Design Guidelines
September 2019: Issue 4

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Section 18
Security.

www.canterbury.ac.nz/learningresources

Standards in the Design Guidelines Suite

Design Standard Guidelines Index:

	01	**General**
	02	**Architecture**
	03	**Audio Visual**
	04	**Civil**
	05	**Communication Cabling**
	06	**Design for Access and Mobility**
	07	**Documentation Standards**
	08	**Electrical**
	09	**Environmentally Sustainable Design (ESD)**
	10	**Fire and Life Safety**
	11	**Interior Design**
	12	**Hydraulics**
	13	**Infrastructure**
	14	**Landscaping**
	15	**Lifts**
	16	**Mechanical**
	17	**Metering and Controls**
❯	**18**	**Security**
	19	**Signage and Wayfinding**
	20	**Structure and Seismic**

Document Control

Revision History

Revision Number	Description	Section Owner	Date
Issue 1	Original Draft	-	-
Issue 2	Internal Review	-	-
Issue 3	First public circulation	-	October 2016
Issue 4	Updated Issue	*R. Oudshoorn*	*September 2019*

Current Document Acceptance

Update Authored	Approved	Date
M. Oliver	*R. Oudshoorn*	*September 2019*

Key Updates from Previous Issue

Revision Item	Details
18.1.1 Security Processes on Campus	*Project specific upgrades to coordinate with wider campus upgrades. Refer to clause for details.*
18.2.2.2 Additional Compliance Deliverables	*Final paragraph amended.*
18.2.4 CCTV	*CCTV camera requirements amended*
18.2.6 Duress Alarms	*New clause*
18.3.7.3 Vehicle Barriers	*New clause*
18.4.2.2 Emergency Door Release units (EDR)	*Exception to requirement outlined*
18.4.4 Sliding & Swing Doors	*Security control board requirement added*

Contents

18.1 Overview

The mission of the University of Canterbury Security is to enhance the quality of life for the entire University community by maintaining a safe and secure campus where the safety of all is balanced with the needs of our community.

Design of the built environment at the University should aim to assist Security in this mission. To achieve this, design consultants should consider all opportunities to ensure the campus is free from crime, easy to secure and evacuate if and when required, and provides a civil and open environment that fosters learning.

This section of the Design Standard Guidelines is intended to be read in conjunction with **Section 01 – General** and any project specific brief and agreements.

18.1.1 Security Processes on Campus

It is important to the University to provide a safe and secure campus for the benefit of every person using it. To accomplish this, activities undertaken by the University's Security Services include:

- Monitoring of CCTV camera's
- Segway, foot, and vehicle patrols
- Emergency Call Point System
- Coordination with Emergency Services

Design of the built environment at the University of Canterbury shall consider and facilitate these activities through consultation with the University of Canterbury Security and Campus Community Support department.

The University are continuously looking to upgrade their security networks and processes across the wider campus. Individual projects may present opportunities to contribute to bigger picture security upgrades, and therefore the scope and design of security measures for each particular project should be discussed with Campus Services at the early design stages. For example, this may include;

- *Additional cameras covering areas within or adjacent to the project area to extend the campus wide CCTV coverage*
- *Additional vehicle barriers to add layers of zonal control to vehicles within the campus*

18.1.2 CPTED Principles for Passive Security

Building and spatial design should consider security and safety in combination with all other design attributes and considerations. Included early, passive security measures can be implemented with often minimal cost or impact on design and lead to improved safety and security outcomes for staff, students and the general public.

A commonly recognised approach to design that achieves these outcomes is known as Crime Prevention Through Environmental Design (CPTED). CPTED is a philosophy based on considered design and the effective use of the built environment and activity leading to a reduction in the incidence and fear of crime, as well as an improvement in the quality of life.

A CPTED approach reduces criminal opportunity and fosters social interaction among legitimate users of space. The emphasis is on prevention rather than apprehension and punishment. There are four key overlapping CPTED principles which are:

- **Surveillance** - People are present and can see what is going on
- **Access Management** – Methods used to attract people and vehicles to some places and restrict them from others
- **Territorial Reinforcement** – Clear boundaries encourage community 'ownership' of the space
- **Quality Environments** – Good quality, well maintained places attract people and support surveillance

The University's intention is not to implement a full and formal CPTED assessment for each project, unless specifically required or requested.

