panels/fire pumps

If a fire indication panel (FIP), sub-indication panel (SIP) and/or fire pumps are to be monitored, an auxiliary output or relay providing a “dry contact” is to be used to interface with the intruder detection system.

Monitored fire pumps should have outputs for RUN, FAULT and ISOLATE status.

Cabling and connection is required from the contact to an individual input on the associated controller or expander module.

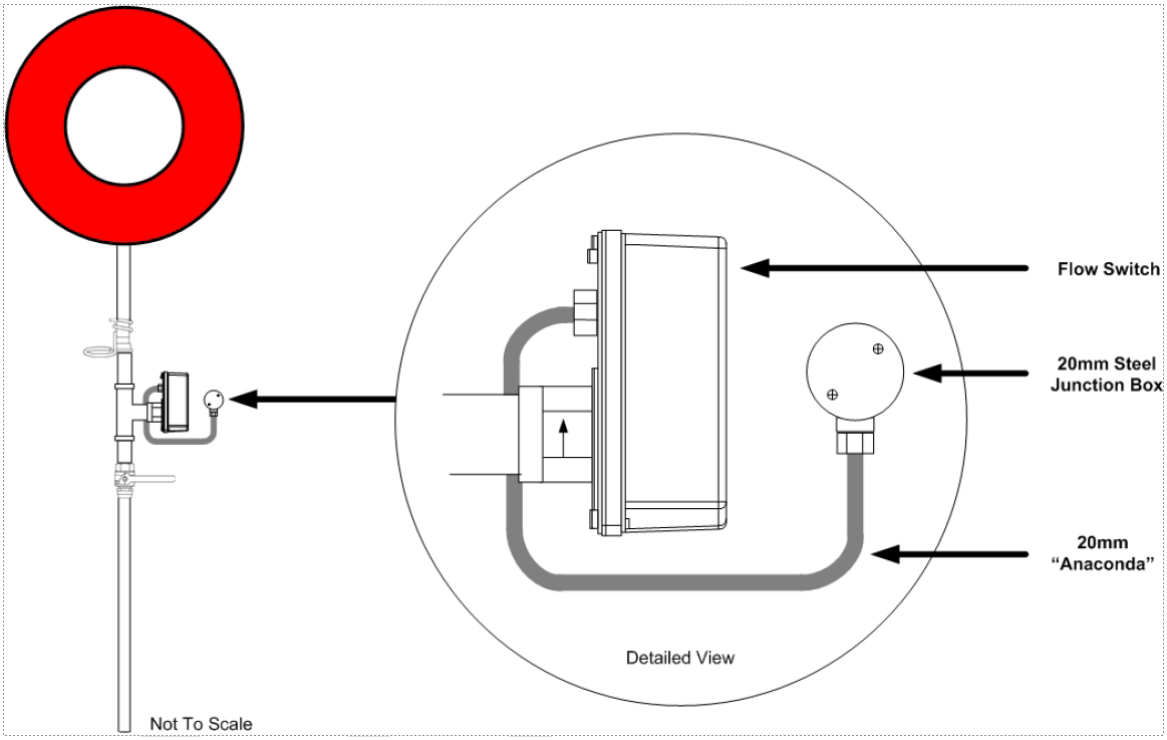
Fire hose reel flow switches

Flow switches, fitted with an approved tamper are to be installed on fire hose reels.

Cabling to the flow switch is to be concealed within 20mm sold screwed steel conduit where exposed, converting to a steel junction box and flexible steel conduit terminating at the flow switch.

Conduits are to be adequately fixed to mounting surfaces with galvanised, double-sided saddles.

Matching steel and waterproof flexible conduits fittings are to be used throughout.



System configuration and programming

Inputs

Each input is to be individually defined with a unique name which clearly and unambiguously identifies the location and type of the connected security device. Identical input identification names cannot be used.

The identified location of the security device is to match the location's final identification name and number.

Programming detail must not be subjective or open to interpretation.

Acceptable identifications align with the convention "room, block, device type", for example: *A07 Admin office PIR.*

All communicated input events are to be logged to the system's event history memory and computer interface.

