



Security Systems Installation Specifications & Mechanical Lock and Door Hardware Specification

Version 5.7
September 2026

AUTHORITY

Version	Authorisation	Approval Date	Effective Date
4.1	Security Manager, Facilities Management		July 2005
4.9	Security Manager, Facilities Management		December 2006
4.10	Security Manager, Facilities Management		February 2009
4.11	Security Manager, Facilities Management		March 2011
4.12	Security Manager, Facilities Management		October 2011
4.13	Security Manager, Facilities Management		November 2012
5.0	Security Manager, Facilities Management	August 2015	August 2015
5.1	Security Manager, Facilities Management	December 2016	December 2016
5.2	Senior Security Manager, Estate Management	November 2017	November 2017
5.3	Head, Security & Traffic	July 2019	July 2019
5.4	Head, Security & Traffic	May 2021	June 2021
5.5	Director, Security & Traffic	April 2023	April 2023
5.6	Director, Protective Services	March 2025	March 2025
5.7	Director, Protective Services	September 2026	September 2026

DOCUMENT CONTROL

Review and History

The content of this document, Security Systems Installation Specifications, is managed and controlled by Security Services who will ensure that it is reviewed when any significant equipment or software changes necessitate it.

Version	Reviewed by	Approval Date	Sections modified
4.1	Security Systems	July 2005	Entire document
4.9	Security Systems	December 2006	Major Rewrite
4.10	Security Systems	February 2009	Various Changes
4.11	Security Systems	March 2011	Changes to design and installation standard

4.12	Security Systems	October 2011	Various Changes
4.13	Security Systems	November 2012	Various Changes
5.0	Security Systems	August 2015	Major Rewrite
5.1	Security Systems	June 2016	Various Changes
5.2	Security Systems	November 2017	HBUS/Bluetooth
5.3	Security Systems	July 2019	Mobile credentials, Gallagher 6000 HS Controller, Mechanical Lock and Door Hardware addition, CCTV models
5.4	Security Systems	June 2021	Touchless exit button 6.1 Existing infrastructure (if used to accommodate new equipment) to be upgraded Upgrade of Mortice Locks and CCTV
5.5	Security Systems	April 2023	6.1 Existing infrastructure (if used to accommodate new equipment) to be upgraded Update of Mortice Locks and CCTV 6.8.1 Mortice lock models 6.8.17 Help Points (housing, intercom and licences) 10.2 CCTV camera models 10.8 Existing CCTV cameras (new) 12.6 Rooms controlled by access control (New)
5.6	Security Systems	March 2025	6.1 Gallagher 7000 Controller Enhanced 6.8 Replacement doors to be fitted with new electronic lock and door hardware 6.8.4 Exit and Break glass for Auto doors 10.2 Cameras 12.7 Secured fixed leaf doors
5.7	Security Systems		6.1 Door controllers. Existing controllers to be upgraded to 7000 Enhanced 6.8.5 Reed Switch Contacts 6.8 Electronic door locks 6.8.4 Automatic Doors 6.8.14 Power Supply 6.8.17 Help Point 7 Cable requirements 7.2 Cable Support 10 CCTV Camera models, licences updated and Server/Archivers 12 Mechanical locks and rooms controlled by access control Appendix C – Equipment List

Contents

AUTHORITY.....	3
DOCUMENT CONTROL	3
1. INTRODUCTION	8
2. DEFINITIONS	8
3. GENERAL.....	8
3.1. Redundant Equipment and Cabling	9
3.2. Making Good	10
3.3. Fit for Purpose	10
3.4. Soldering	10
3.5. Device Terminations	10
3.6. Vermin and Insects	11
3.7. Audible Alarms.....	11
4. APPROVED SYSTEM INTEGRATORS	11
4.1. Certification	11
5. GALLAGHER COMMAND CENTRE	11
5.1. Overview.....	11
6. SPECIFICATIONS.....	12
6.1. Door Controllers	12
6.2. System Inputs and Outputs	13
6.3. BCA Compliance.....	14
6.4. Electronic Security Doors in Designated Fire Exit Paths	14
6.5. Card Readers.....	14
6.6. Anti-Pass Back.....	15
6.7. Door Interlocking.....	16
6.8. Electronic Door Locks	17
6.8.1. Electronic Mortice Locks – Preferred locks for all standard doors	17
6.8.2. Electromagnetic Locks – (for double internal doors) Approval by Security Systems representative. 18	
6.8.3. Electric Strikes - With Approval by UNSW Security Only	19
6.8.4. Automatic Doors	19
6.8.5. Door Reed Switch Contacts	20
6.8.6. Request to Exit Devices.....	20
6.8.7. Free Handle Egress	21
6.8.8. Cable Transfer Devices	21
6.8.9. Break Glass Door Release Unit	21
6.8.10. Lift Interface	21
6.8.11. Equipment Enclosures	22

6.8.12.	Keying and Locks.....	23
6.8.13.	Equipment Labelling	23
6.8.14.	Power Supply	23
6.8.15.	Battery Backup.....	24
6.8.16.	Interface to the Fire System	24
6.8.17.	Help Points.....	24
6.8.18.	Integration	25
6.9.	Intruder Alarms.....	25
7.	CABLE REQUIREMENTS	25
7.1.	Wiring and Cable	26
7.2.	Cable Support	27
7.3.	Cables in Ceiling Space.....	29
7.4.	Conduits.....	29
7.5.	Cable Duct.....	30
7.6.	Fixings	30
8.	INSPECTIONS, TESTING AND COMMISSIONING	31
8.1.	Works Inspections	31
8.2.	Programming	32
8.3.	Testing and Commissioning	32
8.3.1.	Commissioning Reports	33
8.3.2.	Performance and Acceptance Testing	34
8.4.	Completion	34
8.5.	Warranty/Defects Liability Period	35
9.	MONITORING	35
9.1.	IAS Configuration and Control	36
9.2.	Reed Switches.....	36
9.3.	Duress Buttons.....	36
9.4.	Gallagher T20 Terminal.....	37
9.5.	Status Indicator Panels	38
9.6.	Passive Infrared Sensors (PIRs)	38
10.	CLOSED CIRCUIT TELEVISION SYSTEM (CCTV)	38
10.1.	Standards and Compliance	39
10.2.	IP Indoor and Outdoor Approved CCTV Cameras (and Associated Housing)	40
10.3.	PTZ Cameras (and Associated Housing).....	40
10.4.	Multidirectional Camera	40
10.5.	Dual-Head Camera	40
10.6.	CCTV Storage	40
10.7.	LPR (Licence Plate Recognition) cameras	42

10.8.	CCTV Licencing	42
10.9.	Existing CCTV Cameras.....	42
11.	Defects Liability	42
12.	Mechanical Lock and Door Hardware	44
12.1.	Mechanical Locks.....	44
12.2.	Mechanical Lock Door Hardware.....	45
12.3.	Electronic Locks & Magnetic Locks	46
12.4.	Electronic Lock Door Hardware	46
12.5.	Door Closer Hardware	46
12.6.	Panic Bar and Exit Hardware	48
12.7.	Auxiliary Locks and Hardware.....	50
12.8.	Rooms controlled by access control	52
12.9.	Keys.....	52
	Appendix A: Example of a Gallagher Equipment Programming Commissioning Sheet	53
	Appendix B: Example of a Gallagher Equipment Programming Commissioning Sheet.....	56
	Appendix C: Equipment List	57

1. INTRODUCTION

The UNSW Security System Installation Specifications sets out UNSW's minimum requirement for design, construction and maintenance of the security systems. It ensures the installation of new and refurbished systems are fit for purpose and are cost efficient to maintain and operate.

This specification is to be read in conjunction with the EM Security & Traffic Design Standards.

2. DEFINITIONS

Term	Definition
EAC	Electronic Access Control
IAS	Intruder Alarm System
Security Contractor	Installation company installing equipment
SMS	Security Management System

3. GENERAL

The existing electronic security systems installed at the University of New South Wales include the following:

- Gallagher 'Command Centre' based Security Management System (SMS) for management and control of the IAS (Intruder Alert System) and EACS (Electronic Access Control System).
- Genetec SASD system comprising of IP CCTV cameras.
- Axis I8016-LVE Network video intercom Help Point System; and
- Salto integrated access control (please speak to UNSW representative prior to installing this product).

This standard covers the design and installation of field equipment pertaining to the above.

The Security Contractor shall ensure that all systems and equipment installed as part of these works are identical make and model and fully compatible with the existing and new systems installed onsite, to provide a seamless and fully integrated solution.

UNSW Security Systems must be consulted with for all security system works (prior to the commencement of any works).

The design, quality control, installation and testing of the installation shall comply with all relevant Government Standards, Australian and International Standards and local Statutory Authority Regulations as amended.

- The Building Code of Australia
- Disability (Access to Premises - Buildings) Standards 2010
- AS/NZS 2201 Intruder Alarm Systems
- AS/NZS 4806 Closed Circuit Television (CCTV)
- AS/NZS 1170.2 Wind Loads
- AS/NZS HB3 Drawing Standards
- AS/NZS 1049 Telecommunication Cable – Insulation and Sheath – Polyethylene
- AS/NZS 1099 Tests for Electronic Equipment

- AS/NZS 1100 Technical Drawings
- AS/NZS 1101 Graphical Symbols for General Engineering
- AS/NZS 1102 Graphical Symbols for Electrotechnology
- AS/NZS 1104 Informative Symbols for use on Electrical and Electronic Equipment
- AS/NZS 1345 Identification of the Contents of Pipes, Conduits and Ducts
- AS/NZS 1428 Design for access and mobility (All Parts)
- AS/NZS 1768 Lightning Protection
- AS/NZS 1882 Earth and Bonding Clamps
- AS/NZS 2052 Metallic Conduits and Fittings
- AS/NZS 2053 Non Metallic conduits and Fittings
- AS/NZS 2279 Disturbances in Mains Supply Networks
- AS/NZS 2546 Printed Circuit Boards
- AS/NZS 3000 S.A.A. Wiring Rules
- AS/NZ 3080 Telecommunications installations - Integrated telecommunications cabling systems for commercial premises
- AS/NZS 3901 Quality Assurance Standards
- AS/NZS 3905.2 Quality Systems Guidelines
- AS/NZS 4251.1 Electromagnetic Compatibility - Generic Emission Standards
- IEC 297 Dimensions of Mechanical Structures of the 482.6 mm (19") series
- ISO 9001 Quality Assurance Standards (for construction)
- ISO 9002 Quality Systems Guidelines (for construction)
- ISO 9003 Quality Systems (for construction)
- Local Electricity Supply Authority
- Australian OH&S Statutory Requirements (Work Safe – Australia)

The latest issue of the referenced standards and documents shall apply.