Instead, high level design considerations have been developed and included throughout this document to suit the context of the campus and these should be applied when undertaking any building or spatial design, for both internal and external spaces at the University.

18.1.2.1 Further Reference Material

The design considerations put forward in this document are based on **the Ministry of Justice - National Requirements for CPTED in New Zealand - Part 1 and Part 2** which define seven qualities that characterise well designed, safer places. These requirements should be referred to in full should a detailed CPTED assessment be required for the project.

18.1.2.2 Additional Compliance Deliverables

The design consultants are to progressively incorporate the requirements and considerations in the design guideline into the design and submit the following additional deliverables:

At the End of Concept Design - Submit a marked up site plan conveying; the bulk and location of the building, campus connections, travel routes and desire lines, entry points and circulation.

At the End of Preliminary Design - Submit a series of marked up floor plans conveying how passive security principles have been applied in the design of; space hierarchies, communal/community areas, entrances and lobbies, service areas, landscaping.

At the end of Developed Design – Submit design documentation suitable to confirm the approaches and strategies used for the inclusion of passive security principles in; materiality, entrance design, doors and windows, lighting, rubbish and storage, and master keying.

18.2 Active Security Considerations

18.2.1 Access Control Security Zoning

Building access is managed in order to provide protection to the University community and property whilst continuing to assist in the provision of an open, safe, comfortable and efficiently run environment that contributes towards meeting the teaching and research objectives of the University.

Areas requiring electronic Access Control (in the form of Magnetic Clamps or mortise locks with Card Readers appropriate to the area and risk) are:

- All Level 1 (i.e at ground level) external doors
- Laboratories
- Network Communications Rooms
- Access at floor level from circulation stair
- Lifts (When accessing secured areas)
- Computer Work Rooms

Other areas shall be designed to be free access during operating hours and secure at other times

Where afterhours entry is required a T20 card plus pin reader shall be installed, on internal doors required to be secured a T11 card only reader is to be installed.

In some instances manual locks may be suitable for afterhours entrances.

Care must be taken to provide an environment which actively discourages both tailgating/ghosting through secure lines and 'stair dancers'.

Alternative manual locking systems should be discussed with the University to facilitate ease of access during long term power outages.

18.2.1.1 Access for Contractors & Temporary Staff

Access for contractors and temporary staff shall be provided through a University of Canterbury Visitor ID account and swipe card only.

This will allow the University to give them certain access to buildings and areas on campus in accordance to the projects they are currently authorised to work on.

The same principle may apply to keys being made available but is to be considered on a case-by-case basis and in accordance with the University security policy.

18.2.1.2 Further Requirements for Restricted Areas

Access to Communications Rooms, Plant Rooms, and areas storing valuable goods shall be restricted to required personnel at all times.

These rooms shall not have any signage that identifies the room's purpose other than that required to discourage general entry.

A door closer shall be fitted in all instances and locks should be configured in such a way that the room cannot be left unlocked.

In buildings where electronic card access is not practical a mechanical lock supplied via University of Canterbury Facilities Management shall be installed.

Care shall be taken in the design/construction of the room to ensure it is not possible to gain access to the room via a cable pathway or overhead plenum space.

18.2.1.3 Other High Risk / High Importance Areas

Areas designated as high risk or sensitive by the University may require specialist alarms or detectors.

The preference is to connect these areas directly to the Gallagher FT System and where this is not possible a Bosch standalone alarm control unit is to be used. Examples include,

- Walk in chillers (which require specialist alarms or approved manufacture).
- Other high value items flagged for extra security by designers

18.2.2 Advertisement of Security Measures

In recognition of the dual role of security as both a deterrent of crime and in assisting once it occurs - it is the University's preference for all active security measures to be clearly displayed and signposted.

18.2.3 Existing Alarm Infrastructure

The University has a centrally controlled and integrated Gallagher FT Access and Alarm system, which is installed across both Ilam and Dovedale sites.