All other functions as to be performed as outlined in the table below:

Device type	Status	Sound area siren	Keypad message
Intruder detectors	Alarm	Yes	Yes
	Restore	No	No
	Tamper	No	Yes

Device type	Status	Sound area siren	Keypad message
Duress	Alarm	No	Yes
	Restore	No	No
	Tamper	No	Yes
Connected fire alarm system	Alarm	No	Yes
	Restore	No	No
	Tamper	No	Yes

System input functions are to be performed as per the table below:

System input	Status	Sound area siren	Keypad message
Monitored system points	Alarm	No	Yes
	Restore	No	No

User programming

Each user is to be individually defined with a unique name which clearly and unambiguously identifies the user with both first and last names. Identical user identification names cannot be used.

A minimum 4-digit personal identification number (PIN) is to be assigned to each user. The system is to be programmed to permit users access to the functions and abilities as detailed on the following table on entry of the associated PIN at any system keypad.

User type	Functions	Abilities
Installer	All functions	All abilities
Master code	Turn areas on/off Review events Program users Isolate inputs System testing Adjust system time	Multiple area on/off Access to all areas Force isolate on exit Turn off all sirens Acknowledge messages Enable/disable tampers
User	Turn areas on/off	Single/multiple area on/off Access to intruder areas as required

The installer code is not to be distributed to anyone except PSG.

The master code is not to be issued to any user as a personal PIN code. It is to be used only for system administration by school staff allocated as system coordinators. The manufacturer's default master/installer user codes are to be changed in alarm systems following commissioning.

Communications programming

Systems are to report the following conditions:

Input	Alarm/Restore from alarm Tamper/Restore from tamper Isolated/de-isolated (including by user number or event)
Intruder detection area	Armed/disarmed (including by user number or event) Enable/disable processing of tamper alarms
24 hour armed area (system, duress, fire etc.)	Armed/disarmed (including by user number or event) Enable/disable processing of tamper alarms Area should be armed warning
Main controller	Cabinet tamper/restore from tamper External siren tamper/restore (where used) Mains failure/restore from failure Low battery LAN fuse failure Detector fuse failure Battery test failure Single weekly time report between 0001-0500 Module substitution
Keypad	Cabinet tamper/restore from tamper Too many code attempts Communications failure Duress alarm
Expander module	Cabinet tamper/restore from tamper

	External siren tamper/restore (where used) Mains failure/restore from failure Low battery LAN fuse failure Detector fuse failure Battery test failure Communications failure
Intelligent door controller	Cabinet tamper/restore from tamper Mains failure/restore from failure Low battery LAN fuse failure Detector fuse failure Communications failure Door forced open (per door) Door lock tamper (per door) Door open too long (as required)

CCTV

For information about where CCTV can be installed, school responsibilities for management of CCTV and how footage can be collected and shared, refer to the CCTV use in schools procedure.

General requirements

All CCTV equipment is to be installed in accordance with AS 62676: Video surveillance systems for use in security applications and AS 3000: Electrical installations (wiring rules).

CCTV systems in schools are to record to a network video recorder (NVR), or locally hosted standalone server with video management software in place, via internet protocols (IP) on ethernet fibre. Cloud based systems are not to be installed.

CCTV systems can utilise existing spare fibre backbone cores in the school's data racks to facilitate a direct physical connection between blocks.

CCTV equipment is not to be connected via an active network link to any other department equipment and shall not utilise the school's ethernet network to transmit or store data, or communicate with any source or destination. Separate rack mountable PoE switches must be installed for CCTV. More information about network infrastructure requirements is outlined in Network and infrastructure below.

CCTV systems must include only fixed cameras. Pan tilt zoom system controls are not permitted.

DNIPS compliant Cat6A network points are to be installed for cameras where there are no existing spare network points. Orange coloured Cat6A patch leads of the matching cabling manufacturer are to be used.

Where systems are expanded, or existing cameras are being integrated to a new system, all cameras are to be migrated to record to a compatible NVR and redundancy recorder system wherever possible.

CCTV systems are not to have remote, online, or app-based access, or any audio capturing functions enabled.

Cameras

Cameras are to be installed above 2400mm and below 5000mm above AFFL. Where this is not possible, cameras should be under the surveillance of at least one other camera wherever possible. All cameras installed lower than 2700mm AFFL are to have a vandal protection level of IP67/IK10 or equivalent.

Cameras are to have inbuilt alarm trigger options for motion detection and tamper alarm.

