SECTION 13: SECURITY

Contents

13.1 INTRODUCTION

The section provides the minimum standards for the electronic security design for new developments and/or upgrades to existing buildings.

The building security concept shall be established during the design stage of each project and shall be based on a risk-based approach. The design consultant shall meet with the University Security Manager and relevant stakeholders to identify the security risks which are required to be mitigated. These security measures shall become the basis of the security concept design. The design consultant shall then develop the detailed design based on the security concept design.

The design consultant is required to produce their own project specification which incorporates this section and other sections of the Design Standards, notably, the Electrical Services, Fire Protection and Detection Services, External and Internal Building Elements and Standards for the installation of Telecommunication Networks; together with the requirements of all relevant codes, standards and good practice guides.

This section of the Design Standards only takes into consideration the physical security measures employed to deter, detect, and delay unlawful activity. Information Technology security measures are outside the scope of this document.

13.2 PRINCIPLES OF SECURITY CLASSIFICATION

The security classification of buildings, or areas within buildings, is based on the degree of damage which could be caused to the University through personal injury; loss of, or damage to property (including intellectual data) or interruption to a critical service.

13.2.1 Classification Criteria

The following is a general list of functions of particular concern requiring security consideration:

- Storerooms containing radioactive material or dangerous chemicals;
- Containment labs;
- End of Trip Facilities and Bike Hubs;
- Computer labs, with after-hours access;
- Biological resource facilities;
- Lecture theatres;
- Areas of substantial intellectual or monetary value (e.g., computer software design, saleable medical research etc.);
- Places handling substantial quantities of money;
- Areas in which critical administrative functions are carried out (e.g., office of The Vice Chancellor, University Information Division Computer Room, Information Division Plant, Network Distribution Switch rooms, Student Records Office and Comms rooms);
- Sensitive waste storage;

- Mission critical plant rooms or infrastructure such that the loss of functions would significantly disrupt the day-to-day operations of the University or areas of the University;
- Rooms where examination papers are stored;
- Rooms or buildings housing vulnerable or “at risk” individuals;
- Extended hours areas, such as informal study spaces and libraries;
- Accommodation facilities;
- Crowded places, such as sports stadiums, concert event spaces, etc. These spaces may be outdoors as well as indoors.

This list is not meant to be exhaustive. There may be rooms or areas other than on the list above requiring security consideration. These rooms or areas should be clearly identified by the design consultant based on the risk-based approach described.

13.2.2 Application to Building Design

The protection afforded to the assets is linked to the hierarchy of space that exists within all environments. The general hierarchy is as follows:

Category of Space	**General Condition of use/access**	**Comments**
Public	Areas that are freely accessible to members of the public.	External spaces, buildings with free access.
Semi-public	Areas that are accessible to members of the public by invitation but where there are no specific criteria in place.	Social environments, sporting facilities and free events.
Semi-private	Areas that are restricted to those with a legitimate reason for being there plus invitees that meet agreed criteria.	Areas where visitors are required to pay a fee or are subject to some form of screening.
Private	Areas that are restricted to those with a legitimate reason for being there. Visitors are escorted at all times.	Working areas of the University restricted to staff members and students etc. Visitors carrying out specific tasks.
Secure	Areas where access is limited to nominated individuals only. Visitors are not normally allowed but where necessary are escorted at all times.	Areas containing critical equipment, facilities or items of intrinsic value. Visitors are normally excluded except for essential maintenance staff.

In accordance with the principles of Crime Prevention through Environmental Design (CPTED), the territorial definition of these spaces shall be clear and unambiguous; in addition, the transit between the spaces shall be reflected in the form and function of the access control measures to be adopted.

The greater the difference in status between adjacent spaces, the more robust shall be the physical measures, the more stringent the access controls between them and the level of surveillance practiced. Therefore, access to a secure area should be via a controlled door (appropriate to the location and usage), be alarmed and monitored by OSD; whereas access to a semi-private area may not require a controlled door, an

alarm or to be monitored unless these are identified as appropriate controls during the risk assessment process.

Building Design principles relevant to security include:

- End of Trip Facilities and Bike Hubs;
- Computer labs, with after-hours access;
- Biological resource facilities;
- DDA and OH&S requirements;
- Passenger lift control functions
- Design of the shell of the building;
- Design of internal user areas
- Security of accessible low-level windows etc;
- Combining all high-security functions to one area of a building
- Lighting design;
- Crime Prevention Through Environmental Design (CPTED;
- Specific operational requirements of the building or areas.

Refurbishments and new building designs shall have as a minimum but not limited to:

Access Control:

- All main entry points and electronic locking and monitoring of all external doors;
- All facilities occupied by students after hours;
- All floor entry points including lift lobbies, all stairwells where possible;
- All communications rooms;
- All biological resource facilities;
- All centrally managed teaching and learning spaces;
- All containment level spaces i.e PC 3, 4, QC 3, 4.

Fire Requirements:

- An interface between the fire panel and Gallagher panels to indicate an alarm and to drop power to all electronically locked doors;
- In the event where a door cannot be fail safe, discuss with the University Security Manager for approval

Intrusion Detection:

- Required to monitor the main entry level and perimeter entrances;
- An assessment of all spaces shall be undertaken to determine requirements and reviewed in consultation with the University's security office to be incorporated into the design;

- Intrusion detection devices (e.g., PIRs, Reed Switches, etc) should have a Remote Arming Terminal (RAT) installed at strategic locations for arming/disarming and to provide alarm/system status.

Emergency Services:

- An Emergency Services Key Vault (Grey Box) keyed to the University's CyberLock electronic key system will be supplied by the University Security Office and installed by the builder.

Optical Surveillance Devices (OSD):

OSD coverage to a standard commensurate with the location and purpose of the image. Areas to be covered include:

- All entry points;
- External coverage of external doors;
- Entry/exit points of private or restricted areas;
- Student A/H facilities and computer rooms
- Entry points to a floor;
- General circulation spaces;
- Alarmed locations, where required by the University;
- External public gathering spaces and thoroughfares surrounding University properties.

13.3 UNIVERSITY APPROVED CONTRACTORS

All security system hardware must be installed by a University of Melbourne approved security contractor.

All restricted master keyed locks, cylinders and keys must be supplied through the University of Melbourne's nominated locksmith.

A current list of approved security contractors and the current nominated locksmith are available from the University Security Office or University Project Manager.

13.4 OPERATIONAL REQUIREMENTS

Security works must meet all the requirements of national and local statutory authorities and shall be in accordance with the latest version of the following:

Standard Reference	Description
AS/NZS 3080:2013	Telecommunications Installations – Generic cabling for commercial premises
AS/CA S008:2010	Requirements for customer cabling products
AS/ACIF S009:2013	Installation requirements for customer cabling (Wiring rules)

AS/NZS 3084:2017	Telecommunications installations – Telecommunications pathways and spaces for commercial buildings
AS/NZS 3085.1-2004	Telecommunications installations – Administration of communications cabling system – Basic Requirements
AS/NZS 3000:2018	Electrical installations (known as the Australia/New Zealand Wiring Rules)
AS 2201.1-2007	Intruder alarm systems – Client's premises – Design, installation, commissioning and maintenance
AS 2201.2-2004	Intruder alarm systems – Monitoring centres
AS 2201.3-1991	Intruder alarm systems – Detection devices for internal use
AS 2201.4-1990	Intruder alarm systems – Wire-free systems installed in Superintendent's premises
AS 2201.4-1990/Amdt 1-1990	Intruder alarm systems – Wire-free systems installed in Superintendent's premises
AS 2201.5-2008	Intruder alarm systems – Alarm transmission systems
AS/NZS 2201 Set-2008	Intruder alarm systems set
AS 4360	Risk Management
HB 167:2006	Security risk management
ASTM F571-87 (2016)	Standard Practice for Installation of Exit Devices in Security Areas
AS/NZS 60950.1:2015	Information Technology Equipment – Safety – General Requirements
AS 4806.1-2006	Closed Circuit Television (OSD) Management and Operation
AS 4806.2-2006	Closed Circuit Television (OSD) Application Guidelines
AS 4806.3-2006	Closed Circuit Television (OSD) PAL signal timings and levels
AS 4806:4-2008	Closed Circuit Television (OSD) Part 4: Remote Video
AS 5007 – 2007	Powered doors for pedestrian access & egress
AS 1428	Design for Access and Mobility

- Building Code of Australia and building permit conditions;
- Electricity supply authorities;
- Fire brigade requirements;
- The rules and regulations of local government;
- All other relevant codes and standards.