It is the preference of the University that proposed security devices are compatible with these systems.

18.2.4 CCTV

As a minimum, CCTV coverage shall include:

- All ~~*main*~~ entrances to *buildings are to be monitored by external cameras to* capture persons entering.
- Major carparks (Lighting Design needs to allow for CCTV illumination levels)
- Major pedestrian routes (as designated by the University)

The preference is for these to be fixed cameras mounted at 3m above ground level.

Cameras shall be Internet Protocol (IP) cameras of approved manufacture and should be capable of power over ethernet (POE) operation if possible.

Designers shall also be wary of the effects of their design on areas of existing CCTV coverage and security, any concerns or potential issues should be flagged to the University of Canterbury Project Manager for consideration and resolution.

18.2.5 Emergency Call Point System

The University has a campus-wide emergency call point system comprising easily distinguishable towers with the following functions:

- Emergency help points with direct connectivity to University Security
- Low level CCTV platform
- Wide area broadcast system for use in evacuation and other emergency

The purpose of this system is to provide a greater level of support to the campus community both day to day and to provide rapid support and information during an incident.

Any new development on campus will likely invoke a need for students and staff to travel further from the existing emergency call point system - and therefore additional call point system towers should be considered. This will be confirmed in consultation with the University of Canterbury Security Department.

18.2.6 Duress Alarms

The provision of duress alarms should be considered where circumstances may warrant these additional provisions. For example; staff working alone, during extended operating hours, or where there is a specific risk of hazard.

Where duress alarms are being considered the design should be integrated with appropriate complementary measures such as passages of safe retreat (access to a place of safety) and CCTV coverage.

18.3 Passive Design Considerations

18.3.1 Access: Safe Movement and Connections

The University requires well-defined routes, spaces and entrances that provide for convenient and safe movement without compromising security. This must consider movement in both internal and external spaces, the likely modes and times of travel, and access and mobility.

Safe access is provided between key destinations and entrapment spots eliminated. Access shall be designed to maximise visibility and avoid creating potential hiding places. When potential entrapment spots cannot be designed out, they shall be gated or secured at night.

Spacial planning shall endeavour to avoid internal elements such as dead-end corridors or blind corners.

Multiple exit points are to be provided from public spaces and along pedestrian routes. These should be clearly signposted in advance of entrances to any movement predictors such as footbridges or passageways.

Consequences of the number and type of connections points should be considered. Access to the rear of buildings especially should be considered and, if this cannot be restricted, other measures such as enhanced visibility and good lighting need to be incorporated.

18.3.2 Surveillance & Sightlines: See and Be Seen

Good visibility, sightlines and casual surveillance should be provided at all times - but particularly in all publically accessible spaces.

Building design should create the opportunities for informal surveillance from the adjacent buildings or through active frontages.

Internally, spatial planning should ensure that the location of manned facilities, such as reception or help desks, creates the opportunities for informal surveillance of building entrances and key circulation routes.

External physical elements such as continuous solid fences, blank walls or planting beside footpaths that impede sightlines or visibility and reduce opportunities for surveillance should be avoided. Where used, these elements should be low or highly visually permeable to help visibility.

18.3.2.1 Lighting

Lighting should be a primary consideration and integral to the overall spatial design. It should be designed with management and maintenance in mind (i.e. lighting fixtures should be vandal resistant and kept out of reach). Redundancy in the lighting scheme needs to be considered to ensure that lighting is not compromised if bulbs are not replaced immediately after failing.

Consultants shall provide a comparison of design lighting levels for roads and public spaces on the campus to the requirements AS/NZS 1158 for discussion with the University.

Lighting should be considered for places that used at night (i.e. car parks, major pedestrian and bicycle routes, public spaces, building entrances, access and egress routes) and for areas where safety risks have specially been identified. Where appropriate these areas should also be the subject of specific CPTED lighting assessments.

Careful consideration should be given before providing lighting in areas not intended for night-time use as lighting can give a false impression of safety. Generally lighting should not be provided in such areas.