Cameras are to be set to record a minimum of 12.5 frames per second (fps) on motion, and continuously at a minimum of 2.5 fps.

Cameras should not be angled to directly face lighting or sunlight.

Camera types

Area	Example	Camera type
Camera inside	Admin counter	Bubble dome
Camera outside, viewing an area between buildings, less than 2700mm AFFL	Walkways, block exterior, common areas, installed 2400mm – 2700mm AFFL	Vandal proof dome camera
Camera outside, viewing an area between buildings, installed 2700mm – 5000mm AFFL	Walkways, block exterior, common areas, installed 2700mm – 5000mm AFFL	Turret camera
Camera outside viewing a large area or open space	Car park/fence link/blocks from a distance (e.g. sheds)	Varifocal turret dome/camera
Camera is outside viewing an area between buildings and connected via coaxial cable	Walkways, block exterior, common areas, where no fibre is available and coaxial cable	As above, IP camera over coaxial cable

Minimum requirements for cameras

Camera type	Resolution	Infrared	Lens
Bubble dome	5MP	Up to 10m	2.8mm
Vandal proof dome camera	5MP	Up to 30m	2.8mm
Vandal proof turret camera	5MP	Up to 30m	2.8mm
Varifocal turret camera	5MP	Up to 30m	2.8mm – 12mm varifocal

Recording and monitoring

Recording

CCTV systems are to include installation of two data rack mountable network video recorders (NVRs). NVRs are to be properly installed and secured in data racks. One NVR should be located in the centre of network (CoN) in a lockable cabinet/room which is covered by the school intruder detection system. The second NVR, installed as a back up/redundancy measure in the event of damage/critical failure to the primary NVR, should be located in a rack which is:

- in a separate block to the CoN; and

- in a room that is secured whenever not in use (including during business hours) and covered by the school intruder detection system.

NVRs are to:

- be compatible with the IP protocols of system cameras and capable of supporting the required resolution;
- have sufficient channel/licences for expansion; and
- have sufficient storage to record at least 31 days of footage at the recorded frame rates as specified for cameras. Backup NVRs should retain no less than 7 days of footage.

A guide for NVR capacity is below:

Number of cameras	NVR Capacity
0-10	16 channel/licence
10-25	32 channel/licence
25+	64 channel/licence

Monitoring station

Monitoring stations for CCTV are to be set up as a password protected login system. Monitoring station hardware is to be installed in a room that is secured when not in use (including during business hours). Any peripherals (e.g. mouse, keyboard) required for use are to be supplied. Monitoring stations are to be dedicated to CCTV equipment only and not connected on the school ICT network.

Network and infrastructure

All works are to comply with the Departmental Network Infrastructure Procedures and Standards (DNIPS). The relevant State Wide System Technician is to be advised of any proposed deviations, and details in writing must be directed to ICT SS Design Services (formerly Network Design) (network.design@qed.qld.gov.au) for review and approval.

Where no spare fibre cores or sufficient communications cabinet space is available for use with the CCTV equipment, assistance for an acceptable solution should be sought from and approved by ICT SS Design Services (formerly Network Design) (network.design@qed.qld.gov.au), and the relevant State Wide System Technician is to be advised of any proposed deviations.

CCTV infrastructure is to be rack mountable, properly installed and secured in available space within lockable data racks as per manufacturer specifications.

All equipment, cables and fibre patch leads are to be labelled as “CCTV”. Labelling must be sufficient so that all cables and leads can be easily reconnected if disconnected inadvertently.

Inter-building/structure extension of the copper horizontal subsystem for CCTV is not permitted.

Centre of network

The following is to be installed in the school centre of network (CoN), or where the primary NVR is to be located:

- primary NVR;
- fibre switch/core switch;
- rack mountable PoE switch (for any cameras running from the applicable block);
- rack mountable UPS capable of delivering minimum 2 hours power; and
- correctly earthed Cat6A patch panel (if required).

Network data racks

The following is to be installed in the data rack of each block where CCTV cameras will be installed covering the building:

- rack mountable PoE switch;
- rack mountable UPS capable of delivering minimum 2 hours power;
- Cat6A patch panel (if required); and
- secondary NVR.