All equipment and installations shall comply with the referenced documents. Where conflict arises between the requirements of the standards and reference documents, the most stringent requirements shall be applied.

As a minimum requirement, all work shall comply with AUSTEL standards, AS3000 wiring rules, AS2201 Intruder Alarm Systems and AS4806 CCTV. In addition, UNSW Security Systems shall specifically approve all design work. All equipment and services must be compatible with and meet the requirements in this specification. All tenderers need to show an existing track record working with Gallagher equipment for at least five years and their employees are to be accredited by Gallagher (International) Limited to work on Gallagher equipment.

The successful tenderer will need to supply references showing that they have a proven ability to work on large, complex and integrated systems comparable to those installed at UNSW. Works in this contract are to be performed by direct employees of the successful tenderer. No sub-letting of any part of this contract is permitted (unless otherwise stated) without prior written approval of UNSW.

3.1. Redundant Equipment and Cabling

Remove and store all equipment, systems and sub-systems to be replaced or made redundant by this project. Where redundant equipment is removed, the adjacent surfaces shall be made good to match surrounding finish. This shall include, but not be limited to repair of door frames and doors. Also, refer to Clause 3.2, of this document Making Good.

All redundant cabling shall be labelled as per Clause 7.1 Wiring and Cable. All redundant cabling shall be isolated from field equipment and devices are stored in a manner in which

redundant cabling will not interfere with the operation of any security equipment but can be readily re-commissioned when required.

At the completion of the project, all redundant equipment shall be handed to UNSW Security Systems.

3.2. Making Good

When execution of the Works causes damage, or removal of equipment leaves an unsatisfactory finish, repair such damage or finish with materials compatible with the surrounding material and finished off flush with the adjacent surface.

This shall include, but not be limited to repair or replacement of door frames and doors, and re-establishment or making good of all panels, housings, and other areas necessary to be re-established which are, in the opinion of UNSW Security Systems, damaged in the course of the Works.

3.3. Fit for Purpose

Provide all equipment accessories, whether specifically documented or not, to ensure that the equipment is suitable for its intended purpose, to the approval of the UNSW Security Systems Representative.

Equipment accessories include but are not limited to:

- Connectors and outlets;
- Batteries;
- Enclosures;
- Protective cages and/or covers;
- Anti-tamper and/or anti-removal devices;
- Filters, both optical and environmental;
- Brackets and supporting braces;
- Escutcheons and face plates; and
- Adaptors.

3.4. Soldering

Solder shall be resin cored solder with 65% tin content. No separate flux is permitted. The solder shall provide a good electrical bond between the conductor and the tag.

3.5. Device Terminations

Where device cable tails require termination for the connection of cabling, solder all connections and install heat shrink to fully insulate each termination point.

Heat shrink shall be installed:

- At each cable core and termination point;
- Across the main cable sheath of multi-core cables to fully insulate the cable termination and provide a secure cable connection; and
- As directed by the UNSW Security Systems Representative and the Security Consultant following inspection of the cabling and cable termination onsite.

Application of the heat shrink shall not show any evidence of:

- ruptures, melting due to excess heat or breakages in the insulation provided by the heat shrink; and
- exposed cable cores, terminations or the outer cable sheath.

Loosely applied heat shrink which does not form a secure connection or insulator will not be accepted.

3.6. Vermin and Insects

All enclosures, cabinets, ducting and conduits shall be sealed or otherwise protected to prevent the entry of vermin or other insects which could damage the equipment or cabling.

The proposed method for protection against vermin and insects shall be submitted for approval by the Security Contractor.

3.7. Audible Alarms

To ensure compatibility with other equipment and/or systems, all equipment and/or system audible devices, including CPU audible alerts, installed as a part of this project shall be to the amplitude and pitch as approved by the UNSW Security Systems' Representative. Security Systems representative to confirm and approve any audible devices connected to the Security Systems.

4. APPROVED SYSTEM INTEGRATORS

Refer to UNSW's Security Systems for the current list of Site approved systems integrators.

For small security installations (under \$50,000 in value) the University prefers to use the on-site security maintenance contractor.

For larger projects the University only deals with companies accredited to install both Gallagher and Genetec systems and that have significant experience with the University's systems. Please speak to UNSW Security Systems for a list of authorised security system installation companies. Only contractors who are approved by the UNSW Security Systems representative will be able to integrate and install onto the existing systems.

4.1. Certification

A copy of the Gallagher and Genetec training certificate, and relevant documentation of the technician who performed the commissioning of the new system, must be provided for each installation.

5. GALLAGHER COMMAND CENTRE

5.1. Overview

The existing system is a Gallagher 'Command Centre' SMS utilizing 'FT Series' controllers and data gather panels connected to SMS servers located at UNSW.

The Gallagher system provides control and monitoring of the main entrances to each building, general areas, internal areas and the like. Validated access through electronically controlled doors is provided by the use of proximity cards and card readers.

The operation of the existing Gallagher system throughout UNSW campuses shall not be impeded, affected or otherwise by new installations.

System is to provide Access Control for 24 hours entry to building via specific entry points. Free egress for all system doors is always to be maintained (unless specified otherwise). Building Systems will be closed and at predetermined times via accessed Time Zone allocation to the appropriate zone. After hours entry is gained via a valid user operating the designated access door.

All individual building equipment shall operate via card reader assigned to that building or area (e.g. door free access/door secure and any Ancillary Reads, Doors assigned to that zone).

All Electronic Security Controlled Doors on a designated evacuation egress route must go to free access in the event of a fire alarm unless otherwise stated for individual doors.

Each building is to have a contact connected (input) from the building fire panel to the Gallagher controller, for an alarm activation on Gallagher (in the event of a fire alarm).

External Doors shall indicate a door open alarm on the operator terminal. Alarm to be timer controlled from 0-180 sec for a valid egress. An unauthorized access shall generate an immediate alarm condition locally (sounder) and at the Command Centre.

All licenses pertaining to security systems are to be supplied by the contractor.

6. SPECIFICATIONS

6.1. Door Controllers

Gallagher Controller 7000 Enhanced field controllers, with 8H modules attached, shall be installed to carry out the functions specified in this document. Each Controller 7000 Enhanced must not exceed eight (8) door objects.

Door Controllers shall be connected to the SMS to carry out the functions specified in this document.

Door Controllers and associated peripheral equipment (e.g. power supply, battery, fuses etc.) shall be mounted within secure enclosures and to the approval of the UNSW Security Systems' Representative.

All Gallagher expansion modules shall be HBUS.

Controllers can have the following devices connected:

- Gallagher HBUS I/O.
- Gallagher T Series Multi-Tech Readers & Terminals (T15 Multi-Tech Reader – for access-controlled doors; T20 Multi-Tech Terminal for alarm-controlled area or Card & PIN Access Doors. Readers are to be black in colour;

Controllers, including all enclosures, power supplies and expansion boards to be installed no higher than 1.8 metres from the ground.

All new T Series Multi-Tech Readers & Multi-Tech Terminals are to be connected as HBUS Configuration only. All readers & terminals must be Bluetooth compatible (capable) & configured

If existing hardware does not support or does not have availability for HBUS Connection a new Controller 7000 Enhanced with 8H Module must be installed along with FT & AUX PSU's as detailed within this specification

All new readers to be installed and functioning as Bluetooth readers (T15) with HBUS only.

Where any existing Gallagher controller is to be associated/impacted by an installation, including the addition or modification of doors, the existing controller shall be upgraded to a Gallagher Controller 7000 Enhanced, including the required 8H module(s), as part of the project works.

When installing additional equipment on existing UNSW Gallagher controllers (for refurbishments etc.):

- Existing controllers to have a maximum of 8 Door objects per controller.
- The power supplies that are connected to the existing controller (that is being utilized as part of a project) are to be upgraded to ensure they have 2x 7-amp power supplies (one for the Controller, the other for auxiliary). Existing power supplies that are not 7 amp are to be removed by the contractor and replaced to meet these requirements. These power supplies are to be installed in appropriate power supply enclosures. The contractor is to also ensure there are 4 separate inputs on each controller monitoring both power supplies' Battery Low and Mains Fail.

Power supplies are to be dedicated to each controller (not shared between multiple controllers) – this is to be rectified and separated at time of installation

Each Controller is to have a fire trip relay installed and connected to the fire panel. Each Fire Trip relay to be connected to a separate input on the Gallagher controller

Door controllers shall be installed within approved communications rooms or electrical risers and shall not be installed in corridors, public areas or other unsecured locations. Any proposed controller location outside an approved communications room or electrical riser shall require prior written approval from the UNSW Security Systems Representative.

Controllers (and associated expansion modules) shall be accessible for maintenance but protected from unauthorised access, tampering and accidental damage. Power outlets and network ports serving the controllers shall be concealed within the controller cabinet or associated power supply enclosure. External power outlets, network ports and exposed cabling will not be accepted.

6.2. System Inputs and Outputs

The EACS shall monitor the status of all system inputs and control all output functions as stated in this document and as shown on the Security Services drawings.

System alarm inputs, which the EACS shall be capable of monitoring shall include, but may not be limited to the following:

- Door reed switch contacts;
- Door lock monitors;
- Door release Request to Exit (REX) buttons;
- Break glass door release units;
- Duress buttons;
- Help point alarms

- Remote door controls and over-ride functions;
- Spare inputs (remaining inputs from base configuration); and
- Alarm inputs from interfaced systems.

As a minimum requirement, all inputs shall be 'end of line' resistor monitored, via End of Line Resistor Modules (EOLMs), and provide indication of normal, alarm, cable short and cable open conditions.

All door-related inputs, including reed switch, exit and lock sense inputs, together with Controller Mains Fail and Battery Low inputs, shall be connected directly to the controller where sufficient input capacity is available.

Where eight (8) maglock/mortice/strike lock doors are connected to a single controller and insufficient controller input capacity is available for the Mains Fail and Battery Low inputs, an HBUS expansion module shall be provided to accommodate these inputs.

PIRs, sirens, equipment alarms and breakglass alarms shall be connected to available controller inputs/outputs where sufficient capacity exists. Where sufficient capacity is not available on the controller, an appropriate HBUS expansion module shall be provided.

6.3. BCA Compliance

The door controllers and doors directly powered by the Access Control System, including all electrically released/locked doors, shall meet the requirements of the Building Code of Australia (BCA), council, fire and other regulations as required. This shall include all cabling to the doors and associated devices.