Lighting controls, such as PIR sensors, should be used to draw attention to activity in areas where activity is discouraged at night. For example, plant areas at the rear of buildings.

In relation to the type of lighting, it should provide good visual guidance and orientation. Fittings should be placed to ensure uniformity of lighting levels over an area, including to the sides of paths, avoiding glare and reducing the contrast between shadows and illuminated areas, except when highlighting a specific area or feature.

Consideration needs to be given to vegetation or other elements to ensure that it doesn’t interfere with the effectiveness of lighting.

Lighting illumination sources should be of a type and spacing that enables accurate colour and facial recognition.

Internal security lighting shall be provided in balconies, verandas, corridors, stairwells and exterior doors.

Care should be taken when installing external lighting that it is placed or designed to avoid vandalism and damage

18.3.3 Layout: Clear and Logical Orientation

Buildings (and the campus as a whole) should be laid out to discourage crime, enhance perceptions of safety and help with orientation and way-finding. This is critical in spaces where there is a perceived risk to personal safety (e.g. stairwells, car parks, bike stands and lobbies).

Active frontages are required, particularly at ground level and adjacent any external public spaces.These external public spaces should be of a high quality, serve a purpose and support an appropriate level of legitimate activity. Landscaping and the creation of high should be used to support legibility.

With particular reference to facilities with an intended 24 hour use, building layout should actively reduce the likelihood of lone working and distances of travel between likely night time use areas and key facilities. Where possible 24 hour facilities should be located on Level 1 of a building.

18.3.3.1 Signage and Wayfinding

Building entrances and exits should be clearly signposted or otherwise clearly defined and easily accessible. These will be well-lit and facing the any public spaces with lobbies visible from the outside.

Orientation and way-finding should also be considered in the internal spatial planning, especially how it may change between day and night usage.

Signage should be legible and informative to route choice and wayfinding, including access routes and facilities. It should identify access to assistance such as 24 hour UC helpline and the emergency services.

Lit and non-lit routes should be identified on route maps and other such signs to assist night-time route choice.

18.3.4 Activity Mix: Appropriate Integration of Use

Mixed-use of space shall be encouraged through the incorporation of activity generators, and designers should aim to promote levels of human activity which is appropriate to the space, in an effort to reduce crime and promote a sense of safety.

Concentration of conflicting or vulnerable uses should be avoided.

Encouraging appropriate night-time uses, which are complementary to each other, is to be considered to provide more ‘eyes on the street’, and contribute to the safety of a place at night.

18.3.5 Sense of Ownership and Care

Spaces should be clearly indicated as to whether they are public, communal, semi-private or private by using design techniques and elements appropriate for the context and the intended use of the space - and promote a sense of ownership, respect, responsibility and community.

Stakeholder engagement in the planning and design process is encouraged, especially decision making about a spaces’ design and management, as it is an effective way to develop pride in a place and a sense of ownership.

People who feel ownership of a place are involved in defining its identity. Elements and features, such as public art and sculpture, can help to personalise a space and promote local identity, sense of place and ownership.

18.3.6 Quality Environments: Well Designed, Managed and Maintained

Care shall be taken to create good quality and attractive spaces that increases their safety and use, and promotes a greater respect for the environment. The design and layout of spaces should support their management and maintenance.

Materials and fixtures should be vandal resistant. This includes avoiding long expanses of blank walls or fences, especially in light colours, and use of robust and graffiti-resistant materials and finishes.

Imaginative responses to potential maintenance and vandalism problems should be considered, such as commissioning murals by students or using vandal-resistant textures.

18.3.7 Physical Protection: Appearance & Function

Any necessary physical features should be designed to appear intrinsic, unobtrusive and if possible provide a positive visual feature.

The potential for security features to have a visually negative impact needs to be carefully addressed. These can create a poor image or a fortress-like appearance and can give the perception that places are unsafe.

For example, treating gates and fencing as public art or incorporating a simple design motifs whilst still allowing visibility through them.

The building design should avoid external design features that make access to upper levels easier and locate lifts within secure entrances.

18.3.7.1 Internal Areas

All critical assets shall be obscured from direct lines of sight through windows and doors.