13.5 ELECTRONIC SECURITY SYSTEMS

The *Gallagher Command Centre Site Management System* shall be specified for intrusion detection and access control applications in university buildings and/or areas.

IndigoVision cameras and Network Video Recorders (NVRs) shall be specified for surveillance and monitoring purposes.

2N IP Intercom units shall be specified for intercom units and Blue Phone communication purposes.

13.5.1 Building Access Control Design Criteria

Online Access Control System

The microprocessor-based control unit shall be a fully redundant system (that shall remain in operation if the *Security TCP/IP network* is offline) with a distributed processing network topology.

Whilst operating, the system shall grant or deny access through a door to a card holder based on the presentation of a properly encoded card to an authorised card reader at a valid time of day, day of week and card status. Each individual card transaction, both through entry or egress card readers, shall log as a separate event at each door, i.e., entry shall be distinguishable from egress at the same door.

The system shall be connected to a dedicated security Virtual Local Area Network (VLAN). Battery backup shall be provided to maintain normal access control operations including all memory and the real time clock calendar for not less than 8 hours should mains power fail. The battery shall be automatically recharged when mains power is applied.

When the dedicated security LAN becomes offline, all events and transactions shall be retained in its memory. These events and transactions shall automatically be uploaded to the database of the Gallagher Command Centre management software when the security LAN connection is re-established.

All events and transactions shall be stored in the central database with time & date stamps. The time & date stamps shall be referenced for security data retrieval.

Gallagher Command Centre site management software is in use at the University of Melbourne. All building security systems shall be connected to the Security network and shall be programmed as per sections 13.13, 13.14 and 13.15 of these Design Standards.

Note that not all Gallagher Command Centre management software functionalities are required. The Security Contractor shall refer to the capabilities of the Gallagher Command Centre management software and liaise with the Security Office to identify specific features or functionalities for implementation.

Specific requirements shall include (but not limited to) the following:

- In principle, the design should encourage persons (staff, students, visitors and contractors) to enter or leave a building through the same access control points;
- The design should limit the number of public access control points. As far as practical, public access should be limited to one door;
- Doors shall be named according to conventions outlined in section 13.15 of these design standards;
- Floors shall be named according to convention outlined in section 13.15 of these design standards;
- Security controllers shall be named according to location;
- Label all security panels, security equipment and cables according to a labelling scheme agreed with the University Security Office during installation;
- Provide regulated power supply and battery system to back up the operations of the access controller and electronic door locking devices for 8 hours when there is a mains failure. Refer to section 13.11.11 for details;
- Label all batteries with the installation dates;

- Mechanical key override must be provided for all external access control doors and any internal access control doors that have no secondary path of access to the internal side of the door;
- All mechanical cylinders must be keyed to the University of Melbourne's restricted keying system as nominated by the University Security Manager;
- All handles on electric strike doors shall be locked to avoid doors being opened mechanically by the handle and triggering a ‘forced door’ alarm;
- Install door closers on all monitored doors.

The design consultant shall discuss with the University Security Manager and other stakeholders to identify other specific requirements for implementation.

Electronic Key System

The electronic key system shall be CyberLock.

A user shall be able to turn the cylinder and open a door if the user carries a valid electronic key (with pre-programmed data).

The transaction or event shall be kept within the memory of the electronic key. The data shall be uploaded to the system database when the user presents the key to an online reader. At the same time when a user presents his/her key to an online authorizer, the programmed data stored in the electronic key memory will be updated (e.g., to update the list of accessible doors, to cancel key, to delete a door from the accessible door list, etc.).

Electronic key cylinders shall be utilised as an alternative to an online access control installation for ‘back of house’ services areas, where installation of an online access control solution is difficult or not viable e.g., roof access hatches that can’t be locked via a wired electronic locking device.

In addition, the electronic key system shall be used as the override cylinder on all comms room online access control installations, refer section 13.5.2 – Door requirements.

In all other instances, an online access control solution is preferred. Usage of the CyberLock system within a security design requires approval by the University Security Manager.

Door Requirements

The following sections detail the security door hardware required for each type of door. The design consultant shall recommend the required door type for each access control point based on the outcomes of the security risk assessment. If a required door hardware configuration does not match any one of the door types, the design consultant shall consult the University’s Security Office to agree with the proposed configuration.

It should be noted that not all door hardware (e.g., lever, handle, thumb turn, key cylinder, door seal, etc.) are included in the following sections. Door hardware is normally included in the door hardware schedule under the architectural package. The design consultant is required to coordinate with the Project Architect to ensure all security-related door hardware is included in the door hardware schedule.

Bottom rail locks and Euro cylinder are not to be installed.

Push and pull plates are the preferred mechanical hardware on doors secured by Mag Locks, additional door locks are not required.

Main Entry Doors

Where double doors are installed, the inactive leaf shall be secured with a lockable ADI panic bolt of no less than 300mm on the bottom of the door and a non-lockable panic bolt no less than 400mm on the top of the door. Alternatively, a lockable ADI panic bolt can be installed at the top of the door no less than 500mm in length. Lockable ADI panic bolts are to be keyed to the University restricted master key system, as nominated by the University Security Manager.

Door Types

FEATURES / HARDWARE	DOOR TYPE			
	A	B	C	D
ENTRY: Proximity card reader installed on the unsecured side of the door (See section 13.11.7)	X	X		
EGRESS: Proximity card reader installed on the secured side of the door (See section 13.11.7)	X			
EGRESS: Push button installed on the secured side of the door unless an electric mortice lock is used		X		
Electric door strike, electric mortice lock or magnetic lock. The Security Contractor shall select the appropriate door lock device to suit the specific door type	X	X	X	
Local door alarm sounder for DOTL and Forced Door alarms (except in biological resource facilities, unless approved otherwise)	X	X	X	X
Break glass door release unit. The break glass unit shall be installed on the secure side and shall be monitored	X	X	X	
Reed switch door monitoring	X	X	X	X
ADI lockable panic bolt on fixed leaf (where applicable)	X	X	X	
ADI or other University approved blocker plate installed (where applicable)	X	X	X	X
Automatic door closer	X	X	X	X
Door status indicator			X	
Custom signage (where applicable)			X	
No external door furniture on external emergency exit doors			X	

Type A Door (Full Access Control)

These doors shall have the following hardware/features:

- All Type A doors shall be controlled by Gallagher Controller 6000 Controllers;
- ENTRY: T15 Multi-Tech card reader installed on the unsecured side of the door (See section 13.11.7);
- EGRESS: T15 Multi-Tech card reader installed on the secured side of the door (See section 13.11.7);
- Electric door strike, electric mortice lock or magnetic lock. The University's preference is for electric door strikes to be used. The design consultant, in conjunction with the University's Security Manager shall select the appropriate door lock device to suit the specific door type;
- Break glass door release unit. The break glass unit shall be installed on the path of egress and shall be monitored;
- Reed switch door monitoring;

- Local door alarm sounder for DOTL and Forced Door alarms;
- ADI lockable panic bolt on fixed leaf (where applicable);
- ADI or other blocker plate approved by the University Security Manager (where applicable);
- Automatic door closer.

Each entry/egress card transaction at each door shall be logged as a separate transaction in the access control system database.

Type B Door (Partial Access Control)

These doors shall have the following hardware/features:

- All Type B doors shall be controlled by Gallagher Controller 6000 controllers;
- ENTRY: T15 Multi-Tech card reader installed on the unsecured side of the door (See section 13.11.7);
- EGRESS: Push button installed on the secured side of the door unless an electric mortice lock is used;
- Electric door strike, electric mortice lock or magnetic lock. The University's preference is for electric door strikes to be used. The design consultant, in conjunction with the University's Security Manager shall select the appropriate door lock device to suit the specific door type;
- Break glass door release unit. The break glass unit shall be installed on the path of egress side and shall be monitored;
- Reed switch door monitoring;
- Local door alarm sounder for DOTL and forced door alarms (where applicable);
- ADI lockable panic bolt for fixed door leaf (where applicable);
- ADI or other blocker plate approved by the University Security Manager (where applicable);
- Automatic door closer.

Any Partial Access Controlled Door shall be cabled such that a future upgrade to a Type A door shall not require any additional cabling between the security controller and the future egress T15 Multi-Tech card reader;

Each entry card and push button transactions at each door shall be logged as a separate transaction in the access control system database.