All door control devices, such as card readers, exit buttons, key switch overrides and the like shall be installed between 900mm and 1200mm above fixed floor level and shall be installed no less than 500mm from an internal corner, in accordance with AS 1428 (Design for access and mobility).

Ensure doors meet BCA requirements and provide written confirmation to UNSW Security Systems, to the acceptance of the test by the appropriate authority, as a condition to the granting of Practical Completion.

6.4. Electronic Security Doors in Designated Fire Exit Paths

Any security doors that are also identified as Fire Exit Emergency doors are required to comply with Building Code of Australia Standards, relevant Australian Standards and Occupational Health & Safety requirements for emergency exit and fire safety.

6.5. Card Readers

Where nominated on the drawings, the Security Contractor shall supply and install access control Card Readers / terminals

All readers are to be Gallagher T Series Multi-Tech Readers & Terminals (T15 Multi-Tech Reader – for access-controlled doors; T20 Multi-Tech Terminal for alarm controlled area or Card & PIN Access Doors.

Readers are to be black in colour.

Card readers shall be nominally mounted between 900mm - 1100mm above finished floor level (unless otherwise specified). Refer to the Architectural drawings for further information. Access to card readers to be installed on a levelled surface.

Card readers shall not be mounted back-to-back on either side of the wall, however shall be mounted offset at a distance to maintain integrity of card reader operation.

Where nominated, Gallagher protector reader covers shall be installed.

Card readers shall be secure and shall not compromise security if tampered with. Card readers mounted externally must be fitted with Gallagher protective reader covers.

Card details shall be correctly read and processed without undue attention to the speed or orientation at which the card is presented to the reader.

The design of the reader shall permit one handed card operation.

There shall be both audible and visual indication on the card reader to indicate a successful card read. The reader shall be complete with an LED which changes state when the associated barrier is in the access or secure mode as described. Unless specified otherwise, card readers shall be programmed to operate as follows:

- Door Secure: Red LED illuminated;
- Valid Card Read: Momentary audible signal (i.e. single reader beep) and green LED is illuminated for duration that door control relay output is active (i.e. lock is in the unsecured position);
- Invalid or Unauthorised Card Read: Extended audible signal (i.e. reader beeps) and Red LED flashes twice and returns to illuminated red LED indication;
- Card readers shall be configured to provide an audible warning signal approximately five seconds before a Door Open Too Long (DOTL) alarm is generated (time to be programmable);
- When the system is fully loaded, the time elapsed from presentation of a card at the reader to granting access if all data is valid, shall not exceed one second;
- The EACS shall monitor each individual card reader and provide an alarm if the card reader has gone off-line, providing information on which card reader has stopped operating and its location;
- The EACS shall monitor each individual card reader cover plate and provide an alarm if the card readers cover plate has been removed; and
- The mounting of card readers shall maintain the vandal resistant integrity of the reader.

It shall not be possible to open the door controlled by the card reader by tampering with the reader or its wiring in any way. Card readers shall contain no wiring for activation of control devices monitoring of any door input devices such as reed switches and REX devices and the like.

Additionally, where T20 readers are nominated on the drawings at the entrance to an area containing IAS volumetric detection (i.e. PIRs), the card reader shall be configured to enable arming and disarming of the Intruder Alarm System of their respective area/zone.

6.6. Anti-Pass Back

The EACS shall include software application modules to allow the programming of any or all readers as anti-pass back readers via the SMS.

The anti-pass back function shall be programmable and accessible by authorised persons only.

The anti-pass back function shall be global across all readers such that areas can be defined from the outer most ring of security (e.g. perimeter) to internal rooms within buildings. The number of areas within any other area shall be limited to four however the number of area groups within the total EACS shall be at least 1000.

Anti-pass back shall include such features as:

- Disable/Enable switching of global functions;
- Enable but allow access on violation, and generate an alarm (soft anti-pass back);
- Enable and restrict access upon detection of violation, and generate an alarm (hard anti-pass back);
- Count occupants within any anti-pass back area;
- Link anti-pass back areas together to restrict access upon previous area access status across all readers; and
- List all occupants within any defined anti-pass back area based on other conditions associated with times, cardholders, departments and the like.

6.7. Door Interlocking

The EACS shall have a door interlocking functionality inbuilt within the system and shall provide the following functionality:

- Monitor the door open/closed and interlocked status (e.g. reed switches installed at the door/gate and/or roller door);
- Interlocked doors shall be displayed in a separated each-to-distinguish console on the SMS graphics;
- Provide controlled access of nominated doors via the electric locking device installed;
- Provide the ability to override the nominated interlock group via the Gallagher SMS graphics;
- A valid interlock group override shall suppress the door monitoring to allow entry or egress without initiating an intrusion alarm;
- Once monitoring suppression has been initiated, the door monitoring shall be reinstated immediately following the closure of the barrier/door/gate or minimum via operator as programmed;
- In the event that a door is breached without a valid command from the SMS or due to a system fault, a “forced door alarm” shall be activated at the SMS Operator terminals;
- Should the barrier/door be held open in excess of a pre-determined period a “door open too long” alarm shall be initiated at the SMS; and

- Prevent doors from being activated or opening whilst any one door within the nominated interlock group is open.

6.8. Electronic Door Locks

As part of installation, the contractor must:

- Provide electric door locks, as shown on the drawings, connected to the EACS as specified.
- Provide all door and doorframe cut-outs, door coring and conduits required for the installation of all electric door lock cabling and fitting. All cables to electric door locks shall be concealed and located on the secure side of the access control door.
- Provide readily available captive connectors at the electric door lock for connection of the associated lock cables to facilitate easy removal and replacement of electric door locks.
- independent door reed switch shall be provided and connected to the 'Door Sense' input on the EACS. Integrated lock reed switches shall not be used for door position monitoring due to their increased susceptibility to failure.; and
- Terminate cabling, test and commission electric door locks to the approval of the UNSW Security Systems' Representative and the Consultant.
- Where a door is replaced as part of a refurbishment, all associated mechanical and electronic door hardware, including electronic locks and door furniture/handle sets, shall also be replaced and shall comply with the requirements of this specification. The lock barrel for all access-controlled doors shall be replaced by the UNSW Locksmith, coordinated through the UNSW Security Systems Representative

6.8.1. Electronic Mortice Locks – Preferred locks for all standard doors

Electric mortice locks are to comply with the following minimum:

- Lockwood 3570ELM0SC (to be installed on wooden doors).
- Lockwood 3782ELSS (to be installed on Aluminum doors).
- Generally, power to lock (fail safe) unless otherwise specified.
- 12 Volt DC continuously rated.
- 'Free' door handle exit hub micro-switch.
- Integrated reed switch which shall be provided in addition to the door reed switch contact.
- Dead latch and door closed status monitoring.
- Provide audible indication of the lock operation.
- Provide visual indication of the lock status via LED's integrated with the door furniture/handles (internal doors only).
- Complete with internal door release switch and be free handle exit.
- Operation of free handle suppresses the associated access control door alarm.

- Locks to be fail safe for designated fire exits.
- All other internal and external doors fail-safe or fail secure upon application and verification by the Security Systems Manager.
- Transfer hinges must be Lockwood Assa Abloy LC8810 or Equivalent (where this transfer hinge is not suitable due to frame/door/hinge make, external door loops may be used with approval by the UNSW Security Systems); and
- Installed by APPROVED specialist trades.

Mortice locks (as per the specified model/brand) are the preferred for all standard internal doors.

The dead latch status monitor shall be wired in series with the integrated door position switch and shall be configured as a 'Lock Position Status' input on the Gallagher SMS.

The 'Free' door handle exit hub micro-switch shall be configured as a "Request to Exit" input on the Gallagher SMS.

6.8.2. Electromagnetic Locks – (for double internal doors) Approval by Security Systems representative.

All electromagnetic locks must be fully monitored. The appropriate electromagnetic lock must be installed depending on door size and height – ensuring the secure holding force is maintained.

Electromagnetic locks are to comply with the following minimum:

- Padde EMZ8SM for external/internal single doors.
- Padde EMZ8DM for external/internal double doors or approved equivalent.
- Padde EMZ4SM for internal single doors.
- Padde EMZ4DM for internal double doors or approved equivalent.
- 12V DC continuously rated.
- Provide Lock Status Sensor (bond sense) to detect that the both the magnetic armature plate is secured to the lock.
- LED indication (Red – Locked and Green – Unlocked).
- Integrated door position switch (reed switch) to detect when the door is in the closed position.
- To include appropriate mounting equipment for inward and outward swing doors.
- Installed by APPROVED specialist trades.

Magnetic Locks are required to be fitted to internal double doors only (external door locks to be installed upon UNSW approval).

The integrated reed switch, the lock status sensor and early warning alarm shall be wired in series with integrated door position switch and shall be configured as a 'Lock Position Status' input on the EACS.

*Maglocks are not to be used for restricted or sensitive areas such as labs

6.8.3. Electric Strikes - With Approval by UNSW Security Only

Electric strikes to be installed on CATS room doors (that do not have a card reader assigned), fire doors and mechanical plant room doors only. All other installation of electric strikes must be approved by UNSW Security Systems:

- Padde ES9000 Pre-Load Electric Strike with monitored latch keeper; and
- Installed by APPROVED specialist trades.

For doors that are exposed to the weather (e.g. roof, external louvered doors), Electric Strikes are to be installed. These locks require a cover/shield to protect the lock from these conditions.

6.8.4. Automatic Doors

Automated (Auto) Door locking is to be provided by Auto Door Company. Where access control is to be fitted to the door an options board is to be supplied. If the auto door is on a fire egress path, fire panel connections are to be arranged and installed by the auto door installation company.

The University recognizes that other types of locks may be required in certain circumstances. On these occasions UNSW Security Systems staff must be consulted for approval before locks, other than those described above are fitted to doors.

Auto Door Interface/Auto Door Operator (Disabled Access Auto Closer)

Interface to Auto Doors shall be achieved through direct connection of Gallagher Inputs & Outputs to Auto Door Options Board Only – NO stand-alone interposing relays (timer relays) will be accepted without UNSW Security Systems approval

All auto door Day / Night timing & control shall be achieved through Gallagher SMS logic control

As a minimum the below connections are required

- 1 x Door Trigger Output
- 1 x Day / Night Output
- 1 x DOTL Input
- 1 x DNL Input
- 1x Request to Exit
- 1x Break-Glass

All Request to Exit & Break-Glass devices connected to Auto Doors / Auto Operators shall be connected through the SMS I/O – direct connection of Exit Pushbuttons is to be avoided and shall require approval by UNSW Security Systems

Auto Door / Auto Operator safety beams shall not be connected to or function provided by SMS System.