18.3.7.2 External & Landscaping

Obscuration or concealment screening using trees and hedges, berms, solid fencing and walls can be used to prevent direct line of sight to key assets or restrict access areas.

However, care should be taken to not to obscure any camera views of buildings entrances, approaches, or perimeters. In particular alcoves should be avoided wherever possible. Where shelter is required open canopies should be installed.

Perimeter controls appropriate to the building location and usage could include:

- Fences and gates suitable for both pedestrian and vehicular traffic
- Soft landscaping such as foliage or ponds
- Barrier protection for man-passable openings (greater than approx. 250mm x 250mm) such as air vents, utility openings and culverts.

18.3.7.3 Vehicle Barriers

The use of vehicle barriers to provide levels of zonal control for vehicles within the campus, and to prevent proximity to building entrances is required, however these barriers shall be considerate of access and mobility.

Vehicle barriers should be designed to the performance criteria outlined in PAS68. Design to other appropriate standards can be considered on prior approval from the University.

18.3.7.4 Secure Fenced Areas

All assets, plant and infrastructure essential for the continuity of the University shall only be located on the outside of buildings where it can be explicitly proven that the perimeter security of these elements has been considered and meets all best practice requirements.

This shall also apply to any areas with explosive substances such as LPG tanks.

18.4 Materials & Equipment

18.4.1 Entry Devices

18.4.1.1 Card Readers

All card readers shall be Gallagher approved type and manufacture.

University sites with external readers shall be Prox /Pin readers (T20) with Prox only readers (T11) used on internal doors, unless extra functions are required.

Where readers are likely to be subject to adverse conditions a vandal proof cover shall be fitted.

Readers and other fittings shall be mounted in an easily accessible position as guided by **Section 06 - Access and Mobility**.

18.4.1.2 Keypads

The preferred keypad entry a Gallagher T20 Reader in PIN only configuration. However, other keypads may be used upon prior approval from the University.

18.4.1.3 Key-switches

Key switches used on site shall be compatible with the University Kaba system and will be provided by the University to the contractor. Unless otherwise specified.

18.4.2 Exit Devices

18.4.2.1 Request to exit buttons (REX)

Request to exit buttons (REX) shall be green double pole push buttons mounted in a single gang plate engraved with “Push to Exit” flush where possible and within easy reach of the door in a location easily seen when approaching the door. These shall be mounted between 1.0 and 1.3 metres above floor level.

1 pole shall be wired in series with the lock power the second pole shall signal “exit” to the access control system. REX units must not require power to operate, unless an EDR unit is installed alongside the REX device. All REX buttons are to be terminated onto cabling via screw terminals , soldered connections are not acceptable.

18.4.2.2 Emergency Door Release units (EDR)

EDR’s are required on all doors unless fitted with a free handle mortise lock.

Emergency ‘Break glass’ units are required at all 24/7 secured exits. The preferred units are resettable type CQR or EM- Rex and flush mounted between 1.0 and 1.3 metres AFL where possible.

They shall be mounted flush where possible, within easy reach of the door, and located to be easily seen when approaching the door.

The units must be wired directly in series with the lock power supply; it is not acceptable to break the lock supply via auxiliary relays or electronic means. The activation of the EDR shall be monitored by the access control system.

18.4.3 Specified Lock Equipment

Magnetic Clamp Locks

The preference for lock equipment is to use magnetic clamp locks wherever possible.

Approved electromagnetic locks are to be 500kg force standard 12v DC with lock bond sensing of approved type and manufacture.

Other Magnetic lock brackets (including Z type fittings) are acceptable on prior approval from the University and must incorporate the following features:

- Anodised to match the lock or powder coated to match the door frame or surrounds
- The bracket must not be removable with the lock in the locked state, a dome head bolt with the dome on the insecure side is the minimum standard. Brackets and locks must be securely fitted to allow for regular closing of the armature plate against the lock.
- The Z bracket must fully cover the lock termination plate in the secure state.

Mortise Locks

For doors lower than 2100mm high (not permitted in new installations) mortise locks can be used. Unless otherwise advised mortise lock furniture will be supplied by the University.