Type C Door (Controlled / monitored / 24 Hour emergency doors)

These doors shall have the following hardware/features:

- All Type C doors shall be controlled by Gallagher Controller 6000 controllers;
- Electric door strike, electric mortice lock or magnetic lock. The University's preference is for electric door strikes to be used. The design consultant, in conjunction with the University's Security Manager shall select the appropriate door lock device to suit the specific door type;
- Local door alarm sounder for DOTL and forced door alarms;

- Break glass door release unit. The break glass unit shall be installed on the path of egress side and shall be monitored;
- Reed switch door monitoring;
- Door status indicator;
- ADI lockable panic bolt for fixed door leaf (where applicable);
- ADI or other blocker plate approved by the University Security Manager (where applicable);
- Automatic door closer;
- No external door furniture on external emergency exit doors;
- Custom signage.

Any Partial Access Controlled Door shall be cabled such that a future upgrade to a Type A door shall not require any additional cabling between the security controller and the future entry and/or egress T15 Multi-Tech card reader or push to exit button.

Each transaction shall be logged in the access control system database.

Type D Door (Monitored Door)

These doors shall have the following hardware/features:

- All Type D doors shall be controlled by Gallagher Controller 6000 controllers.
- Reed switch door monitoring;
- Local door alarm sounder for DOTL and forced door alarms;
- ADI or other blocker plate approved by the University Security Manager (where applicable);
- Automatic door closer.

Each transaction shall be logged in the access control system database.

Special consideration shall be taken regarding doors of the following nature.

Comms Room Doors

Access control door type A or B (minimum) fitted with Padde ES9000 and CyberLock key system as an override, as opposed to the traditional physical University master key system unless otherwise approved by the University's Security Manager.

Plant Room Doors

Type B access control doors shall be nominated for plant room access control. The traditional physical University plant room master key system shall be used on all Plant and Comms risers unless otherwise approved by the University's Security Office.

Biological Resource Facilities

Local alarm sounders and strobes shall be excluded from installation into these facilities unless otherwise approved by the University Security Manager.

Electro-Mechanical Doors

The installation of an electro-mechanical operated door (e.g., main entry doors) shall meet Australian Standards AS5007 – 2007 & AS1428.

Where electronic access control is installed, the system shall be programmed to lock/open the main entry doors based on user defined time schedule. T15 Multi-Tech card readers shall allow access outside normal business hours. The high-level wiring configuration to achieve this has been illustrated in Appendix A – Automatic Door Wiring Diagram, of this section of the Design Standards.

Electro-mechanical doors shall provide:

- Audible alarm at the door for DOTL and forced door alarms;
- Monitored battery backup in the event of mains power failure. In the event of an electrical power failure, the battery backup system would keep the doors locked and secure;
- The ability to physically monitor the doors when open/closed;
- The ability to monitor the status of the electric lock;
- Fail safe mode allowing a person to open the doors manually when there is a mains failure;
- Entry & exit radar detectors;
- Lock it Well K2 two position spring return key switch keyed to the University's master key system (IN);
- Lock it Well K4 four position key switch (auto/exit/open/locked) keyed to the University's master key system (OUT).

The electronic access control system shall interface with the door actuator at low-level via a relay. When access control functionalities are activated (e.g., during afterhours), the entry and exit radar detectors shall be deactivated accordingly.

The design consultant shall arrange for the University's Security Office to supply the correct cylinder in the K2 (IN) & K4 (OUT) key switches prior to installation.

The door operator shall provide separate individual alarms to the security system (Gallagher Command Centre) when:

- There is a 240-volt power failure at the door;
- low battery voltage is detected at the door;
- There is a fault with the battery charger.

All alarms shall simultaneously be reported to the University's Security Office directly and appear at the Gallagher Command Centre Server & workstation to alert an operator.

Sliding Door (Non-auto)

Non-automatic sliding doors should not be fitted with electronic access control devices, due to the ability for them to be left open and not automatically secure after use. Suitable Lockwood mechanical door locking hardware should be installed on any non-automatic sliding door.

Bicycle Hubs – Access Control:

The following equipment shall be provided:

- Doors to be Type A;
- T15 Multi-Tech card readers (2);
- Padde single magnetic lock;
- Door closer/Self closing hinges;
- IndigoVision camera;
- Break glass;
- Black powder-coat pedestal to suit break glass and card reader.

13.5.2 Electronic Intrusion Alarm System

Any Intrusion alarm systems installed at the University of Melbourne shall be based on Gallagher Controller 6000 equipment. The alarms are monitored from the University of Melbourne Security Control Room.

Specific requirements shall include (but not limited to) the following:

- Appropriate intrusion detection devices shall be placed at locations or areas identified in the risk assessment;
- The design consultant shall select the appropriate device types to meet the specific requirements;
- Controller 6000 shall be programmed for event driven data transfer with the University's Gallagher Command Centre servers via the University's IP network. A TCP/IP port to be provided adjacent to the Controller 6000. The University Project Manager shall be responsible for acquiring an appropriate IP address from the University of Melbourne Security Office;
- Remote Arming Terminal (RAT) - all RATs shall be the Gallagher T20 MultiTech Reader device;
- Alarms shall sound locally and simultaneously be reported to the University of Melbourne Security Control Room;
- At each door, or where there is a passive infra-red detector in the area, a sounder shall be installed locally. When an alarm is triggered, the sounder shall go off, providing alarm signalling locally;
- All alarm inputs shall be terminated with end-of-line resistors recommended by the manufacturer;
- Each alarm device shall be wired to a separate input allowing each device to be monitored individually;
- Alarms shall be monitored for 4 states (i.e. normal, alarm, tamper (open circuit) and tamper (short circuit));
- Provide regulated power supply and battery backup of the intrusion detection system for 8 hours when there is a mains failure. Refer to section 13.1.11 for details;
- A Licensed and University approved structured cabling contractor shall be engaged to connect the intrusion alarm system to the Gallagher Command Centre management software by patching through the Security TCP/IP Network;
- Interface with the OSD system allowing the cameras to be linked to alarm activations with pop-ups on high priority alarms.

- All inputs shall be named according to convention as per section 13.15;
- As required, alarm inputs shall be tied with outputs providing the capabilities to interface third-party systems or to switch on/off an alerting device, e.g.:
- After a DOTL alarm is acknowledged, the sounder shall be deactivated automatically;
    - When an alarm is triggered, switch on the lights installed within the alarmed area

The design consultant shall discuss with the University Security Manager and other stakeholders to identify other specific requirements for implementation.

13.5.3 Optical Surveillance Devices (Formerly OSD Systems)

This section has been renamed to bring its terminology in-line with the Australian Surveillance Devices Act 2004.

Operational requirements for each camera shall be developed in accordance with AS4806.1-2006 allowing field of view and detection grade to be specified, along with all other relevant Australian Standards, Codes and Authorities.

General Principles

The use of Optical Surveillance Device(s) (OSD) at the University of Melbourne is to assist security personnel to provide staff and students with a safe environment in which they can work and study. This is primarily achieved with OSD through:

- Active observation;
- Providing a visual deterrent;
- The recording of images.

General Camera Requirements

- All power for University security cameras shall be derived from the comms room to which it has been cabled back to. The use of local GPO's (general purpose outlets) to power Security cameras is not permitted;
- No camera will be fixed to a heritage building environment without the appropriate approvals;
- Planning and placement of all underground infrastructure, including pull boxes, must be approved by the University's Project Manager;
- Placement of external camera poles will be subject to agreement with the University Security Manager and Grounds Manager;
- Any poles on which security equipment is mounted must be engineered for the load imposed;
- As part of the installation commissioning process, all cameras must be adjusted (if required) to ensure the best possible picture is achieved during the hours of darkness;
- Wherever possible cameras will be placed at a height that allows them to be safely accessed for repairs and maintenance without the need for specialised access equipment;

- External cameras will be of a vandal proof design with no loose cables or easily vandalised mounting brackets;
- Traffic control zone cameras must be mounted so as to provide optimum views without impeding the flow of traffic or coming into contact with pedestrians or vehicles;

In accordance with applicable legislation, cameras will not be used to capture or view private activities unless clear and obvious signage is placed within the area in which the activities take place. Cameras will not be installed in private areas such as toilets or change rooms.

Camera Placement Requirements

The purchase or installation and placement of any security camera must be authorised by the University Security Manager.

Camera specification and location must be individually assessed based on the specific environmental conditions and desired purpose for the camera. OSD system design and camera placement is to be based on industry best practice and be provided to the University Security Manager for review and sign-off.