Disabled bathroom auto doors are to have a manual key override installed (for emergencies) which will be keyed by the UNSW Locksmith.

Where an automatic door is fitted with a key switch, the key switch must be compatible with and capable of being re-keyed to the UNSW keying system.

The UNSW Locksmiths will supply the required key barrel, and the Electrical Contractor is responsible for installing the supplied barrel into the key switch.

6.8.5. Door Reed Switch Contacts

Supply and install Sentrol 1078C door reed switch contacts, fully recessed into the door and door frame, at the locations shown on the drawings. For double doors, a separate reed switch shall be provided to each door leaf, with both reed switches wired in series to the associated Door Sense input. The reed switch contact and magnet shall be installed and:

- fully recess mounted into the door and door frame; and
- Securely fixed to the door and door frame with suitable adhesive.

Independent door reed switch contacts shall be provided irrespective of the provision of reed switches integrated to the electric door lock and shall be connected to the 'Door Sense' input on the EACS (excluding 3570 mortice).

Terminate cabling at both ends and install ELM's at the reed switch. Solder and heat shrink all cable terminations as specified.

6.8.6. Request to Exit Devices

Touchless exit button

Request to Exit (REX) Touchless exit buttons to provide users with a valid exit request of electronically access controlled doors.

REX Touchless Exit buttons shall be SPRINT SPRL3761 series or approved equivalent. REX touchless buttons shall be clearly engraved "TOUCHLESS EXIT" (or "PRESS TO EXIT" for REX buttons) in large block letters 5mm in height and mounted on a curved stainless steel finish switch plate. The engraved text shall be coloured black and located centrally above the push button.

All REX buttons shall be mounted at a uniform height and at a uniform height with card readers, unless otherwise approved by the UNSW Security Systems Representative.

REX buttons located exposed to the environment shall be IP66 rated.

REX button installation shall prevent activation from the non-secure side. Provide all shrouds, brackets, fixings, fabrication and the like required to achieve this requirement.

The REX device shall be connected as an input (normally closed) to the Door Controller to provide a request for exit signal and log to the SMS.

Operation of a REX device shall temporarily unlock the door to allow a single exit for a predetermined exit time or until the door is sealed, and log as a 'valid exit' at the SMS audit trail.

Where required exit push buttons will be considered pending approval by UNSW Security

6.8.7. Free Handle Egress

For electric mortice locks, which have a 'free' handle egress operation a micro switch in the lock shall act as the REX device and log to the SMS.

6.8.8. Cable Transfer Devices

Provide cable transfer devices to comply with the following minimums:

- Lockwood Assa Abloy LC8810 lead cover, including door recess box or approved equivalent (cable transfer hinges, curly cord or exposed cable transfer units are not suitable). It should be noted, if the opening angle of the door is more than 120° or the distance between hinge and doorframe is greater than 20mm, provide Lockwood LC8811 lead cover;
- Conceal all cabling; and
- Install to electric strike lock doors, where the doors consist of two leaves, so that cabling can transfer from the frame of the door to the door leaf.

6.8.9. Break Glass Door Release Unit

Provide Break glass door release units for nominated doors as shown on the drawings. Break Glass units are to be the Sprint D115G series or approved equivalent.

The Break glass unit shall be of a dual monitoring type and shall be of the plastic, collapsible and key resettable insert type.

The Break glass unit shall include two poles, both normally closed. The first contact shall connect the positive of the electric lock power to the electric lock. The second contact shall be connected to an IAS input via a local End of Line Module (ELM) to provide an alarm at the SMS when activated.

Where the unit is being provided to control an automated or motorized door (i.e., sliding door, roller shutter etc.), the second contract shall connect to the automated/motorized door controlled 'fire release' signal. The interfacing, connection and the like (inclusive of all wiring) to the automatic sliding door controller shall be undertaken by the automated/motorized door contractor.

The Break glass unit shall be inset engraved with "EMERGENCY DOOR RELEASE" and shall be green in colour.

The Break glass unit shall be mounted at a height of 900mm - 1100mm (centered) above FFL, adjacent to and aligned with the doors associated exit device (i.e., card reader or RTX button). Where the break glass unit cannot be mounted adjacent to other security devices, the break glass unit shall be mounted below other security devices typically at 900mm (centred) above FFL.

6.8.10. Lift Interface

The EACS shall interface with the lift control system for monitoring and control of the Lift Independent Service Mode (ISM). When a signal is received from the EACS, the lift car shall operate into the independent service mode.

Upon use of a valid card at the local lift card reader, the lift shall be place in Independent Service Mode (ISM) and shall report this status back to the EACS/SMS. The lift shall remain in

the independent service mode until a valid card is used at the local lift card reader or until a pre-set time has expired (to be programmable via the SMS). The independent service mode shall also be controllable via the SMS operator terminals.

The lift interface shall allow for the future control of all lift floors (each floor to be controlled separately by a separate output) via the EACS.

Where lift interface is required, liaise and coordinate with the Lift Contractor for all cabling requirements, card reader installation and interfacing requirements.

6.8.11. Equipment Enclosures

Security control equipment shall be installed within a dedicated security services equipment enclosure (inclusive of cabinets and racks) supplied and installed as part of these Works. Equipment enclosures shall be wall mounted and installed in the approved locations or as indicated on the Security Services drawings.

Should additional control equipment enclosures be required to be installed (these must be Gallagher standard or dual cabinets), these shall be supplied as part of this Contract in locations approved by the UNSW Security Systems' Representative.

All enclosures shall be complete with lockable door(s) (on Gallagher master key system/Dirak system) and dust seals and no higher than 1.8 metres from floor.

All internally mounted enclosures shall meet with high protection category IP55 and Impact Category IK09 standards.

Should enclosures be required externally, these shall meet with a high protection category IP66 standard, and installation location shall be approved by the UNSW Security Systems' Representative.

Enclosures shall be supplied with perforated rear mounting plates and top entry cable gland plates to facilitate top entry of cables from over-head cable trays, cable ducts or conduits.

Penetrations provided for cable access shall be suitably sealed to prevent moisture ingress and protection of cables. Screws shall be complete with captive fibre washers.

Enclosures shall be securely fixed in position using fixings suitable to maintain the weight of the 150% of the panel in its completed state.

Equipment installed as a part of this Contract shall not be installed in equipment enclosures containing other services equipment without the written approval of the UNSW Security Systems' Representative.

The equipment enclosures shall be installed at a height of approximately 1.8m above finished floor level (FFL) from the bottom of the enclosure, wherever possible.

Should this height not be available, an alternative location shall be agreed with the UNSW Security Systems' Representative.

Panels shall be supplied with rear mounting plates and top and bottom entry cable gland plates to facilitate top and bottom entry of cables from over-head cable trays, cable ducts or conduits, as well as from underground/in slab conduits.

Final installed location must provide a clear and safe access for service and maintenance of installed equipment.

Refer to Section 6.1, **Door Controllers**, for approved controller locations and associated expansion modules. Door controller for approved locations of controllers associated expansions.

6.8.12. Keying and Locks

All Gallagher-controlled doors fitted with a key barrel shall be keyed to the UNSW Gallagher Mechanical Master Key System, managed by the UNSW Locksmith. The lock barrel shall be supplied and installed by the UNSW Locksmith in coordination with the UNSW Security Systems Representative

6.8.13. Equipment Labelling

All equipment enclosures, including panels, cubicles and racks, shall have self-adhesive labels, which shall match adjacent labelling schemes in respect to letter heights and colours.

All core equipment located within enclosures shall also have labels.

All device cabling to have field descriptive labelling.

Equipment labels and adhesives shall be of a suitable construction and material suitable for use in an outdoor area.

Equipment labels shall be Panduit Raised Panel Component Labels with over laminates and Brady EPREP Polyester Equipment Labels. Equipment labels shall, as a minimum, detail the controller number and IP address (provided by UNSW Security Systems) to be on the lid of controller

Duplication of equipment/device identities will not be accepted.

6.8.14. Power Supply

AC power shall be suitably fused and designed to operate from a single phase. All 240 Volt AC power supply connections shall be in accordance with the minimum standard requirements of AS 3000 and installed in accordance with good engineering practices.

The power supplies shall be a power box or Gallagher brand with minimum 7 Amp and shall have a stand by battery minimum 7 Ah for controller supply or 12 Ah for lock supply

Security Services General Purpose Outlets (GPO's) shall be installed on a separate final sub-circuit.

Security low voltage DC power supplies shall be provided in accordance with AS: 2201.1 and AS: 3000 respectively

Where a Gallagher dual cabinet is installed, it must be equipped with a Gallagher 8 Amp power supply and 1x 7 Amp battery.

Electric locks shall be powered by an independent power supply and shall not be powered by the same power supply as the SMS/EACS/IAS controllers.

Alarm monitoring of the mains supply shall be provided from the secondary side of the step down transformer and shall be monitored for fail alarm.

The mains fail and battery low alarms shall be connected to and monitored at the SMS.

Alarms shall be monitored 24 hours a day and report as a priority alarm.

Minimum of two power supplies per Gallagher controller, unless otherwise specified. Power supplies to locks should be separated from power supplies for control equipment. If Auxiliary supply requirement exceeds 7 Amps, additional supplies will be required. Power supplies are to be clearly labeled with their corresponding controller number and role (controller supply or lock supply)

Each power supply and respective back up battery is required to be installed in its own enclosure. Each power supply shall have individual monitoring for the Battery Low and Mains Fail.

All power supplies, unless noted otherwise, shall be installed within nominated equipment panels, racks or enclosures.

6.8.15. Battery Backup

Maximum load of power supplies must not exceed 80% load capacity.

Backup batteries (12 V 7.2AH/12AH Gel batteries).

Battery chargers shall be capable of restoring batteries from a fully discharged state, to a fully charged state, within a period of 16 hours after restoration of supply and, at the same time, maintain the installation in a fully operational state.

Alarm monitoring of the batteries' charged status shall be via a Low Battery Alarm reporting to the SMS. It shall operate even if the mains power has not failed. It is permissible for the Low Battery alarms to represent a single alarm to the SMS.

Batteries shall be suitable for continuous stand-by duty and batteries shall be Sealed Lead Acid type.

Batteries shall be labelled with the installation date.