Mortise must operate on 12v DC and include REX indication and lock status indication.

Other Locks

V or Cobalt locks may be used on approval from the University and must include lock status indication

Approved electric strikes may be used on approval of the University, and must be commercial type with full latch and locked monitoring.

Drop bolts and shear locks shall not be used on University sites.

18.4.3.1 Protection for Equipment

All audio visual (AV), information technology (IT) and other valuable equipment shall be adequately protected from vandalism and potential theft.

Key equipment items should be securely locked or bolted where they reside by using either Kensington lock solutions, or other custom based approved security methods. No equipment valued over $500 should be left unsecured in a teaching space.

Only combination Kensington lock types shall be used. The University will provide approved combination key settings which can be obtained upon request when installing and configuring the Kensington locks.

18.4.4 Sliding & Swing Doors

All auto sliding doors shall be fitted with an advanced security control board.

All doors must be capable of interfacing to the access control system if access control is not fitted to the door a key operated mode switch mounted at 1200mm AFL will be required.

A wall mounted push button or emergency door release shall be provided on the inside of the building adjacent to the door

Sliding door controllers shall be Assa Abloy Entrance Systems Besam units

Swing door operators shall be Assa Abloy Entrance Systems Powerswing Units

All doors shall be monitored for “Door Position” and “Door Locked” (Bond sense) and door control signals shall be connected via dedicated cable pairs for each state. PIRs etc. shall not be used as junction points.

Auto Sliding doors shall be monitored as above, control shall include a lock input and an open input, on operation of the fire release or an afterhours card entry the door shall drive open.

Readers shall be wired in a dedicated cable from the interface panel.

Power to automatic sliding doors shall be via a standard 230 volt switch socket mounted at a high level eternal to the door pelmet, it must be possible to isolate the door without removing the pelmet.

18.4.4.1 Access Control Interface Cabinets

All controlled doors are to be individually cabled back to a central interface panel, this panel shall be housed in a switchboard style metal cabinet of Bremca or similar manufacture.

The minimum size of access control interface cabinets shall be 1m x 1m x 80mm (and consider the need for future expansion).

The interface will contain the following equipment:

- Gallagher Door Controllers
- Input/ Output Boards
- Time-clock Door Shunt Relays and Timers
- Din Style Terminals for the connection of cabling between the doors and the Gallagher controllers.
- Key Switch and 'Break glass' relays if required
- Fire Release relays
- Power Supplies
- Standby Batteries

18.4.5 Fire Release Action on UOC Sites

All University sites fitted with access control shall be wired for fire release on all access controlled doors upon activation of the fire alarm, locks only shall release readers will remain powered.

The method of operation is based on this trade providing a relay which is held energised by normally closed contacts in the fire panel; the relay will be housed in the Access Control Panel and powered by the access control system power supply. The Fire Alarm is not to be used to power this relay. The circuit is to be energised in failsafe configuration and loss of power or circuit continuity will release the access controlled doors. The operation of this relay will be monitored by the Command Centre.

18.4.6 Standalone Security Alarms

Alarm Panels shall be Bosch 16Plus and be connected to the University Monitoring Station via supplied phone lines.

Reporting format shall be Contact ID.

The University will provide user codes, including master codes and common codes.

Detectors shall be selected to best meet the level of risk and detection area and shall be wired as 1 detector per panel zone.

The location of Keypads and Alarm Panels shall be agreed with the University before installation commences.

18.4.7 Power Supplies and Battery Back Up

Power supplies are to be rated for 20% relief minimum of the rated continuous load

Power supplies providing in excess of 1 amp are to incorporate a separate battery charging circuit and not float the batteries across the charger load output.

All power supplies must be monitored for mains fail and low battery state.

The 230 volt supply in the panel is to be terminated in a double switch socket outlet within the Interface panel, the power supply / charger will then be plugged into this socket. Direct connection of 230 volt into the power supply unit is not acceptable.

All batteries are to be labelled with date of installation.

18.5 Installation Requirements

18.5.1 Cabling

All access control cables must have a minimum of 20% cable relief provisioned and must be continuous in length, joints are not permitted. Cabling within cabinetry shall be housed in pvc slotted cable ducting of the appropriate sizing.