All cameras designated to provide identification images must be situated between 2.4m and 2.8m from the fixed floor level.

Where possible, all cameras are to be mounted in such a manner, and at such a height, as to allow for ongoing maintenance without specialised equipment.

Recording Equipment

The IndigoVision Network Video Recorders (NVRs) shall be specified for recording Security cameras for security purposes.

Prior to installation of cameras, recording streams/licenses shall be confirmed with the University's Security Office.

Where any new installation requires additional recording capability additional NVRs may be required. Installation of four (4) or more cameras requires the installation of an NVR with sufficient capacity to record a minimum of eight (8) external cameras of the same specification as those being installed.

***NOTE**: A multi-sensor camera is considered one (1) camera per sensor for recording purposes.*

It is the responsibility of the security contractor to ensure all new devices have the appropriate licenses required to capture OSD images onto the University of Melbourne's IndigoVision network.

All recording equipment shall be connected to the University of Melbourne network and configured to synchronize their clocks with the University NTP server.

NVRs must be installed in University dedicated Network racks housed in comms rooms.

NVRs that are 100TB or more must be directly connected via fibre to the University's data network.

Recording Requirements

All Security cameras shall meet the following recording requirements:

- Recording capacity: 30 days;
- Alarm / Event triggered recording: 25 fps;
- Recording format: H.265;
- All cameras shall record at a minimum of 4096 kbps upon alarm or event;
- All external cameras and entries to buildings shall record at 25 fps 24/7 at a minimum of 4096 kbps;
- All internal cameras (excluding entry points) shall record at 25 fps, 24/7 at a minimum of 4096 kbps during Alarm / Motion / Event triggered recording, but can otherwise be set to relevant ACF or background recording functions as mentioned above;
- All cameras shall be recording 24/7.

Camera Types

Cameras shall be compatible with the IndigoVision recorders and Control Centre management software. The preferred specification is for a suitable megapixel (MP) camera to be used. At a minimum, 1080p high definition (HD) specification cameras shall be used.

To be compatible with the IndigoVision recorders and Control Centre management software all cameras installed should be selected from the IndigoVision range of products or ONVIF compatible products certified as compatible by IndigoVision and approved for use by the University's Security Manager. All cameras shall be supplied with Enhanced Management Software license. All ONVIF cameras shall be supplied with appropriate licenses to record to their designated NVR.

It is the responsibility of the security contractor to ensure all new devices have the appropriate licenses required to stream and record OSD images onto the University of Melbourne IndigoVision network.

Camera Type	
Dome	A
Bullet	B
Multi-sensor	C
Fisheye	D
PTZ	E

Location	Camera Type				
	A	B	C	D	E
Offices	X				
Building Entrances	X	X	X		
Retail	X		X	X	
External Building and Grounds Coverage	X	X	X		X
Campus Entrances		X	X		X
General Internal Circulation Spaces	X		X		
Labs	X			X	

Galleries	X		X	X	
Libraries	X		X	X	
Theatres	X		X	X	
Learning and Teaching Spaces	X		X	X	
Lift Lobbies	X		X		
Escalators	X		X	X	
Accommodation/Residential	X	X	X		
Car Parks	X	X	X		
Bicycle / Scooter Hubs	X	X	X		
Features					
Minimum 4MP	X	X	X	X	X
IR	X	X	X	X	X
Analytics	X	X	X	X	X
Overview Coverage	X	X	X	X	X
Facial Identification	X	X	X		
Retail/Libraries	X		X	X	
Pedestrian/Vehicular	X	X	X		X
License Plate Recognition		X			
Campus Entrance/Object Identification		X	X		

Dummy Cameras

Dummy cameras will not be used. It is the responsibility of the security contractor to ensure any newly installed device is operating and recording as soon as practical after its physical installation.

Operational Requirements

The University shall define the operational requirements for OSD systems using the parameters set out in the Australian Standard AS4806.2-2006. The definition shall include:

- Coverage grade – identification, recognition, detection, monitoring and vehicle number plate visual recognition;
- Image size at maximum target distance – percentage of picture height;
- Field of view (FoV);
- Maximum target distance;
- Mounting height;
-

General Standard Camera Guidelines

Camera options for any space internal or external must be approved by the University Security Manager.

13.6 MECHANICAL SECURITY SYSTEMS

All mechanical locks (and associated keys) for doors, access hatches, services areas and the like, must be part of the University of Melbourne's restricted master key systems.

For all new buildings and refurbishments, the project team must provide a door hardware schedule to the University's nominated locksmith, who will provide a Keying Schedule outlining the relevant locks and key hierarchy structure for sign off by the University's Security Manager and project team.

The project team will be responsible for coordinating the keying requirements of all stakeholders, including the University's Security Office and providing this information to the University's nominated locksmith.

All door hardware must meet University Design Standards, as outlined in Section 5 (External and Internal Building Elements) and throughout this section.

13.7 EMERGENCY HELP POINTS (BLUE PHONES)

Blue Phones are an essential part of the University's safety offering and shall be considered as part of any security design. Consideration must be made in conjunction with the University Security Manager.

Blue Phones form part of the broader University security services and as such are not required as part of every project, however assessment and determination must be made on a project-by-project basis.

Current specifications can be requested from the University's Security Office.

13.8 LIGHTING

The main external entrance to a building shall be well lit after dark. Refer to Section 7 - Electrical Services for details of lighting controls.

At other perimeter doors and other ground level points of potential access shall be well illuminated by security lighting after dark as per the Australian Standards (AS/NZS 1158.3.1).

At locations or areas where digital recording Security cameras will be installed, the location or placement of light fittings will be critical. The security lighting from the building shall extend and integrate into existing light corridors such that continuous lighting of trafficable paths is maintained.

In order to allow high quality video footage to be captured, the lighting level shall be a minimum of 15 lux at a horizontal level of 1.5 meters above the finished floor level. The contrast ratio between the maximum to minimum (average) lighting level shall be no greater than 1:3.

13.9 RADIO EQUIPMENT

Buildings with basement levels or underground car parks shall have a radio repeater installed to facilitate communications on the digital radio network in place at the University.

13.10 INTERFACE WITH THE FIRE PANEL

The Gallagher system shall interface with the fire panel at low-level via relay. When a fire alarm is triggered, a relay output shall be provided by the fire panel. When this relay output is received by the Gallagher Controller 6000 controller, the Gallagher Command Centre security management software shall display an alarm indicating that power to the door locks has been lost.

All electronic access-controlled doors should release (but not open) upon a fire alarm via this method. Arrangements for a door identified as a high-security door are to be agreed with the University Security Manager.

13.11 SECURITY EQUIPMENT (HARDWARE)

13.11.1 Electric Door Strike

Electric door strikes shall be PADDE ES 9000 or FSH FES90M-P. Blocker plates shall be installed on external doors to prevent tampering with electric strikes. Each door strike shall be complete with:

- Keeper security status monitoring (i.e., wired for both N/O & N/C);
- Each electric strike shall be configured for fail safe mode.

13.11.2 Electric Mortice Lock

- Electric mortice lock (with dead latch) shall be LOCKWOOD 3574 EL AM2R/L--SC. Each electric mortice lock shall be configured for fail safe mode;
- The mechanical override lock cylinder shall be keyed to the University Master key system;
- Cable transfer devices shall be specified as Lockwood LC8810 or LC8811 stainless steel concealed recessed flex conduit.

13.11.3 Magnetic (Static) Locks

- Magnetic locks shall be Lockwood PADDE Z8 monitored single or double electromagnetic lock or from the FSH ECO5700, FEM5700 monitored range;
- The design consultant shall obtain permission from the University Project Manager prior to specifying magnetic locks;
- Magnetic locks shall require separate power supplies each with battery back-up and failure monitoring, via interface to the Gallagher Command Centre management software;
- Each magnetic lock shall be fused individually.
- All mounting screws shall utilize lock-tight as per manufacturers recommendations.

13.11.4 Controller Panels

All new Security Controller panels shall be Gallagher Controller 6000 (C300100). The controller shall be connected to the security VLAN and shall communicate directly to Gallagher Command Centre Site Management Software.

Controller 6000's shall be housed within a Gallagher Cabinet or approved alternative within Comms rooms where one exists.

All panels shall have tamper status monitoring via mechanical switches in the cabinet, or via optical switches located on the Controller. Tamper alarms report to the University Security Control room.

For typical applications where Card Readers are required, The Controller 6000 will be expanded upon with a Gallagher 8H Module (C300182) or 4H Module (C300142).