Where there is no available space in existing data cabinets, particularly in the CoN for the necessary CCTV equipment, advice must be sought from the relevant State Wide System Technician and ICTSS Design Services (formerly Network Design) (network.design@qed.qld.gov.au). Details of any proposed solution must be detailed in writing for review and approval.

Physical installation

Cameras are to be securely affixed in accordance with manufacturer's specifications. Camera housing, mounts and cabling are to be sealed to prevent intrusion by insects, vermin or weather.

Cameras should be installed with the manufacturer's relevant junction box mount. Wall mount or pendant mount brackets should only be used to avoid obstacles in the camera view where no other option for camera location exists. Junction boxes should be opaque metal, and have no viewing window showing the data point.

Cabling should be kept internal to walls and ceiling spaces wherever practicable. Where conduit is required for cabling, rigid white communications conduit should be used with double-sided hot dip galvanised steel saddles affixed every 300mm. Adequate mechanical protection should be installed for all external conduit and enclosures under 2.1m and in direct sunlight.

Any non-functional/ “dummy” cameras/empty housings are to be decommissioned and completely removed. Any area where decommissioned cameras have been removed is to be appropriately repaired /made good.

Installation of any equipment on areas with asbestos containing material is to be carried out in accordance with the schools Asbestos Register and the installer’s Safe Working Method Statement (SWMS).

Poles installed for CCTV

To manage the cost of installation and maintenance CCTV on poles should be avoided wherever possible. Before any poles for CCTV are considered, the relevant Regional Infrastructure Advisor should be consulted.

CCTV poles are to be installed at least 1500mm from any building or climbable structure (e.g. outdoor furniture, trees, etc).

Prior to commencing work installing any poles for CCTV, the installer is to determine the location of all underground services such as water, gas, electricity and communication pipes or lines by engaging an authorised service locator.

Prior to installation of a pole within 1000mm of any underground service, consider of the applicable service provider must be obtained.

The installer is to ensure any services, surfaces and finishing damaged during the course of construction are reinstated as part of the project, at the contractor’s expense.

Electronic access control

General requirements

Whether a cabled or wireless access control system is installed, it is not to be connected via an active network link to any other department equipment and is not to utilise the school's ethernet network to transmit or store data, or to communicate with any source or destination. Separate rack mountable PoE switches must be installed for the system to utilise existing spare fibre backbone cores.

Provision of a back-up battery to permit system operation in the event of mains power failure should be included.

At any block with electronic access control installed, readers with a physical key override, keyed to the school's restricted key system, must be installed at any staffroom entry to the block, as well as at least one main external access point which can internally access all rooms in the block.

Cabled/integrated systems

Intelligent door controllers

The number and location of door controllers must allow for the efficient cabling, connection and operation of the system with an absolute minimum of externally run cabling.

Door controllers are to be co-located with other LAN modules such as the intruder detection system controller or system expander modules.

Each door controller is to have the following minimum input and output facilities for each controlled door:

- A dedicated and separately fused 12V DC power supply output for readers associated with the door;
- Dedicated outputs for data signals to/from readers associated with the door; and
- Separate and dedicated inputs for 'request to exit' (REX) and 'request to entry' (REN) signals from REX or REN switches associated with the door.

Door controllers are to have the capability for two readers to be associated with a single door to permit the installation of both an entry reader and an exit reader.

Each door controller is to be capable of automatically switching the status of any associated door at different times of the day, based on parameters passed on from the controller. The following access criteria modes are required:

- Access: door is unlocked, no entry credential required;

- Secure: door is locked, a valid entry credential is required for access. Door re-secures after access or within the programmed door access time period; and
- Pending access: door is secure and switches to access upon presentation of the first valid access credential within a programmed time period.

On presentation of an access credential to a reader connected to an intelligent door controller, the controller is to check validity of access based on ALL of the following criteria:

- correct facility code;
- authorised credential in database;
- authorised door reader;
- authorised associated intruder detection area control; and
- authorised time period.

The door controller is to unlock a controlled door within 0.5 seconds of the presentation of a valid credential at a reader associated with the door.

Door controllers are to monitor the condition of, and access on, each door and report all events to the alarm panel for further processing, data storage, signalling or enunciation.

Separate alarm messages are to be transmitted to the controller for each of the following alarm conditions from each door:

- door forced open;
- door open too long (ajar);
- door not locked;
- invalid access attempt; and
- door lock being tampered.