6.8.16. Interface to the Fire System

A fail-safe low-level interface shall be provided between the Fire System and each electronically access control door within an egress path, unless "free handle egress" is provided by an Electric Lock.

Door lock overrides shall automatically restore once the fire alarm(s) have been reset at the Fire Indicator Panel.

6.8.17. Help Points

Axis I8016-LVE Network Video Intercom (housing supplied through Cunneen Signs), with an installed Help Point to be visible through the University's CCTV network. The Help Point to have a standard UNSW 'Help Point' sign affixed above the Help point (signage also supplied by Cunneen signs). The Help point must include power, network and VOIP. When installing the help point, the intercom must have cable wiring from Negative to NO/NC and I/O 1 to COM. When the Help Point button is pressed, an alarm (input) to be activated on Genetec and UNSW Security Emergency number is called. An additional CCTV camera in the vicinity to the Help Point is to be installed to ensure adequate coverage of the Help Point.

Each Axis Help Point shall be integrated through Genetec Security Center system using Sipelia and Genesys Cloud for audio via a SIP trunk.

The Contractor shall provide, configure and commission the following licences for each Help Point:

- one Genetec Sipelia intercom connection licence; and
- one Sipelia channel licence,

including SMA for each licence. All licences, configuration and integration requirements shall be included in the Contractor's scope and pricing.

6.8.18. Integration

The CommCard solution is to be used for integration between Gallagher FT and Salto off-line readers. Where this solution is used a workstation and encoder is to be provided by the contractor to enable ID/Access cards to be encoded to allow access to the accommodation. UNSW Security Systems management are to be consulted for approval prior to any non-Gallagher installation.

UNSW Security Systems management to be consulted prior to any integration for acceptance and approval to the UNSW Security Systems.

6.9. Intruder Alarms

UNSW Security Systems will need to be consulted for approval prior to the installation of intruder alarms connected to the Gallagher system.

In the event of an intruder alarm being approved, this shall be achieved by using the Gallagher T20 Multi-Tech Technology Only.

T20 Pin Code Terminals & GBUS Remote Arming Terminals (RATs) will not be accepted. All terminals are to be card only and Bluetooth capable.

7. CABLE REQUIREMENTS

All wiring shall comply with the latest edition of AS/NZS 3000, applicable Australian Standards, manufacturer requirements and this specification.

All cabling shall:

- be new, pink in colour, fit for purpose and delivered to site on unbroken reels with the manufacturer's label attached;
- be installed neatly, securely and within the secure boundary of the room, building or site;
- be concealed within walls, ceilings or other building structures wherever practicable;
- where concealment is not practicable, be installed within cable containment approved by the UNSW Security Systems Representative before installation;
- be protected from mechanical damage, tampering and environmental conditions;
- be installed with due regard to future inspection, removal and replacement;
- maintain a minimum separation of 300 mm from electrical power cables and other systems cables, including data, video, audio and sensor cables; and

- be installed without kinks, crushing, stretching, sharp bends, excessive tension or damage to the cable sheath or insulation.

Exposed, loosely supported, unsecured or poorly installed cabling will not be accepted.

Any cabling or cable containment that is visible or exposed, including cabling or conduit installed on walls, ceilings, corridors, plant areas or other accessible locations, shall require prior approval from the UNSW Security Systems Representative before installation. Approval shall include the proposed route, containment type, fixing method and finish. Exposed cabling or containment installed without prior approval will not be accepted.

Cable containment shall be continuous, suitably sized, securely fixed, straight, level and free from sharp edges. Conduit shall be adequately supported, properly terminated and protected from damage, tampering and water ingress where applicable. Bushes, grommets or equivalent protection shall be provided at cable entry and exit points. Exposed cable containment shall be painted or finished to match adjacent structures, unless otherwise approved.

The following minimum containment requirements shall apply:

- rigid or flexible PVC or HDPE conduit within internal secure areas;
- rigid or flexible steel conduit in external areas, including external walls, walkways and other exposed locations;
- rigid or flexible HDPE conduit for underground installations; and
- steel cable duct, cable ladder or cable tray where required.

Standard concealed internal cable routes do not require individual approval, provided they comply with this specification.

Adequate slack shall be provided at equipment and termination points to allow inspection, adjustment, removal and replacement without placing strain on the cable or termination. Suitable strain relief shall be provided. Intermediate cable joints or connections shall not be permitted unless approved in writing.

All copper cables shall have stranded copper conductors with PVC insulation and an overall PVC sheath, unless otherwise specified. Cable sizes shall be selected with due consideration to voltage drop, particularly for cable runs exceeding 80 metres.

Security system cabling shall not be installed within or on cable containment containing other services without written approval. Security cable trays and containment shall be separate from UNSW IT and Communications cable trays and containment.

Any damaged, poorly supported or non-compliant cabling or containment shall be removed and rectified at the Security Contractor's cost. The UNSW Security Systems Representative may direct the Contractor to expose, withdraw, replace or rectify any cable or containment where damage or non-compliance is suspected.

7.1. Wiring and Cable

The following must apply with respect to wiring and cables:

- Installation that can be readily removed, repaired or replaced. At levels where there are no terminations, a loop of (2) two metres shall be provided.

- Wiring shall be loop-in method. Joining of cables will not be accepted other than those within the tampered termination cabinets.
- Where mechanical damage may occur, cables shall be protected by conduit or cable duct.
- All cables are to be pink sheathed and have stranded conductors.
- Attention shall be paid to voltage drop calculations when determining cable sizes.
- All multicore cables shall have a minimum of two spare cores over and above the requirements as set out in the table detailed in 6.1.2 below.

In addition, 4 core cable is to be run to all reed switch only doors.

Cables shall be appropriately labelled at both ends.

Communications cabling is to pass through equipment termination cabinets before termination to device.

Dedicated 240v mains supply by UNSW for all equipment from nominated distribution boards. Liaise with Security Systems Manager for appropriate locations and availability. (By others)

Fibre Optic cabling by UNSW.

7.2. Cable Support

All cables shall be supported by one of the following: catenary, cable tray, cable duct or the like and shall be:

- Suspended 600mm centre
- Looming at 300mm centres
- Not laid on ceiling tiles
- 300mm separation from other electrical circuits
- Spare data pairs to risers and readers (or 25% whichever is greater)

All cabling to EACS and IAS field devices cabling shall be provided with a pink sheath and shall be typically cabled in accordance with the following *Table, UNSW Cable/Wiring Requirements:*

Device	Cable	Core	Function
T Series Multi-Tech Card Reader / Terminal	6 Core	Red	+ Vdc
		Black	- Vdc
		White	HBUS A
		Blue	HBUS B
		Yellow	
		Green	
Mortice Lock	6 Core	Red	+ Vdc
		Black	- Vdc

		White	DOTL
		Blue	DOTL
		Yellow	DNL
		Green	DNL
	4 Core	Red	Green LED
		Black	<i>Spare</i>
		White	Exit
		Blue	Exit
Electric Strike	6 Core	Red	+ Vdc
		Black	- Vdc
		White	DOTL
		Blue	DOTL
		Yellow	DNL
		Green	DNL
Maglock / Drop Bolt	Fig 8	Non-Trace	- Vdc
		Trace	+ Vdc
	6 Core	Red	<i>Spare</i>
		Black	<i>Spare</i>
		White	DOTL
		Blue	DOTL
		Yellow	DNL
		Green	DNL
Auto Door / Auto Door Closer	6 Core	Red	
		Black	
		White	DOTL
		Blue	DOTL
		Yellow	DNL
		Green	DNL
	4 Core	Red	Day / Night
		Black	Day / Night
		White	<i>Door Trigger</i>

		Blue	Door Trigger
Request to Exit	6 Core	Red	+ Vdc
		Black	- Vdc
		White	N/C
		Blue	N/C
		Yellow	<i>Spare</i>
		Green	<i>Spare</i>
Break Glass	4 Core	Red	<i>Spare</i>
		Black	<i>Spare</i>
		White	N/C
		Blue	N/C
PIR	4 Core	Red	+ Vdc
		Black	- Vdc
		White	N/C
		Blue	N/C
Reed Switch	4 Core	Red	<i>Spare</i>
		Black	<i>Spare</i>
		White	DOTL
		Blue	DOTL

7.3. Cables in Ceiling Space

Cables shall be supported at intervals not exceeding 600mm utilising catenary wires. Alternatively, cables shall be installed on trays.

A clearance of 400mm is to be maintained from the false ceiling, luminaries, hot water pipes or other heat or electrical noise generating equipment and/or cables.

Cables shall be neatly grouped together and supported using approved clips or ties.

7.4. Conduits

Conduits shall be concealed wherever possible. Where the Security Contractor believes that it is not possible to conceal conduits, the UNSW Security Systems Representative's approval shall be gained in writing prior to installation of exposed conduits.

Install conduits in situ within wall cavity, secure ceiling, wall or floor space, contained in floor slab, chased into walls to be rendered and otherwise hidden by finished building structures. Should it appear not possible to conceal a conduit, clarify the position with the UNSW Security

Systems Representative, and do not proceed with the installation until advised by the UNSW Security Systems Representative.

In some exceptional circumstances, conduits may be installed surface mounted in coordination with other services installed within these buildings. However, approval shall be gained in writing from the UNSW Security Systems' Representative prior to installation.

If required, carry out chasing required and grouting in or recessed boxes, conduits and the like. Finish grouting flush with the wall surfaces.

Conduits installed must be:

- purpose made for all fittings, draw boxes, bends and couplings.
- joined using an approved solvent cement.
- secured using metal saddles spaced at 600mm (maximum) centers and within 150mm of all fittings.
- installed so that cables can be drawn in at draw boxes only. Inspection elbows shall not be classified as draw points.
- filled with cables to not more than 60% of its capacity; and
- between buildings or through set ceilings, a diameter of 50mm to be a minimum (if conduits installed underground).

7.5. Cable Duct

Where cables are installed in ducting, they shall be grouped, and cable tied for easy identification.

Holes in duct through which cables pass shall be grommited.

Changes in direction in duct shall be set such that the actual bending radius of cables is not smaller than the minimum bending radius of cables as per the manufacturer's recommendations.

Cables shall not be installed in ducts unless in a secure monitored area, and only after prior approval has been given by the UNSW Security Systems' Representative.

Cable duct must be:

- Fitted with removable covers.
- Fitted with the manufacturer's standard bends, elbows, couplings and reducers.
- Manufactured from extruded PVC.
- Filled with cables to not more than 60% of its capacity.