13.11.5 Controller Cabinets

Controller equipment shall be housed within a Gallagher Dual Cabinet (C200104). Where space doesn't permit a Dual Cabinet, a Gallagher Single Cabinet (C200100) should be used.

All Gallagher cabinets must be installed with glands for cable entry and exit points, to maintain cabinet IP ratings.

All cabinets shall be keyed alike (refer to the University Security Office for keying instructions).

Where space is an issue, third party cabinets can be used, following approval from the University's Security Office.

Controller cabinets are to be labelled with the building code and controller number as per the naming convention specified in section 13.15.

When possible, GPO's powering the controller equipment and Network connection points shall be located immediately above the cabinet.

13.11.6 Expansion Interface Modules

Expansion Interface modules are used to add alarm monitoring points and output control points to the security system. Subject to the requirements of each project, the appropriate input/output modules shall be selected for the job.

Appropriate modules are:

-HBUS 16 In 16 Out Board (C300688)

-HBUS 8 In Board (C300680)

-HBUS 8 In 4 Out Board (C300684)

-HBUS 8 In 2 Out Door Module (C300660)

Expansion modules must be wired as per the manufacturer's requirements.

All Expansion Interface Modules shall be housed within a security cabinet that is monitored for tampering, as per section 13.11.4.

13.11.7 Access Cards

Access cards (Staff, Student or Visitor cards) shall be issued by the University of Melbourne.

13.11.8 Card Readers

Gallagher T15 (C300480) Multi-Technology card readers shall be used on all new installations.

If the installation is part of an existing card reader system, the existing card readers and associated cabling shall be upgraded to the Gallagher T15 Multi-Technology card readers.

All card readers are to be installed at a height between 1000-1200mm providing easy access to disabled persons.

13.11.9 Request-To-Exit Button

- Touchless Button: Where required, the design consultant shall specify Neptune NEITB68W or similar as approved by the University Security Manager. The touchless buttons shall be installed at a height between 1000-1200mm adjacent to the controlled door. Additional cabling is required to ensure the LED indicator light is operational.
- Push Button: Where required, the design consultant shall specify Green mushroom head SEADAN SSE, 4350, DP/DT or similar as approved by the University Security Manager. The push buttons shall be installed at a height between 1000-1200mm adjacent to the controlled door.

13.11.10 Break Glass Units

Break glass release units shall be white in colour double-pole KAC WW2200/SW, SEADAN kw200/SW/B or similar approved by the University Security Manager. They shall be installed at a height of between 900-1000mm adjacent to the secure side of the door.

When the glass is broken in an emergency, the controlled door shall:

- Unlock automatically (1st pole);
- Initiate an alarm (2nd pole).

All break glass units shall be monitored for tamper and shall be installed along the path of egress.

13.11.11 Duress Buttons

A duress button shall be specified when there is a need for a silent alert in a threatening situation.

Examples include but are not limited to public facing receptions, health clinics, counselling services.

All new duress button installations/upgrades of existing must be accompanied by the installation of a Security camera, (see section 13.5.4). The location of the camera is to be confirmed with the University's Security Office prior to installation. Wireless duress buttons are generally not approved for use and are only to be specified with approval from the University's Security Manager in special circumstances.

Where required, the design consultant shall specify from the Honeywell 269R/270R/269SN range of hold-up devices or an alternate approved by the University Security Manager.

13.11.12 Assistance Buttons

An assistance button shall be specified when there is a need for communication between a person and the security control room. This may be in an emergency or as an alert.

Examples include but are not limited to: DDA bathrooms and change rooms, gyms.

Where possible these should be accompanied by the installation of a Security camera (see section 13.5.4). The location of the camera is to be confirmed with the University's Security office prior to installation.

Cameras should not be installed in bathrooms or changing rooms.

Where required, the design consultant shall specify from the 2N intercom range (see section 13.11.16)

13.11.13 Lockers

When a centrally managed locker system is specified, the Gallagher Locker Solution must be used. Allowance for installation of control panel for each locker i.e. equipment to be allocated a locker space or a bulkhead included. Please note this control panel must be able to be easily accessed.

Space allocation for a RAT for each locker bay is required.

Lock type must be supplied and installed by the security contractor. The University uses Core Electronics solenoid locks.

Cable to be supplied by the security contractor.

Cabling of the locker banks to be undertaken by locker manufacturer

Equipment fit-off including lock to be completed by security contractor on site once lockers in place and in working order.

Locker numbering must be top to bottom, left to right.

Numbering convention as per below:

Bay – Locker

01-001

Per building:

Each bay of lockers to be uniquely numbered.

Individual locker to be uniquely numbered.

All new locker solutions must be accompanied by the installation of a Security camera (see section 13.5.4). The location of the camera is to be confirmed with the University's Security Office prior to installation.

When a locally managed locker system is specified, preference is for a manual key or code system to be used to meet local user requirements.

13.11.14 Door Monitoring

Reed Switches

SENTROL 1078 1" (one inch) reed switch shall be specified for all doors connected to the access control or intruder detection systems.

Each encapsulated reed switch shall consist of an individual magnet to be installed in the door leaf. Under normal situations, the magnet shall be installed at 100mm from the leading edge of the door. Whilst the switch and the end of line circuitry (EOL) shall be mounted in each door jamb head at the location matching the mounting location of the magnet.

The magnet to operate the reed switch shall be concealed by recessing into the door leaf and the gap between the reed switch and magnet shall not exceed 4.0 mm.

For wide gap and roller door applications, other reed switches would be required. The design consultant shall recommend a brand and model to suit the application to the University's Security Manager for approval.

For applications which require surface mount reed switches, the design consultant shall recommend a brand and model to the University's Security Manager for approval.

Door Status Indicators

Door status indicators shall be specified for all Type C doors. Each door status indicator shall consist of:

- Clipsal series 2000 plate;
- Green LED (engraved: 'Door Available');
- Red LED (engraved: 'Door Unavailable').

The design consultant shall specify custom mounting brackets where required.

Local Door Sounders

All local door sounders shall be Fulleon AWD sounder (RS Stock No. 626-141) or other as approved by the University's Security Manager. They shall be triggered via software programming and driven off a separate relay located on the same controller that the associated door is wired to.

The local door sounder shall be programmed so that it is silenced when the associated alarm is acknowledged by the control room operators.

13.11.15 DC Emergency Power Supplies

12-volt/24 volt DC battery backup regulated power supply and battery system shall be specified to maintain power to the electric locks and security systems (including access control, intrusion detection and OSD systems) for an 8 hour period should normal "mains" power be disrupted. The backup power supply system shall be fully monitored by the Gallagher Command Centre security system.

13.11.16 240 Volt Power Supplies

All security panels and other equipment & devices shall be wired on circuits dedicated to security. A Lock-dog shall be installed on each associated circuit breaker. Each 240V GPO shall be labelled with “ESSENTIAL SECURITY EQUIPMENT DO NOT DISCONNECT”.

13.11.17 Passive Infra-Red Detectors

Where required the design consultant shall specify from the Bosch Tritech range of PIR’s, or other approved by the University’s Security Manager. A dedicated Fulleon AWD sounder (RS Stock No. 626-141) or other as approved by the University’s Security Manager should be installed per room with any PIR installation in the absence of access-controlled doors in the area.

13.11.18 Glass Break Detector

Where required the design consultant shall specify from the Bosch DS110i Series Glass Break Detectors, or other as approved by the University’s Security Manager.

13.11.19 Intercom System

Where required the design consultant shall specify from the 2N Intercoms IP range of equipment for intercom applications. All new intercoms must be added into the University’s Cisco VOIP telephony system, 2N Access Commander system and any associated systems such as IndigoVision Control Centre, if required. Allowances for a 2N IP Gold License along with any other required licenses shall be made per intercom purchased.

13.11.20 Rising Bollards

Refer to Section 14.3 of the University Design Standards for minimum rising bollard requirements.

Security for rising bollards shall have the following minimum features:

- 2N IP range intercom
- Gallagher card reader
- VSD coverage of the vehicle, the rising bollards, and the traffic lights

13.11.21 Grey Boxes

All University of Melbourne buildings are required to have a University of Melbourne grey box installed for emergency service access. This includes all refurbishments and new building designs unless otherwise specified by the University’s Security Manager.

Grey boxes are keyed to the University’s electronic key system and are supplied by the University’s Security Office.

Installation must be completed by the builder and the following installation requirements apply.