A “restore” message is to be transmitted to the controller when the door is re-locked after the following door alarm conditions:

- door forced open;
- door open too long (ajar); and
- door not locked.

Should communications with the controller fail:

- all door controllers are to continue to operate without performance degradation;

- the isolated door controller is to continue making access decisions with all access attempts, valid or otherwise, and all alarm activations buffered internally to the isolated door controller. An internal activity buffer of at least 100 events is required; and
- the door controller is to immediately transfer the buffered activity events to the central controller when the communications link is re-established.

Door controllers are to be fitted with automatic restart facilities to enable them to resume processing following a power and backup failure.

Should any door controller fail or stop operation for any reason, only those doors associated with the failed door controller are to be affected.

Readers

Access control card readers are to have the following minimum specification:

- Open Supervised Device Protocol (OSDP) or equivalent secure format;
- operate from the dedicated 12V DC (nominal) power supply output from the associated intelligent door controller;
- be of weatherproof construction and resistant to vandalism, with any externally mounted readers having an IP rating 67;
- incorporate a sounder for user feedback of access attempt or door open too long (ajar) condition; and
- incorporate a multi-coloured LED for user feedback of door or associated intruder detection area status.

Electronic locks

Any installed locks are to be suitable for the particular door, hardware and application required.

Electronic lock of typical wooden pedestrian access doors is to be performed by electric mortise locks that meet DoE design standards with the following functions or features:

- style to match other door locks and meet other architectural requirements;
- model and form which matches the door and door frame;
- fitted with an electrical locking solenoid which operates on 12V DC;
- integrally fitted with a flywheel diode to supress counter electromotive force and protect the locking solenoid;
- fail-secure type, except where specifically required otherwise under the Building Code of Australia or *Building Fire Safety Regulation 2008* (Qld);

- integrally fitted with two switches to provide a single logical output for both door closed and door secure conditions. If a reed switch magnet is required to be fitted in the door jamb for this purpose, this magnet is to be a fully concealed type;
- integrally fitted with a microswitch on the internal lock hub, monitoring use of the free internal door handle. This switch is to always activate before the door condition output changes state and in sufficient time for the access control system to process this signal before the door condition signal; and
- fitted with a matching striker plate in the door or frame.

Door status signals

The logical output from the switches monitoring “door closed” and “door secure” conditions are to be connected to the input of the intelligent door controller which monitors the condition of the associated door. Any end-of-line resistors required for this function are to be located within the cavity created for the door lock.

Request to exit signals

The microswitch monitoring the free internal door handle of each door is to be connected to the dedicated and specific request to exit signal input of the intelligent door controller for the associated door. Any end-of-line resistors required for this function are to be located within the cavity created for the door lock.

Wireless systems

The main control unit should be located in the CoN/data room. Controller nodes are to be installed within ceiling spaces or secure data/store rooms in each building.

At any block with wireless electronic access control installed on each external door, readers with a physical key override, keyed to the school’s restricted key system, must be installed at any staffroom entry to the block, as well as at least one main external access point which can internally access all rooms in the block.

Battery life of readers should be no less than 2 years or 20,000 cycles. Nodes are to have an offline memory of at least the last 100 users in the event of a communications failure and be able to recognise and function for these users.

Occupant warning systems

The advice below is for bell, public address and occupant warning systems with lockdown/evacuation tone capability and is not meant for fire warning/emergency warning and intercommunication systems (EWIS).

General requirements

Occupant warning systems can include bell and public address as additional functions in one system.

Systems must comply with all relevant standards, codes and regulations of the authorities having jurisdiction over such works, including local Councils and those issued by the Department of Environment, Science and Innovation.

Systems must incorporate a lockdown warning facility with dedicated push button controls (as detailed in the Components section below). The lockdown warning facility must override all other public address functions when in use.

The system must be zoned logically and simply, with a minimum of one zone per building, car park or outdoor area. The system must be capable of directing messages to selected zones, while minimising the audibility of these messages in adjacent zones.

Controls must enable the selection and de-selection of zones in a simple and efficient manner.

Network requirements

Systems can utilise existing spare fibre backbone cores in the school's data racks to facilitate a direct physical connection between blocks.

Equipment is not to be connected via an active network link to any other department equipment and shall not utilise the schools ethernet network to transmit or store data or communicate with any source or destination.