7.6. Fixings

All fixings must be comprised of:

- metal thread screws or bolts/dynabolts into expanding type masonry anchors for fixing to

concrete or masonry.

- full thread tapered woodscrews for fixing to timber; and
- suitable expanding anchors for fixings to gyprock.

8. INSPECTIONS, TESTING AND COMMISSIONING

During the Contract, the following types of testing and commissioning shall be conducted by the Security Contractor and UNSW Security systems:

- Works inspections.
- Factory Acceptance Testing.
- Pre-commission testing/Commissioning testing at the installation; and
- Performance and Acceptance testing at the installation.

The Security Contractor shall supply all labour, materials and equipment required to fully commission and test the installation.

All costs associated in demonstrating the performance of the security services, as required by the UNSW Security Systems Representative, shall be borne by the Security Contractor.

The Security Contractor must conduct all tests and inspections, as required by the UNSW Security Systems Representative, to ensure that the systems and all other Works comply with the requirements of the Contract.

Equipment which fails to operate correctly or is found to be installed incorrectly shall be repaired or replaced by the Security Contractor. Where any test is unsuccessful the defective equipment shall be repaired as appropriate and subjected to retest.

Equipment that fails consecutively within a six-month period must be replaced, not repaired.

All equipment to be installed must be documented and information provided to UNSW security systems.

Where the attendance of the UNSW Security Systems Representative, Consultant or other project stakeholders is required, the Security Contractor shall provide written notice of intention to test to the UNSW Security Systems Representative not less than ten working days prior to the conduct of testing.

Installation and/or equipment will only be accepted by the UNSW Security Systems Representative after satisfactory completion of testing.

The testing and commissioning aspect of the works shall allow for any programmed staging of Works as required by the UNSW Security Systems Representative. Where staging of works is applicable, elements of the works may require testing on several occasions as a result of the integration/relocation and commissioning of services and equipment as building works progress.

8.1. Works Inspections

During the course of the Contract, the UNSW Security Systems Representative shall randomly inspect the Works to assess that the Works comply with the requirements of this document.

As requested by the UNSW Security Systems Representative, assist the UNSW Security Systems Representative in performing these Works inspections, including the supply of labour, materials and equipment.

After a Works inspection, the UNSW Security Systems Representative may issue a Works Inspection Report detailing action to be taken to ensure that the Works comply with the requirements of this document.

8.2. Programming

All operating system programming and data entry will be carried out by UNSW Security Systems.

Detailed maps, cable schedules and drawings showing equipment zones, alarm inputs, locations, etc. must be made available to UNSW Security Systems for approval prior to the connection of devices. Power and network details (e.g. DB details, Network port details) for the controller is to be supplied to UNSW as part of the commissioning process.

Completed commissioning sheets detailing controller and hardware information is to be submitted at least 8 weeks (for large installations >8 controllers) or 2 weeks (small installations <4 controllers) prior.

Client data access levels, etc. will be programmed by UNSW Security Systems.

8.3. Testing and Commissioning

The Security Contractor shall fully test and commission all security services to ensure the correct operation of all systems prior to final Performance and Acceptance Testing with the UNSW Security Systems Representative.

During the conduct of commissioning, the Security Contractor shall:

- supply all labor, materials and equipment required to fully test and commission the complete installation to the satisfaction of the Security Manager.
- repair or replace any equipment which fails to operate correctly or does not comply with this Specification.
- any tests shall be carried out in the presence of the Security Systems Manager or his/her representative.
- confirm that all equipment is fully operational and provides the required functionality.
- provide a comprehensive final commissioning report outlining all test results and performance test data on all cables and any other information deemed necessary for future records.
- supply all labour, materials and equipment required to fully commission and test the installation to the satisfaction of the UNSW Security Systems Representative.
- allow for minor programming changes and camera view adjustments as a result of testing and commissioning and/or final performance and acceptance testing.
- repair or replace any equipment that fails to operate correctly, or is considered by the UNSW Security Systems Representative, to be installed incorrectly or not optimally; and

- hand over all passwords installed as part of these Works to the UNSW Security Systems Representative

8.3.1. Commissioning Reports

A Commissioning Test Sheet must be submitted for approval by UNSW Security Systems Representative three weeks prior to the conducting of the full testing and commissioning of the installation.

Commissioning Reports must be submitted in both electronic and hard copy within a week of the completion of each Commissioning Period.

The Commissioning Reports shall include:

- completed, signed and dated Commissioning Test Sheets (A3 size and coloured prints);
- a comprehensive description outlining all tests, results, rectification details, performance test data, and any other information deemed necessary by the UNSW Security Systems Representative for future records.
- actual test equipment images and results, as requested by the UNSW Security Systems Representative.
- relevant system printouts of system data recorded during the Commissioning; and
- dates, times, personnel performing each duty, assisting UNSW Security Systems personnel and the like.
- list of doors with the type of locks installed (and whether they are fail safe or fail secure and connected to the Fire Trip)
- A load calculation needs to be provided – based on all hardware being energized on maximum load according to the manufacturer's specifications.
- Whether each lock is Fail Safe or Fail Secure.
- Which locks are connected to the Fire Panel to release in the event of an emergency

The associated UNSW Security Systems witnessed acceptance testing shall not commence until the Commissioning Report is accepted by the UNSW Security Systems Representative.

The system commissioning documents shall be independent to and separate from the cable schedules, quality assurance and control procedures.

Each test performed shall be signed and dated by the Security Contractor personnel performing the commissioning.

All commissioning sheets with details of controllers, readers, inputs, outputs, expansion boards) must be submitted to UNSW Security Systems at least 7 weeks for large projects (installs that consist of >5 Controllers), or 2 weeks for smaller projects (installs that consist of <5 Controllers) prior to equipment scheduled to come online.

8.3.2. Performance and Acceptance Testing

Final performance and acceptance testing shall be conducted by the Security Contractor and witnessed by the UNSW Security Systems Representative, as a means of demonstrating that all works have been completed and are in accordance with the Specification.

Completion will only be granted once the UNSW Security Systems Representative is satisfied that the whole of the security services installation satisfies the requirements of the Contract.

The Performance and Acceptance Testing of the security services shall be conducted both during normal daylight hours and again at night after hours, as required, and to the approval of the UNSW Security Systems' Representative.

During the Performance and Acceptance Testing, the following items, as a minimum, shall be inspected and witnessed:

- physical inspection of the installation (including the inspection of all head-end equipment, controller, field devices and the like).
- testing of the local functionality of equipment and devices.
- testing of alarm response and annunciation of each point and device.
- check logging and recording of activity for each alarm point and device.
- test required interface with other systems for each alarm point and devices; and
- confirmation that each system performance complies with the project specification.

8.4. Completion

Completion shall only be granted when:

- a physical inspection of the works and functional testing is completed to the satisfaction of the UNSW Security Systems Representative.
- testing and commissioning of all installed equipment is completed, and commissioning sheets signed off by the UNSW Security Systems Representative.
- commissioning, Performance and Acceptance Testing of each system have been completed to the approval of the UNSW Security Systems Representative.
- the UNSW Security Systems Representative is satisfied that all the systems are operating in the correct and specified manner.
- all equipment has been proven to operate faultlessly for a total period of 14 days following the successful performance and acceptance testing of the systems.
- training has been undertaken to a satisfactory level of competency, to the UNSW Security Systems Representative 's approval.
- all documentation has been supplied to the UNSW Security Systems Representative and final draft approval given. This includes all documentation as specified in this specification and Contract.

- all critical defects, as defined by the UNSW Security Systems Representative have been rectified and a programme has been submitted to rectify all remaining defect items (including outstanding variations); and
- all relevant passwords, keys and equipment have been handed back to the UNSW Security Systems Representative.

8.5. Warranty/Defects Liability Period

Once the security equipment has been installed, programmed, tested as per the 'as for construction' design. UNSW FM Security Systems are required to witness test and sign-off on the installation at Practical Completion at which point the Defects Liability Period (DLP), of 12 months, will commence.

As a condition precedent to the end of the DLP, it is a requirement that there are to be no faults or issues with the equipment within 3 months of the DLP end date, as identified by the DLP Maintenance Logs.

It is expected that at the time of the DLP expiration, the contractor will provide evidence that the Security Systems have been tuned to meet the performance of the building and the system is performing equal to or better than at the time of Practical Completion.

9. MONITORING

Each door should monitor a separate input for open sensor (Door Open Too Long), Lock Sensor (Door Not Locked) unlock output and request to exit (for mortice locks). Maglocks to monitor bond sense (Door not locked), a separate reed will provide a DOTL monitor, breakglass and exit button. Strikes to monitor Door Not Locked (strike coil), Door Open Too Long (reed). Auto doors to monitor Door Not Locked, Door Open Too Long, Request to Exit and Break-Glass.

PIRs must monitor normally closed state and tamper.

Supply and install an Intruder Alarm system (IAS). The IAS shall be an integrated function of the EACS / SMS and provide commercial grade intruder detection alarm monitoring to nominated areas. The IAS shall monitor and report the state of intrusion detection and monitoring devices as shown on the drawings.

The IAS shall monitor the status of various doors, roller doors and rooms through reed switches, movement detection devices, tamper switches and the like, and in the event of an alarm or tamper, report this status to the Security Management System (SMS).

The IAS shall be capable of monitoring the following Intrusion Detection Equipment but not be limited to:

- Reed switch units.
- Tamper switches.
- Passive Infra-Red (PIR) detectors; and
- Others intruder detection points as shown on the drawing.

Nominated alarms shall be monitored on a 24/7 basis.

9.1. IAS Configuration and Control

Arrange, install and commission an intruder detection system as an integral part of the SMS to achieve intruder detection in the areas as indicated on the drawings.

A separate sector shall be provided to control each intrusion detection device, including a separate sector for each tamper switch. The devices and sectors must be capable of being grouped into user defined areas.

When the IAS area/zone/sector is armed, movement within the area covered by the movement detectors, activation of a door reed switch or other IAS device shall initiate an alarm.

Unauthorised tampering with intrusion alarm detectors, cabling or equipment cabinets shall cause a tamper alarm to be reported to the SMS. The tamper circuits shall operate twenty-four hours per day, regardless of whether the system is "armed" or "disarmed" and each detector, device or system tamper shall be identified individually.

The system shall be fail-safe to the alarm condition, in the event of a total power failure.

A separate sector (i.e. zone) shall be provided to control each intrusion detection device, including separate identification for each tamper switch. The devices and sectors must be capable of being grouped into user defined Areas.