- To be installed at main entry within one (1) meter adjacent to FIP or MIMIC panel whichever is applicable;

- To be fixed at a height of 900-1200mm, preferably into a concrete pillar or similar strength location;
- To be fixed in such a manner as to be unable to be removed without accessing the inside of the grey box;

The installation of a grey box is considered critical and must be completed prior to practical completion.

13.11.22 Key Switches

Where required, for electromagnetic doors and/or lifts or other applications, the design consultant shall specify that a Lock-it-well override key switch, with cylinder keyed to University master key system, shall be used. The following installation requirements apply;

- To be installed no more than one meter from door at a height of 900-1200mm unless otherwise approved by the University's Security Manager.

13.11.23 Condition of Equipment

All equipment supplied to the University must be new. The use of refurbished or second hand materials and parts is not permitted. Parts that include a manufacturers stamping must not exceed 18 months.

13.12 INSTALLATION AND MAINTENANCE REQUIREMENTS

All security installations shall be performed by businesses and individuals holding a Private Security License in accordance with the Private Security Act 2004 & Private Security Amendment Act 2010.

Electronic security devices shall only be installed and programmed by a specialist University of Melbourne approved Security Contractor. The Security Contractor must be Gallagher Command Centre accredited. Evidence of this accreditation shall be required prior to a log on to the management software is provided.

The design consultant must ensure that the project documentation includes a requirement that all installations are provided with a 12 month maintenance period which will run concurrently with the defects liability period.

Specific requirements shall include:

- The control of security devices shall be centralised via the Gallagher Command Centre site management software;
- Security data of all security devices shall be maintained in a single database (Gallagher database);
- The University requires that the Security Contractor shall be a direct Sub-contractor to the Builder - not to the Electrical Contractor;
- Graphical maps of the project area allowing icons of doors, break glass units, Gallagher panels, cameras, NVR's, remote arming terminals, PIRs, etc to be mapped.

13.13 SYSTEM PROGRAMMING

All programming into Gallagher Command Centre is to be completed by the University's nominated Gallagher programming contractor, and is to be completed as per the details outlined in these Design Standards, including Appendix B. For details of the current University nominated contractor, please contact the Security Office.

- Established programming and naming conventions as advised by the University Security Office shall be followed for any new programming entered into the system.
- All Security Panels shall be located on the graphic maps, including non-functioning devices.
- All doors shall be individually monitored for alarms and all transactions and events shall be logged in the access control system database.
- All cameras are to be programmed into Gallagher Command Centre with an icon placed on the graphical maps that allows the operator to view camera footage.
- All cameras are to be programmed into IndigoVision Control Centre, including all camera setup options, recording schedules, graphical mapping, surrounding camera locations and any other programming aspects in line with University programming requirements.
- All NVRs are to be programmed into Gallagher Command Centre.
- All NVRs are to be programmed into IndigoVision Control Centre, including all NVR setup options, iDRAC configuration, network interface aggregation, and any other programming aspects in line with University programming requirements.
- All intercoms are to be programmed into 2N Access Commander, as well as any other associated systems such as Gallagher Command Centre or IndigoVision Control Centre including icons placed on graphical maps that allows the operator to control intercoms.
- Where appropriate, alarm or events shall have camera associations mapped in programming, in that when an event occurs, the security operator is able to display the linked video footage at the time of the event. Such events include duress alarms, intercom calls, intrusion alarms, fire alarms, etc.
- The function of automatic arming & disarming and locking & unlocking of controlled/monitored doors shall be carried out individually via time zones.

During programming the security contractor shall confirm all system programming requirements with the University's Security Manager prior to completion.

13.14 GRAPHIC MAPS

Graphical maps are to be provided for all new building and refurbishment projects. These maps are to show the actual layout of internal walls and security devices. The Graphical maps should be provided in a tiered system (Home > Campus > Precinct > Building > Building Level) to allow for navigation to each security devices located on the building level.

The building level should include navigation buttons allowing the user to move to each level of the current building and to adjacent internal views of the same building (where applicable).

Graphic maps should be taken from the University's Archibus (Spatial Information Portal SISfm) system and imported into Gallagher Command Centre and IndigoVision Control Centre with a portion of the map describing the Building Number, Building Address, Level, Data Source and date of import of the image. (i.e. 203 - 215 Grattan Street Level 1 - SISfm – 1/1/2017).

13.15 NAMING CONVENTION

Security devices should be programmed using the following naming conventions for each device, as outlined.

Device Type	**Device Acronym**	**Naming Convention**	**Example**
Controller 6000	FT####	Bldg# - FT# "DeviceType" Location	203 - FT0001 L01 Comms Room
Expansion Board 8In/4Out	8IO#	Bldg# - FT# "DeviceType" BUS# Location	203 - FT0001 8IO0 L01 Comms Room
Expansion Board 16In/16Out	16IO#	Bldg# - FT# "DeviceType" BUS# Location	203 - FT0001 16IO1 L01 Comms Room
Expansion 8 In 2 Door Module	2DM#	Bldg# - FT# "DeviceType" BUS# Location	203 - FT0001 2DM2 L01 Comms Room
Remote Arming Terminal	RAT	Bldg# - "DeviceType" "BldgLvl" Description	177 - FT0008 RAT L03 Special Collect 1
Door	DR	Bldg# - "DeviceType" "BldgLvl" Description	387 - DR GND East Store Rm Ent
Door - Reed switch (Access Controlled)	RSA	Bldg# - "DeviceType" "BldgLvl" Description	387 - RSA MEZ East Store Rm Ent
Door - Egress	E/G	Bldg# - "DeviceType" "BldgLvl" Description	387 - E/G B01 East Store Rm Ent
Elevator (Lift)	LFT	Bldg# - "DeviceType" "Lift#" Description	387 - LFT1 Passenger High Rise
Elevator Floor	FLR	Bldg# - "DeviceType" " BldgLvl" "Lift#" Description	387 - FLR L01 LFT1 Passenger High Rise
Elevator Floor Access Zone	ACZ FLR	Bldg# - "DeviceType" " BldgLvl" "Lift#" Description	387 – ACZ FLR L01 LFT1 Passenger High Rise
Card Reader	C/R	Bldg# - "DeviceType" "BldgLvl" Description	387 - C/R Gnd East Store Rm Ent

Access Zone Standard	ACZ	Bldg# - "DeviceType" "BldgLvl" Description	387 - ACZ GND East Store Rm Ent
Access Zone "IN"	ACZ	Bldg# - "DeviceType" "BldgLvl" Description IN	387 - ACZ MEZ East Store Rm Ent IN
Access Zone "OUT"	ACZ	Bldg# - "DeviceType" "BldgLvl" Description OUT	387 - ACZ B02 East Store Rm Ent OUT
Input - Reed switch Only Door	RSO	Bldg# - "DeviceType" "BldgLvl" Description	387 - R/S GND Reception To C/Park
Input - Duress	DURESS	Bldg# - "DeviceType" "BldgLvl" Description	387 - DURESS L06 Reception
Input - Break Glass	B/G	Bldg# - "DeviceType" "BldgLvl" Description	387 - B/G GND Main Entry Auto Dr
Input - PIR	PIR	Bldg# - "DeviceType" "BldgLvl" Description	177 - PIR L03 Stacks Main Corridor
Input - Power Supply Monitoring	PSU	Bldg# - "DeviceType" "BldgLvl" Description	310 - PSU GND Comms Rm
Input - Battery Monitoring	BAT	Bldg# - "DeviceType" "BldgLvl" Description	310 - BAT GND Comms Rm
Input – Glass Break	G/B	Bldg# - "DeviceType" "BldgLvl" Description	487 - G/B GND Office Window
Input – General Fire Alarm	GFA	Bldg# - "DeviceType" "BldgLvl" Description	187 - GFA GND Gate Keepers Cottage
Input - Miscellaneous		Bldg# - "DeviceType" "BldgLvl" Description	387 - FIRE ALARM GND Computer Lab
Relay - Electric Mortice Lock	LKE	Bldg# - "DeviceType" "BldgLvl" Description	177 - LKE L03 West Door
Relay - Strike Lock	LKS	Bldg# - "DeviceType" "BldgLvl" Description	185 - LKS GND Office Door
Relay - Magnetic Lock	LKM	Bldg# - "DeviceType" "BldgLvl" Description	185 - LKM L07 Office Door
Relay - Roller Door	LKR	Bldg# - "DeviceType" "BldgLvl" Description	185 - LKR GND Office Door
Relay - Bollard Lock	LKB	Bldg# - "DeviceType" "BldgLvl" Description	185 - LKB L12 Office Door
Relay - Auto Door	LKA	Bldg# - "DeviceType" "BldgLvl" Description	185 - LKA GND Office Door
Relay - Buzzer/ Sonalert	BUZ	Bldg# - "DeviceType" "BldgLvl" Description	192 - BUZ GND Comms Rm 168
Relay - Strobe	STR	Bldg# - "DeviceType" "BldgLvl" Description	177 - STR L13 Fire Strobe
Alarm Zone	A/Z	Bldg# - A/Z Description	903 - A/Z Burnley Engineering