Separate rack mountable PoE switches must be installed when systems are utilising the fibre. Where no spare fibre cores are available for use with the CCTV equipment, assistance for an acceptable solution should be sought from ICTSS Design Services (formerly Network Design) (network.design@qed.qld.gov.au), and the relevant State Wide System Technician is to be advised of any proposed deviations.

Systems that use wireless connectivity must be encrypted signal or dedicated RF channel.

Copper is not to be used for interbuilding communications.

Speaker location/output

The number of speakers required will be determined by school size, layout and background noise in various areas of the school. System speakers should be installed externally and be able to achieve a level of 80dB at 10 metres.

External speakers should have a vandal rating of IP67. Speakers in high activity or easy access areas should be caged.

Internal speakers (and visual aids where required), should be scoped in high noise areas including:

- manual arts;
- music;
- home economics;
- tuckshop;
- hall; and/or
- any other areas where insufficient sound is achieved by external speakers as noted above.

Systems should have the option for volume control to allow users to adjust where appropriate.

Amps with maximum wattage capacity for approximately double the speaker output should be installed to eliminate distortion.

System capability

Systems should have the capacity for:

- Emergency tone generation (evacuation, lockdown and all clear);
- zoning capability to allow each block to be addressed individually;
- public address ability including remote broadcasting via designated device or mobile phones; and
- school bell and accompanying function.

Systems must comply with the following requirements:

- be simple and logical to operate for staff;
- the Rapid Speech Transmission Index (RATSI) must not be less than 0.5 in at least 75% of each area of coverage and should not fall below 0.45 for the remaining 25% of each area;
- provide a facility for the broadcast of pre-recorded routine, situation and emergency announcements and warning tones. The system must be able to store at least 200 default messages;
- allow the simultaneous broadcasting of different announcements to different zones;

- allow the broadcasting of music and sounds (including the school ‘bell’) to all or selected zones; and
- enable the selection and de-selection of zones simply and efficiently.

The system must only allow one microphone to announce a message in a selected zone. Any other microphone that tries to select the same zone must not be able to announce their message until after the first microphone has de-selected the zone.

Components

Systems should have a desktop controller with:

- programming and frequency tuning of devices;
- handheld or desk mounted microphone;
- activation panel with buttons for:
    - Evacuation;
    - Lockdown;
    - All clear.
- option for secondary activation panel if required by the school; and
- battery backup providing at least 2 hours backup power for the desktop console.

Definitions

Term	Definition
Access Control	The selective restriction of access to a place or other resource.
ACM	Asbestos-containing materials.
Alarm	The state of an input when it is in an abnormal condition (not sealed).
Area	A grouping of inputs that can be armed or disarmed.
Armed	An area that is turned on and is monitoring the state of its inputs.
Controller	The electronic component that processes and responds to the information received from all devices in the system and enables intruder detection and access control.
Credential	unique identification that a user provides to interact with the system. This can be a security PIN, card or username and password.
Disarmed	An area that is turned off and is not monitoring the state change of its inputs. A disarmed area will still monitor for the tamper state.
Door Reed	A magnetic field detector that is used to detect the status of a door/window etc.
Exit Delay	The duration of time that a user has to exit an area after arming it without generating an intruder alarm.
Expander module	Equipment which connects to the main controller and provides additional inputs.
Input	A switch, button or detector that is physically wired to a controller or one of its modules or a logical (non-physical) system process to be monitored.
Intruder detection	An electronic system of monitoring inputs and reporting and recording changes which indicate unauthorised entry into a building or area.
Isolate	Inputs can be placed in the isolated state, where all state changes are ignored. Isolation can be temporary with the input automatically de-isolating when the area linked to it is disarmed, or persisted, requiring a user to manually de-isolate it. Persisted isolation (“sticky isolate”) is commonly used for faulty detectors or those undergoing maintenance, while temporary isolation can allow an area with unsealed inputs to arm successfully.

Term	Definition
Networked Video Recorder (NVR)	IP based appliance which connects cameras through a network and records video captured to a mass storage device.
Open Supervised Device Protocol (OSDP)	An alternative protocol to Wiegand, offering better security and easier installation over a bus interface, allowing multiple readers to be attached to the same cable.
Occupancy warning system (OWS	A public address, bell, or communication system to notify or alert occupants of a broadcast (emergency or otherwise), simultaneously throughout all specified of the building or facility.
Reader	A control point to access doors.
Reed Switch	An electronic switch operated by a magnetic field. Often used to determine if a door is open or closed.
Seal	The state of an input when it is in a normal condition (not in alarm).
Tamper	The state of an input that has been tampered with.