All cabling is to be installed concealed where possible and, in a manner, consistent with NZ Standard 3000 for electrical wiring, and separated from 230-volt cabling.

Voltage drop must be considered for all cable runs, locks must not be compromised in anyway by reduced operating voltage at the lock.

Fire release cabling shall be Red Sheath 1.0 2mm or 1.5 2mm twin TPS cabled by this trade from the interface panel to the fire alarm panel. The fire trade shall connect the cable to N/C terminals at the FAP. Only 1 fire release per building will be provided in the case of multiple interface panels the access control contractor shall interconnect the panels.

18.5.2 Commissioning & As-Built Documentation

Only University approved technicians will be granted access to the Gallagher Server and FT Command Centre Operating System.

The Contractor shall provide Gallagher Door Licences to cover all additional doors installed. Any other Gallaher options installed must be fully licenced if required.

All devices must be fully tested and proven before being commissioned into operation

The University has a numbering protocol for all items of the system this includes a printed label on each door. (May be affixed to Reader in special situations) All interface panels must be fully labelled.

As built documentation showing the location and type of equipment installed is to be provided to the University with another copy left in the interface panel. The University will provide base building layout drawings

The Contractor is to coordinate with the University to alter or change any existing manual locking devices to achieve a fully operating system.

The manufacturer’s warranty period will apply to any equipment installed, and this warranty will be limited by the specific project or contractors stated warranty limitation.

Refer also to **Section 07 - Documentation Standards** for further as-built documentation requirements.

Compliance Checklist

Project Name: Date:

Submitting Consultant: Design Stage:

Section 18 – Security

Compliance Checklist

		Complies	Does Not Comply	Not Applicable	Comments:
1.0	**Design Standard Guidelines**				
All Clauses	Section 01 – General	□	□	□	
18.1	**Overview**				
18.1.1	Security Processes on Campus	□	□	□	
18.1.2	CPTED Principles for Passive Security	□	□	□	
18.2	**Active Security Considerations**				
18.2.1	Access Control Security Zoning	□	□	□	
18.2.2	Advertisement of Security Measures	□	□	□	
18.2.3	Existing Alarm Infrastructure	□	□	□	
18.2.4	CCTV	□	□	□	
18.2.5	Emergency Call Point System	□	□	□	
18.2.6	Duress Alarms	□	□	□	
18.3	**Passive Design Considerations**				
18.3.1	Access: Safe Movement and Connections	□	□	□	
18.3.2	Surveillance & Sightlines: See and Be Seen	□	□	□	
18.3.3	Layout: Clear and Logical Orientation	□	□	□	
18.3.4	Activity Mix: Appropriate Integration of Use	□	□	□	
18.3.5	Sense of Ownership and Care	□	□	□	
18.3.6	Quality Environments: Well Designed, Managed and Maintained	□	□	□	
18.3.7	Physical Protection: Appearance & Function	□	□	□	
18.4	**Materials & Equipment**				
18.4.1	Entry Devices	□	□	□	
18.4.2	Exit Devices	□	□	□	
18.4.3	Specified Lock Equipment	□	□	□	
18.4.4	Sliding & Swing Doors	□	□	□	
18.4.5	Fire Release Action on UOC Sites	□	□	□	
18.4.6	Standalone Security Alarms	□	□	□	

Compliance Checklist

Project Name:	Date:
Submitting Consultant:	Design Stage:

Section 18 – Security Compliance Checklist		Complies	Does Not Comply	Not Applicable	Comments:
18.4.7	Power Supplies and Battery Back Up	□	□	□	
18.5	**Installation Requirements**				
18.5.1	Cabling	□	□	□	
18.5.2	Commissioning & As-Built Documentation	□	□	□	

Date:	□ Acceptable
University Reviewer:	□ Acceptable subject to comments

Compliance Checklist

Project Name:	Date:
Submitting Consultant:	Design Stage:

Section 18 – Security Compliance Checklist	Complies	Does Not Comply	Not Applicable	Comments:
Signed:		□	Resubmission required	