The IAS shall be microprocessor based, configured to monitor all alarm devices. The system shall interface with the SMS for monitoring of all alarm points and users.

The IAS shall include the capacity to allow 20% future expansion without the need for additional hardware or software.

9.2. Reed Switches

Supply and install a 19mm recessed reed switch (or approved equivalent) into the door and doorframe at the location shown on the drawings. These reed switches are to be secured in the door frame with glue/silicon.

All access control doors shall be provided with independent reed switches for each door leaf.

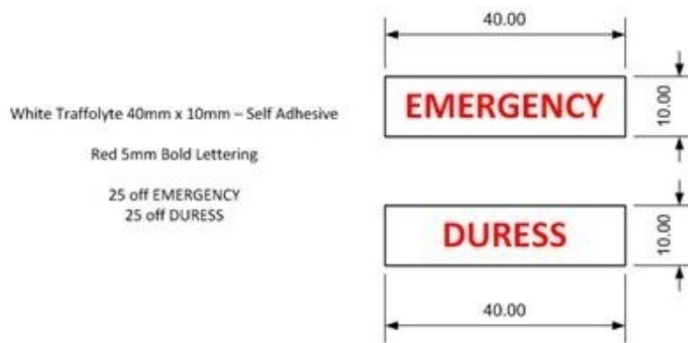
Terminate cabling at both ends and install End of Line Resistors at the reed switch. Solder and heat shrink all cable terminations as specified.

It shall remain the Security Contractor responsibility to ensure that the device is fully operational following installation and connection to the IAS and SMS system.

9.3. Duress Buttons

Supply and install Fixed Duress buttons in the locations as nominated on the Tender Drawings. Duress buttons shall be under-desk mounted, unless noted otherwise. All duress buttons shall be fixed using temper-resistant fixings.

Desk mounted duress alarm push buttons shall be the SMART1001(SD/001) Hold up device, single action shrouded button. Duress required in wet areas are to be Schneider XALK01 (Pushbutton Enclosure Yellow)/ZB5a5844 (Mushroom twist reset Red)/ZENL1121 (Contact Block mount). All duress buttons to have white traffolyte labels with 'Emergency Duress' please see below dimensions of labels:



Wall mounted duress buttons shall be nominally mounted at app. 1100mm (centred) above finished floor level.

The duress alarm push button monitoring shall be integrated to and monitored by the IAS. Duress alarms shall be programmed to a 24-hour zone of the IAS and shall not be affected by the arming/disarming of the system.

For instances where wireless duress buttons are required, UNSW Security Systems must be consulted prior to any wireless duress button installation. Wireless button to be Inovonics EN42X series. Each button must be separately programmed on a separate input (which specifies location i.e. room number). Battery low for each device to also be monitored on a separate input)

Locations where a duress button is installed, must have a CCTV camera viewing the area

9.4. Gallagher T20 Terminal

Gallagher T20 Terminals (multitech) shall provide the system arming and disarming functions necessary to provide management of security operations installed within each Area.

T20 units shall always be installed within the protected area where possible and shall be installed at the locations nominated on the Drawings.

All terminals are to be accessible by card reader, not PIN only.

These units are to be installed as a HBUS unit and provide the local interface to the functions necessary to provide management of the IAS and shall including the following minimum functions and features:

- an on-board microprocessor;
- RS485 LAN connection to the SMS Controller.
- a minimum of 8 Areas (or Zones).
- arming and disarming of Area or alarm inputs.
- activating/deactivating control outputs (momentary or latched), subject to an area's disarmed/armed activation.
- built-in device tamper switch; and

- graphical LCD icons for display of area and alarm status.
- Built in card reader

Viewing and modification of user codes shall be available via the SMS, using an appropriate operator access level. Codes shall be capable of being any combination of four to eight digits.

Upon an alarm condition the T20 unit shall provide clear visual indication, via LCD text description, of each area in alarm.

T20 Units shall be monitored by the SMS for the following alarms, providing information on which unit has stopped operating and its location:

- Off-line (heartbeat monitoring)
- Tamper (removal of unit from wall).

9.5. Status Indicator Panels

Provide local Status Indicators mounted on the ceiling or wall directly above the door(s) at the locations nominated on the drawings. Status indicators shall be clearly visible prior to entering a protected area and illuminate the alarm status of the associated protected area.

The Status Indicator shall provide visual indication of the IAS as follows:

- GREEN Indicator Lamp – to illuminate when the area is in Access Mode (i.e. disarmed);
- AMBER Indicator Lamp – to illuminate when the area is Secure (i.e. armed). Amber indicator to flash whilst the system is in entry or exit delay mode; and
- RED Indicator Lamp – to illuminate when the area is in Alarm.

The status indicator lights shall provide clear indication of the status of the Secure Area from outside the protected area in all ambient lighting conditions.

Status indicator lights shall consist of a stainless-steel electrical switch plate with coloured indicator LED lights with engraved labelling on the faceplate. Submit a sample of the proposed status indicator lights prior to installation. Lamps with incandescent globes will not be accepted.

9.6. Passive Infrared Sensors (PIRs)

PIRs must be:

- Dual Technology PIR & Microwave – Paradox 525DM/DG467 (360 degree)*
- Selectable pulse count and walk test facility

Please refer to 6.9

***For high security areas, further discussions required with Security Systems Manager to determine equipment required.**

10. CLOSED CIRCUIT TELEVISION SYSTEM (CCTV)

Genetec is the CCTV Video Management System used at UNSW. All cameras record to the University's CCTV server which is located in an off-campus data centre.

Location of CCTV cameras to be as per UNSW CCTV Surveillance Strategy Security guidelines and the EM Security and Traffic Design Standards and must be approved by UNSW Security Systems.

The System shall offer a high level of flexibility and automation to maximise operator efficiency and to minimise operator error. Cameras shall be selected automatically and displayed to the CCTV monitors in the event of an alarm being detected by the CCTV System and SMS/EACS High Interface alarms.

All video inputs shall be recorded and available for live viewing and playback, simultaneously at real time (i.e. 30 images per second) without any degradation or impact to system performance.

The CCTV Systems shall provide sufficient storage capacity for recording of all CCTV cameras at 1080p resolution for a minimum of 30 days.

CCTV cameras must be as per the below model/make and must be Onvif compatible.

The provision of the CCTV System shall include, however not be limited to, the supply and installation of:

- fixed and PTZ Colour Cameras – Full body and Dome.
- camera housings and mounting brackets.
- camera installation, positioning and cabling to the network switch.
- interfacing with other systems as described further in this document;
- all necessary software and hardware to achieve fully operational system which meets the intent of this specification.
- all necessary equipment enclosures, racks and panels; and
- network ports to be installed through UNSW IT services on relevant VLAN (UNSW Security systems to advise) with POE enabled.
- All cameras that do not have concealed cable connection should either be ducted into the body of the camera or connected with a conduit bracket.

10.1. Standards and Compliance

CCTV cameras must comply with the following:

- Minimum of 1080p resolution.
- Minimum 30 frames per second.
- While proprietary formats may be available, it is mandatory that the system shall be configured to ensure compliance with the H.265 solution.
- Supports Power over Ethernet (PoE) 802.3af, 12 VDC.

- Dual streaming (H.265 and MJPEG video simultaneously).
- True day/night functionality.
- True high-definition video (minimum of 2.0 megapixels).
- Motorized focus and zoom (controlled remotely); and
- Local storage: Video data can automatically be recorded to a Micro SD Card when the camera loses network connectivity.
- A Genetec camera licence, fail over licence and SMA component must be included per camera for every camera installed

10.2. IP Indoor and Outdoor Approved CCTV Cameras (and Associated Housing)

All indoor single lens cameras to be Axis P3285-LV and external dome cameras to be: AXIS P3285-LVE. Cameras in lift cars to be Axis M3086-V.

10.3. PTZ Cameras (and Associated Housing)

PTZ camera to be: AXIS 5676-E MK II.

PTZ camera with multi directional camera: Axis Q6300-E, Axis Q6325-LE and POE Injector.

Cameras must be ONVIF compatible. The security contractor is to allow for all additional CCTV server, storage and licensing.

10.4. Multidirectional Camera

Axis P3735-PLV Multidirectional camera

10.5. Dual-Head Camera

Axis P4705-PLVE 2 MP/P4707-PLVE 5MP Dual Head Camera

10.6. CCTV Storage

CCTV Archiver Server requirements shall be determined based on the capacity of the existing UNSW CCTV server fleet and the number of cameras being introduced by the project.

The intent of this requirement is to ensure sufficient CCTV recording, storage, redundancy and failover capacity is maintained, while avoiding the unnecessary provision of additional Archiver Servers where sufficient capacity is available within the existing UNSW CCTV server fleet.

For the purposes of this specification, one (1) pair of Archiver Servers comprises two (2) physical servers:

- One (1) Production (PROD) Archiver Server; and
- One (1) Disaster Recovery (DR) Archiver Server.

The following requirements shall apply:

- **Up to thirty (30) cameras:** Additional Archiver Servers are not automatically required. Prior to installation, the UNSW Security Systems Representative shall confirm whether sufficient

capacity is available within the existing CCTV server fleet to accommodate the additional cameras and associated thirty (30) day minimum recording retention requirement.

Prior to procurement, the UNSW Security Systems Representative shall review the available capacity of the existing CCTV server fleet and confirm whether the proposed Archiver Server pair is required.

- **Thirty-one (31) to eighty (80) cameras:** The project shall allow for the provision of one (1) pair of **Genetec Streamvault SV-2041E-R15-240T-20** Archiver Servers, comprising one (1) PROD Archiver Server and one (1) DR Archiver Server.

Model: SV-2041E-R15-240T-20
Processor: 1 x Xeon Silver 4416+
Memory: 32 GB (Recommended)
Storage: 196 TB
Storage bays: 15 (12 used - 3 free)
Form factor: 2U
RAID: RAID 6

- **More than eighty (80) cameras (up to 250 maximum):** The project shall allow for the provision of one (1) pair of **Genetec Streamvault SV-4041EX-R28-672T-24** Archiver Servers, comprising one (1) PROD Archiver Server and one (1) DR Archiver Server.

Model: SV-4041EX-R28-672T-24
Processor: 2 x Xeon Gold 5416S
Memory: 64 GB (Recommended)
Storage: 564.48 TB
Storage bays: 28 (28 used - 0 free)
Form factor: 2U
RAID: RAID 60

Where sufficient capacity is not available, or if the camera count exceeds 250, a detailed server and storage capacity assessment shall be undertaken. The number, model and configuration of Archiver Servers required shall be determined based on the total camera load, storage, bandwidth, retention, redundancy, failover and system performance requirements and shall be approved by the UNSW Security Systems Representative.