Appendix A: Intruder detection system commissioning checklist

Client forms	
QP2168 Alarm monitoring agreement	☐
QP2163 GPRS unit charge agreement	☐
QP2162 Alarm response procedures agreement	☐
QP2166 Site contact information proforma	☐
QP2165 Late to secure procedure agreement	☐
Technical forms	
QP2101 Technical information proforma	☐
QP2164 GPRS unit technical information	☐
QP2169 System area information proforma	☐
QP2171/QP2172 Sector information	☐
QP2173 System User Information Proforma	☐
Equipment	
T4000 checklist	☐
Serial cable 996795 for TTL connection on T4000 to port 0 on control panel	☐
Serial cable 996796 for 232 connection on T4000 to UART board	☐
UART Board 995066 to allow for the second serial port connection	☐
4G T4000 GPRS unit	☐
Hi gain antenna	☐
232 Serial comms task setup guide	☐

Provide to PSG	
Type/Model of Panel installed	☐
Panel Serial Number	☐
Onsite computer details	☐
Installer code	☐
Communicator type	☐
Connection Type	☐
Test of all comms to monitoring	☐
Confirmation Insight is setup on Comms Task 1/2 pointed to Port 1. GSM setup on Comms Task 3/4 pointed to Port 0	☐
Confirmation SkyCommand Synchronised	☐
Test SkyCommand Remote Arm/Disarm	☐

Appendix B: School security site commissioning checklist

Site details			
School/Region/Branch:			
Assessor/School security advisor:			
Project contacts:	[New Schools Project Coordinator] [Project Manager] [Principal and BM]		
Part 1 – Perimeter fencing and external lighting		**Compliant**	**Action required**
A	Obtain details of internal and external lighting schedules as programmed	☐	
B	Confirmed with staff that car parks/access paths to admin are well lit	☐	
C	Security lighting is in place to building perimeters and external paths of access	☐	
D	Discuss options for onsite lighting as a deterrent	☐	
E	Obtain as built fencing diagrams	☐	
F	Inspect perimeter fences and gates to ensure compliance with Fencing Specification and document deficiencies	☐	
G	Discuss any processes in place for security site perimeter and any issues	☐	
Part 2 – Entrance/administration building		**Compliant**	**Action required**
A	Staff are aware of the location of duress buttons, how and when to use them and how to reset (if applicable)	☐	
B	Staff maintain a register of all keys/access cards held and issued and a system to regularly audit this	☐	
C	Staff are able to suspend sick room monitoring feed (if applicable)	☐	

D	The school has a visitor access system or process	☐	
E	The school restricts access to the grand master keys and these are not taken offsite.	☐	
F	The school has a suitable, secure key safe or cabinet for storage of keys	☐	
G	The school's practice is not to mark or label keys, or carrying with lanyards or badges which would allow them to be identified.	☐	
Part 3 – Alarm system operation		**Compliant**	**Action required**
A	Confirmed location of system RAS, expanders (zone list), and user manuals and passwords and training certification,	☐	
B	Obtain training record confirming staff training	☐	
C	Obtain copy of input zone listing on record with PSG	☐	
D	Obtained a copy of the validation report from PSG	☐	
E	Obtained copy of site contact information from PSG	☐	
F	Obtain current panel user listing from PSG	☐	
G	Obtain current open/close schedule from PSG	☐	
H	Obtain current late to secure procedure from PSG	☐	
I	One internal keypad is installed in the admin block directly adjacent to the block's main entry door	☐	
J	External keypads (no less than 1, no more than 4)	☐	
K	External keypads are under cover and in well-lit locations on blocks adjacent natural paths of pedestrian traffic, adjacent school boundary access points	☐	
L	External keypads are fitted with cylinder lock or secure latch to with padlock keyed to the school's master keying system.	☐	
M	Zone listing on record with PSG matches zone listing at panel. Arranged for any updates required to naming conventions, zone details etc.	☐	
N	Put system into test and confirm activation and restore for each duress alarm output is being received by monitoring	☐	