Site Plans		Bldg# - Address - Lvl	387 - 13-21 Bedford St - GND
Schedules		Bldg# - "Time Range" "Day Range" "BldgLvl" Description	203 - 0700-1700 MO-SA GND Entry Door
Camera – External		Bldg# - Ext Location Description "PTZ"	387 - Ext Main Entry 387 - Ext N/W PTZ
Camera – Internal		Bldg# - "BldgLvl" Location Description "-Rm#" "PTZ"	387 - L01 Foyer 387 - L03 Meeting Room - Rm 3.58
NVR		Bldg# - "Bldg Name" "NVR Type" "#"	192 - Physics NVR1 192 - Physics WinNVR2

Common Abbreviations			
Building Level		Cardinal Points	
Abbrev	*Name*	*Abbrev*	*Name*
B02	Basement level 2	North	North
B01	Basement level 1	East	East
GND	Ground	South	South
GND MEZ	Ground Mezzanine	West	West
L01	Level 1	N/E	Northeast
L01 MEZ	Level 1 Mezzanine	S/E	Southeast
L02	Level 2	N/W	Northwest
L03	Level 3	S/W	Southwest
L04	Level 4		
L05	Level 5	Room Numbering Examples	
L06	Level 6	*Abbrev*	*Name*
L07	Level 7	Rm	Room
L08	Level 8	G.01	Ground room 1
L09	Level 9	1.06	Level 1 Room 6
L10	Level 10	E2.04	East Wing Level 2 Room 4
L11	Level 11	B.76	Basement Room 76
L12	Level 12		
L13	Level 13		
ROOF	Roof		
EXT	External		

Any device that is required to be programmed into multiple databases shall conform to the naming conventions listed above and shall be the same in both systems. Any modifications to the name of a device in the primary alarm

monitoring suite shall also be reflected in any additional database the device is listed in.

13.16 CABLING

- No end device should be wired to a Controller located in another building;
- All cabling shall follow the manufacturer's recommended cabling standards.
- GBUS/HBUS cabling must be polarized and must be terminated using a 120-ohm resistor, jumper or termination wire at the last unit. The termination jumper on either the GBUS/HBUS circuit needs to be fitted if the Controller 6000 is the end device for this circuit or the communication port is not in use.
- All terminations into control equipment shall be provided with Ferrules (Boot Laces) sized appropriately for the cable.
- Cables shall not be joined or extended.
- The cabling from the Controller 6000 to the readers shall be a minimum 4-core (14/0.20mm2) cable with cable runs not exceeding 150m as per manufacturer's specifications;
- There is to be a maximum of 10 access-controlled doors installed on each Controller 6000 processor;
- UOM installation practice is to have only 1 card reader wired back per HBUS port, where there is an IN/OUT card reader configuration, 2 readers on the one HBUS line is accepted;
- Figure 8 cable (min 24/0.20mm2) shall be used on electric strike and mortice locks;
- Figure 8 cable (min 26/0.30mm2) shall be used on electromagnetic locks, where double-electromagnetic locks are used, 2x Figure 8 cables shall be used; All Break Glass Units, Egress Buttons, Duress Buttons, Reed Switches, Local Sounders, PIR's and Door Status Indicators shall use 4-core (min 14/0.20mm2) cable;
- All alarm monitored inputs shall be installed with 2x 10k ohm end-of-line resistors at the field device, to allow for monitoring of the following input state conditions: Open / Closed / Short Circuit (Tamper) / Open Circuit (Tamper);
- Any network cabling shall not exceed 90m from point-to-point;
- There is to be no more than 10% in voltage drop for any ELV power cable;
- Refer to section 8.3.7 of the Design Standards for wall penetration requirements.

The security contractor shall submit samples (with technical product data sheets) of all cable types for approval by the University's Project Manager.

13.17 NETWORK INFRASTRUCTURE

The security systems operate on the University Network. Accordingly, the Contractor shall:

- Be appropriately certified, if not certified the Security Contractor must engage a contractor from the University's preferred contractor list;
- Provide structured cabling including all required patch panels, data outlets, etc.;
- Certify all new network cabling and patching as per University's Standards for the Installation of Communications Infrastructure, which can be accessed from the Design Standards web page;
- Network switches will be supplied and configured by the University;
- Provide all required patch cords and fly leads as per the University's Standards for the Installation of Communications Infrastructure, which can be accessed from the Design Standards web page;
- Coordinate connection to and configuration of the active network equipment;
- Notify the Project Manager of additional network switches and related details 4 weeks before hardware is required;
- All security equipment shall reside on the Security VLAN as per IP addresses allocated by the University Security office.

13.18 SYSTEM TRAINING, AS-BUILT DOCUMENTATION AND OPERATION & MAINTENANCE MANUALS

The security contractor is required to provide the following to the University:

- System training to the operators. The security contractor shall liaise with the University Security Manager to identify the training needs including breakdown of the training into levels to meet the operational requirements and the preparation of training materials. Training is to be completed seven (7) days prior to handover;
- As-built documentation – the security contractor shall prepare the as-built documentation to document the as-installed status of the security systems. This shall include (but not limited to the following). Refer also to the University CAD Standards which are located on the Design Standards web site):
- As-built layout drawings;
- As-built cable schedules;
- As-built schematic wiring diagrams;
- As-built cable reticulation and conduit layout;
- Operations & Maintenance (O&M) manuals – the security contractor shall prepare the O&M manuals to document the following:
- Product data sheets;
- Operating procedures of the security systems;
- Maintenance procedures of the security systems;
- User guide;
- Call-out procedures;
- Troubleshooting guide;

- Warranties;
- Test results;
- Final commissioning checklist;

Draft copies of O&M manuals are to be provided at a minimum of four (4) weeks prior to practical completion, with final versions provided no later than four (4) weeks post project practical completion.

The design consultant must include all these requirements in the project specification.

13.19 TESTING & COMMISSIONING

Testing & commissioning shall be a two-stage process. The security contractor shall undertake internal testing to check the functionalities of every device and all equipment against the performance of the security systems specified in the specification. The test results shall be recorded in test results record sheets, which shall be submitted to the design consultant for review and approval.

The security contractor shall also submit a test plan to detail the steps or procedures to verify the performance of the security systems against the specification. The test plan shall be submitted to the design consultant for review and approval. The approved test plan shall become the reference document for final commissioning.

The test plan shall cover (but not be limited to):

- The verification of all system functions and facilities sufficient to demonstrate the correct installation and operation of the system as a whole;
- Both night and daytime tests as applicable to the system components;
- Operational tests designed to verify the operation of all aspects of the system, together with the interfaces between the various security sub-systems and any non-security systems e.g., Fire Panel.

The test plan shall be thorough in its testing and recording and shall effectively demonstrate all performance and operational aspects of the specified security systems. The form of the document shall be mainly a check sheet of system operations, functions and facilities with space to insert numerical values where applicable. A separate column or space shall be provided for comments to be inserted.

Upon the approval of the test results & the test plan and the security contractor is satisfied that the security systems are ready for final commissioning, the security contractor shall organise with relevant stakeholders (including representatives from the University's Security Office and design consultant) to witness the final commissioning of the systems.

The security contractor is to provide at least two persons to conduct the final commissioning and provide hand-held radios such that they may carry out tests and demonstrations in accordance with the test plan for relevant stakeholders to witness. In the case of OSD testing, supply all test targets and recording equipment as may be necessary for the tests. The security contractor shall note that final adjustment on cameras (e.g., focus, angle of view and field of view) may be required to achieve the operational requirements.

With the security contractor undertaking internal testing before final commissioning, it is expected that tests can proceed without delays due to wiring errors or poor adjustment.

As part of the testing & commissioning process, the security contractor shall note that a copy of the final camera view (after final adjustments) for each camera shall be printed.

The copy shall form part of the as-built documentations. The print out of the camera view shall be the reference for the maintainer to adjust the camera view after maintenance works.