O	Confirm all users in the panel are current and that codes are not more than 12 months old. Arranged for any changes required.	☐	
P	Using the open/close schedule from PSG ensure alarm system is being correctly used, no zones are isolated etc. staff are arming/disarming efficiently and raise any issues for improvement.	☐	
Q	Obtained a copy of the alarm response instructions and review to ensure they are clear and all contact details are current. Discuss any recommendations with staff and arranged for changes to be made where required.	☐	
R	Confirm detectors, reed and duress buttons are installed in line with the Electronic security guideline	☐	
S	Site has a dedicated workstation with access to make changes to the alarm panel.	☐	
T	Areas used after hours or by non school user groups are able to be armed and disarmed independently. Instructions for such users exist and are socialised. Alarm response instructions reflect verification and response for non-school users e.g. how are out of hours users verified, who do they call for assistance, any variance in alarm responses when community groups use the space.	☐	
Part 4 – CCTV system		**Compliant**	**Action required**
A	Obtained as builts for CCTV system locations, camera views and user manuals and passwords and training certification	☐	
B	Obtain training record confirming staff training	☐	
C	NVR and back up NVR installed in Centre of Network, data room or secure location	☐	
D	Cameras installed. Obtain camera angle images	☐	
E	Staff onsite have password for NVR and training on how to view and download footage	☐	
F	Monitor/s installed and camera views set up	☐	

G	Monitors are password protected and shielded from unauthorised viewing	☐	
H	Staff are able to suspend live stream of sick room (if applicable)	☐	
I	No audio is being captured by cameras	☐	
J	Confirmed retention is set to no less than 31 days for main NVR and 7 days for back up NVR	☐	
K	Staff have a CCTV policy and a disclosure register	☐	
L	CCTV Signage *As a minimum, **approved signage** should be placed at every entry point to the school grounds as well as the entrance to every CCTV camera's area of operation.* E.g. all vehicle and pedestrian gates, admin and halls, OHSC, everywhere a visitor would enter school grounds.	☐	
M	Obtained copy of CCTV compliance checklist completed last 12 months	☐	
N	List of staff authorised to view CCTV is contained in the CCTV policy	☐	
O	School has a system of recording the release of CCTV e.g. a disclosure register based on the DoE disclosure register sample	☐	
P	There is no CCTV in toilets, change rooms, classrooms, learning/teaching spaces, staff rooms and offices.	☐	
Q	There is a camera capturing the access point to the Centre of Network or data room. Preference is camera is external not internal.	☐	
Part 5 – Security documentation		**Compliant**	**Action required**
A	Technical information has been provided to the school from project team.	☐	
Part 6 – Security awareness		**Compliant**	**Action required**
A	Reviewed end of day (securing premises outside of school hours) processes	☐	

B	Obtained a copy of the most recent End of term security checklist	☐	
C	Obtained copy of or discussed potential for key management policy in line with the key management guidelines	☐	
D	Obtained copy of latest security risk assessment and action plan completed by Principal in last 12 months	☐	
E	Obtained copy of or discussed potential for visitor management guidelines	☐	
F	The Principal and BM have completed the New Principal/business manager security checklist		
G	The Principal and BM know who their school security advisor is, how to contact them, and what support is on offer.	☐	
Part 7 – Incident reporting		**Compliant**	**Action required**
A	Provided report on preceding 12 months' incident reporting and discussed any topical issues and the importance of reporting	☐	
B	Notified Principal of School's most current security risk rating and provided an overview of the analysis process.	☐	
C	Discussed any regional partnerships in place (e.g. with local police) and attendant security benefits.	☐	
D	Obtained an overview of local School Watch advertising which is in place. Staff know how to get additional materials	☐	
E	Confirmed staff know how to report security incidents and get help in an emergency	☐	
Part 8 – Signage and design		**Compliant**	**Action required**
A	Visitors sign	☐	
B	School watch	☐	
C	Other signage noted	☐	
D	Monitoring signage/security provider signage visible in key locations		
E	Trees, shrubs and foliage are not problematic e.g. providing hiding, blocking view, obstructing cameras	☐	

F	Bins are secured away from buildings after hours preferably in a locked enclosure or amenities area	☐	
G	Available canvas for graffiti is minimised	☐	