The design consultant shall include all these requirements in the specification.

13.20 NOTICE OF COMPLETION

The security contractor is to ensure that the security systems are completed and commissioned prior to practical completion. This process shall not be considered complete until the nominated University Security representative, has signed off that they are satisfied with the installed systems and they are ready to operate.

The design consultant shall be responsible to witness the final commissioning of the security systems and prepare the final acceptance certification of the completed installation. Upon satisfactory completion of the project the design consultant shall forward the completed test results to the University Project Manager and the University's Security Office.

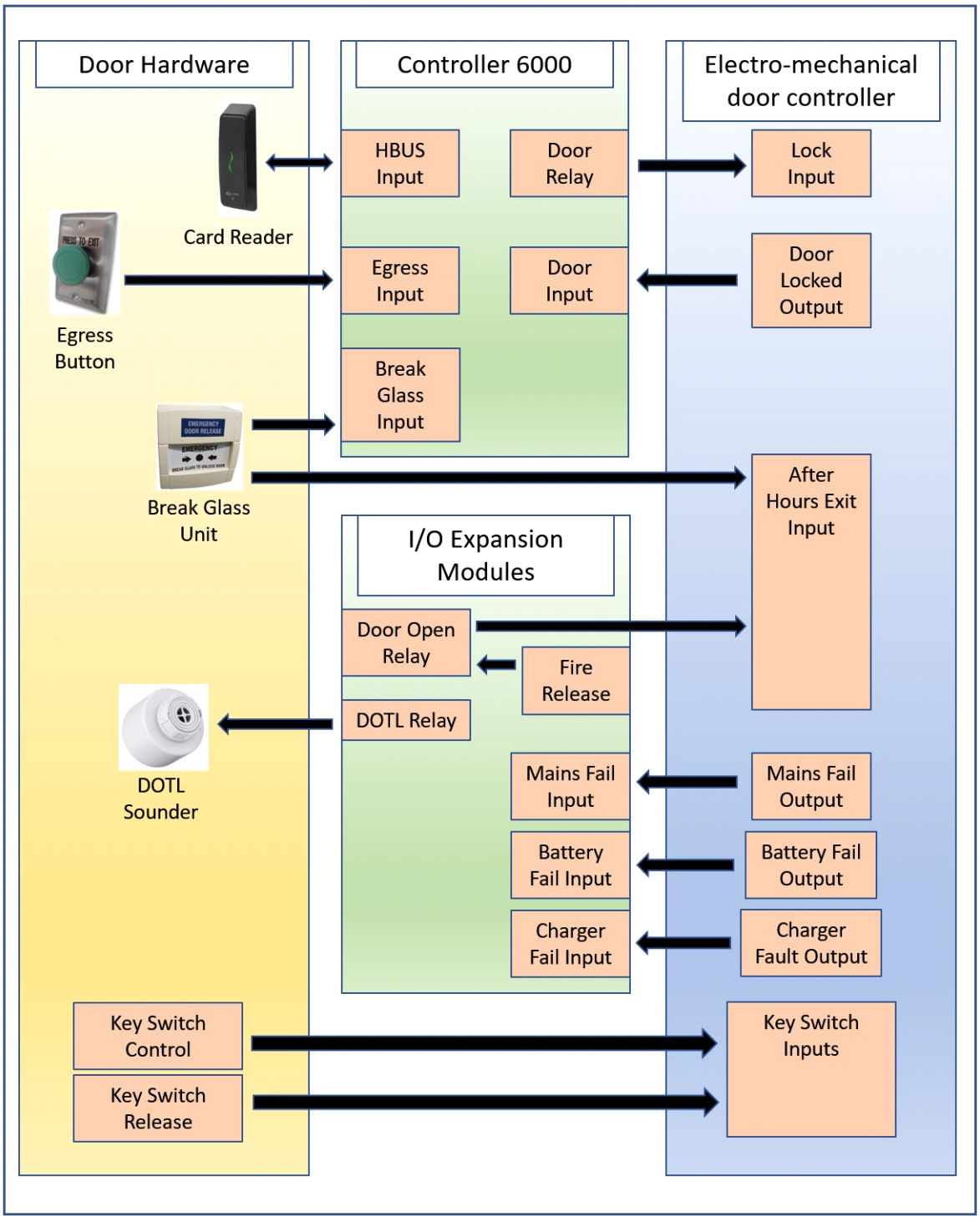
13.21 DESIGN CHANGE AUTHORISATION

All requests for changes to the requirements of the Design Standards must be made on the Modification Request Form. No design work is to proceed based on the proposed modification until the modification request has been approved in writing.

A schedule of all requested modifications together with a signed copy of all approved modifications are to be provided as part of the handover requirements at project completion.

13.22 APPENDICES

13.22.1 Appendix A – Automatic Door Wiring Diagram



13.22.2 Appendix B – Contractor Programming Requirements

Workshare Arrangement for Commissioning of Gallagher Access Control System for the University of Melbourne

The purpose of this document is to establish a workshare arrangement between security sub-contractors for the delivery of Gallagher Access Control and Intrusion Systems throughout The University of Melbourne. It is intended to provide clear

direction on the responsibilities of each contractor when delivering access control and intrusion detection installation works for the University of Melbourne.

Installation Contractor ("IC") – The contractor responsible for the cabling, fit-off of end devices, fit-off of panels, coordination of network and power and pre-commissioning of hardware.

Commissioning Contractor ("CC") - The contractor responsible for the programming and commissioning of software and configuration of the system.

Prerequisites

All contractors must be on the University of Melbourne's approved security contractor list. This list is available from the University's Security Office upon request.

The University's nominated Commissioning Contractor is MGA Electronic Security. Any installation of Gallagher Access Control and Intrusion Systems throughout The University of Melbourne must be programmed into the University of Melbourne's Gallagher Command Centre software by MGA Electronic Security.

Installation and commissioning of all equipment shall be in compliance with Section 13: Security of the University's Design Standards document. This is available via https://staff.unimelb.edu.au/contractors or by contacting the University Security Office.

Installation Contractor Responsibilities

- Procurement of all hardware
- Installation of all cabling and hardware
- Panel fit-off
- Coordination of power
- Coordination with head contractor and third parties (including UoM) of network installation including;
- Patch leads
- Network points
- Coordination with UoM IT for the availability of network switches and ports
- Pre-commission all end points, including completed and signed test plans.
- Note: For devices that require software (readers/controllers), it is expected that the Installation Contractor can confirm the device powers up.
- Terminate and test fire interface and relays.
- Final commissioning of all points alongside Commissioning Contractor. This will require an Installation Contractor technician in the field, working with the Commissioning Contractor technician.
- Provide all necessary documentation (drawings/point schedules/schematics) and other contractual requirements as issued by a Head Contractor or the University of Melbourne.
- Provide final install marked up plans, a schedule of points and any other pre-agreed documentation to the Commissioning Contractor, at a reasonable time prior to commissioning, to enable the Commissioning Contractor to program the system.

- Provide reasonable notice to the Commissioning Contractor for commissioning works. Reasonable cooperation is expected between both Installation and Commissioning Contractors to make these arrangements.
- Schedule commissioning for Buildings/Areas/Level in such a way to minimize repeated attendances for commissioning of small areas or single devices/doors.
- Warrant all hardware, cabling and installation works for a minimum 12 months.

Commissioning Contractor Responsibilities

- Procurement and implementation of all licenses and software.
- Coordination with UoM on access zone and alarm zone programming.
- Coordination of network port programming with UoM IT.
- Programming of all inputs, outputs, doors, access groups and end devices into the Gallagher database.
- Programming of site plans and icons.
- Programming and commissioning of visitor management system (where required).
- Integration with other security sub systems (i.e. Keysafes, OSD)
- Final commissioning of all points, alongside Installation Contractor. This will require a Commissioning Contractor technician working with the Installation Contractor technician in the field.
- Provide commissioning services at the request of the Installation Contractor, provided reasonable notice is given. Reasonable cooperation is expected between both Installation and Commissioning Contractors to make these arrangements.
- Warrant all software, firmware and configuration for a minimum 12 months.

Both the Installation Contractor and the Commissioning Contractor MUST sign- off on the notice of completion of works, before submission to the Head Contractor or University of Melbourne and acceptance that the works are complete.

Integrations and other non-standard functions

Any non-standard functions such as high level integrations to other systems will need to be coordinated separately between UoM the Installation Contractor and the Commissioning contractor.