Camera quantities shall be assessed against the total project scope, including all stages, packages and separable portions of the works. Projects shall not be divided or staged for the purpose of avoiding the applicable Archiver Server requirements.

The availability of existing server capacity shall not be assumed by the Contractor or Consultant. Existing capacity must be confirmed in writing by the UNSW Security Systems Representative prior to finalisation of the CCTV design.

Only the current holder of the UNSW CCTV Maintenance and Support Contract shall be permitted to rack, stack, physically install, configure, commission and integrate Archiver Servers into the UNSW CCTV server fleet.

All proposed server configurations, camera allocations and storage calculations shall be submitted to the UNSW Security Systems Representative for review and approval prior to procurement.

10.7. LPR (Licence Plate Recognition) cameras

UNSW Security Systems representative to approve any LPR camera installation. LPR cameras to be **Genetec AutoVu Sharp AU-K-V-WS850-LC-000** and be installed as per Genetec LPR specifications. For LPR cameras installed at vehicle/Registration height, a bollard (manufactured by Gunnebo) is required to house this LPR camera. UNSW Security Systems to advise specifications of custom made bollard.

All LPR cameras to include:

- GSC-OM-E-1C – Genetec Enterprise camera licence for viewing and recording.
- GSC-AV-S-1SHP – Genetec AutoVu Standard LPR licence.
- ADV-LPR-F-5Y – Five-year SMA/support for the AutoVu fixed LPR licence.
- ADV-CAM-E-5Y – Five-year SMA/support for the Enterprise camera licence.

LPR cameras to be connected to a POE+ network together with power injector.

10.8. CCTV Licencing

The following licences are required to be provided per camera:

- GSC-OM-E-1FC - Genetec Omnicast Failover Camera Connection GSC-Om-E-1FC
- ADV-CAM-E-5Y - 1 x Genetec 5YR SMA
- GSC-OM-E-1C - 1 x Genetec Enterprise Camera License

10.9. Existing CCTV Cameras

In areas being refurbished where existing CCTV cameras are installed, cameras must be replaced with an Axis model in accordance with this specification if the existing camera is a different brand or model. Security Systems must be consulted to confirm whether coverage is required and determine the most suitable camera model.

11. Defects Liability

Provide a warranty for all equipment, materials, works and the like for a Defects Liability Period of one calendar year (plus).

The Defects Liability period shall only commence from the date Practical Completion is granted in writing by the UNSW Security Systems.

All works implemented as part of this Contract which proves to be faulty from workmanship or materials shall be, without additional charge, “fully maintained and serviced” during the defects liability period. “Fully maintained and serviced” shall include:

- immediate correction or replacement of all equipment, materials and works, which prove faulty. Correction or replacement of faulty equipment shall continue until the system is fully operational.
- replacement of all faulty equipment, materials and works, within 24 hours if immediate correction cannot occur; and
- preventative maintenance including quarterly maintenance visits to inspect, assess system diagnostic reports, test and maintain the system operation in accordance with the performance parameters of this specification.

During the Defects Liability Period perform such corrective works as may be instructed in writing by the UNSW Security Systems Representative within five days of such notice.

All works carried out during each visit shall be recorded and copies of all records forwarded to the UNSW Security Systems Representative within seven days of the conduct of the visit.

12. Mechanical Lock and Door Hardware

Please see the list below for the brands and models of each item. No deviations from this list are allowed. Any hardware or locks installed that are not listed will be considered non-compliant and must be replaced

12.1. Mechanical Locks

Dorma Kaba or Assa Abloy to be used for all mechanical locks. Must be one of the following depending on door type installed:

Brand/Supplier	Part number	Item Description	Notes	Item Picture
ASSA ABLOY	3772SS	Lockwood 60mm back set mortice lock in Satin Stainless finish	For single or double timber doors or wide style aluminium doors  Fire rated 4-Hours	
	3772PB	Lockwood 60mm back set mortice lock in Polished Brass finish (Polished Brass finish in C22 - Chancellery Building only)		
Dormakaba	MS2SS	Dormakaba MS2 60mm back set mortice lock in Stainless Steel finish	For single or double timber doors or wide style aluminium doors  Fire rated 4-Hours	
ASSA ABLOY	3573SC	Lockwood 60mm back set mortice lock in Satin Stainless finish	For sliding single or double timber doors or sliding wide style aluminium doors  Fire rated 4-Hours	
	3573PB	Lockwood 60mm back set mortice lock in Polished Brass finish (Polished Brass finish in C22 - Chancellery Building only)		
ASSA ABLOY	3782SS	Lockwood 23mm back set mortice lock in Satin Stainless finish	For single or double narrow style aluminium doors	
	3782PB	Lockwood 23mm back set mortice lock in Polished Brass finish (Polished Brass finish in C22 - Chancellery Building only)		
Dormakaba	SBMSC	Dormakaba 23mm back set mortice lock in Satin Stainless finish	For single or double narrow style aluminium doors	
ASSA ABLOY	3541L1SC	Lockwood 23mm back set mortice dead lock Satin Chrome finish	For single or double sliding narrow style aluminium doors	
Carbine	Acrobat series	With inner escape lever		
ADI	44143000	ADI Lockbolt - SL5 Slimline Satin Chrome	For secondary door leaf locking, when a room need to be secured. ie. Labs with extra wide doors	
ADI	44142000	ADI Lockbolt - 5004 Satin Chrome		
	Notes:	Must be installed on the inside of the door and if required a extended bolt can be installed.		
Carbine	PD7000-L1	Commercial Leverset - Only to be used on existing doors as a like for like replacement	AS1428 Compliant Lever Fire Rated 4hrs	
	PD7062-L1			
	PD7012-L1	Any new doors are to be mortise locks as above.		
	PD7082-L1			

12.2. Mechanical Lock Door Hardware

Assa Abloy door hardware to be used for all doors. Must be Satin Chrome and one of the following – depending on door type installed:

Brand/Supplier	Part number	Item Description	Notes	Item Picture
ASSA ABLOY	1801/1905/70SC	Square end plate handles	For single or double timber doors or wide style aluminium doors	
		Outside plate with cylinder hole and lever, concealed fixing SC		
Dormakaba	601C/601V/25SC	Inside plate with lever only, visible fixing SC	 Fire rated 4-Hours	
ASSA ABLOY	1801/1904/70SC	Square end plate handles	For single or double timber doors or wide style aluminium doors	
		Outside plate with cylinder hole and lever, concealed fixing SC		
Dormakaba	601C/613V/25SC	Inside plate with turn snib and lever, visible fixing SC	 Fire rated 4-Hours	
ASSA ABLOY	1800/1905/70SC	Square end plate handles	For single or double timber doors or wide style aluminium doors	
		Outside plate with cylinder hole only, concealed fixing SC		
Dormakaba	604C/601V/25SC	Inside plate with lever only, visible fixing SC	 Fire rated 4-Hours	
ASSA ABLOY	1807/1905/70SC	Square end plate handles (Exit only)	For single or double timber doors or wide style aluminium doors	
		Outside blank plate only, concealed fixing SC		
Dormakaba	605C/601V/25SC	Inside plate with lever only, visible fixing SC	 Fire rated 4-Hours	
ASSA ABLOY	1814/1939/70LDSC	Square end plate handles	For single or double timber doors or wide style aluminium doors	
		Outside plate with indicating slot and lever, concealed fixing SC		
Dormakaba	653C/613VDA/25SC	Inside plate with disabled turn LH, visible fixing SC	 Fire rated 4-Hours	
ASSA ABLOY	1814/1939/70RDSC	Square end plate handles	For single or double timber doors or wide style aluminium doors	
		Outside plate with indicating slot and lever, concealed fixing SC		
Dormakaba	653C/613VDA/25SC	Inside plate with disabled turn RH, visible fixing SC	 Fire rated 4-Hours	
ASSA ABLOY	4801/4905/70SC	Square end narrow style plate handles	For single or double narrow style aluminium doors	
		Outside plate with cylinder hole and lever, concealed fixing SC		
Dormakaba	N601C/N602V/25SC	Inside plate with lever only, visible fixing SC		
ASSA ABLOY	4801/4904/70SC	Square end narrow style plate handles	For single or double narrow style aluminium doors	
		Outside plate with cylinder hole and lever, concealed fixing SC		
Dormakaba	N601C/N613V/25SC	Inside plate with turn snib and lever, visible fixing SC		
ASSA ABLOY	4800/4905/70SC	Square end narrow style plate handles	For single or double narrow style aluminium doors	
		Outside plate with cylinder hole only, concealed fixing SC		
Dormakaba	N604C/N602V/25SC	Inside plate with lever only, visible fixing SC		
ASSA ABLOY	4807/4905/70SC	Square end narrow style plate handles (Exit only)	For single or double narrow style aluminium doors	
		Outside blank plate only, concealed fixing SC		
Dormakaba	N605C/N602V/25SC	Inside plate with lever only, visible fixing SC		
ASSA ABLOY	4804/4939/70SC	Square end narrow style plate handles	For single or double narrow style aluminium doors	
		Outside plate with emergency slot and lever, concealed fixing SC		
		Inside plate with disabled turn and lever, visible fixing SC		
ADI	4144020	ADI small 201 cylinder pull	For single or double narrow style aluminium doors	
		Used with Kaba NL550SS rim locks for a pull handle		

12.3. Electronic Locks & Magnetic Locks

Must be Satin Chrome and one of the following – depending on door type installed:

Brand/Supplier	Part number	Item Description	Notes	Item Picture
ASSA ABLOY	3570ELMOSC	Lockwood 60mm back set electric mortice lock Satin Stainless finish	For single or double timber doors or wide style aluminium doors	
		Electric Mortice Lock Fail Secure & Monitored	 Fire rated 4-Hours	
ASSA ABLOY	3782ELSS	Lockwood 23mm back set electric mortice lock Satin Stainless finish	For single or double narrow style aluminium doors	
		Electric Mortice Lock Fail Secure & Monitored		
ASSA ABLOY	ES2000	Padde monitored 12 or 24v field changeable electric strike	For single or double timber & aluminium doors	
		Electric Strike Fail Secure & Monitored	 Fire rated 4-Hours	
ASSA ABLOY	EMZ8-SM	Padde Z8 series single monitored electromagnetic lock 580kg	For single timber or aluminium doors	
		Electric Single Maglock & Monitored	 Fire rated 4-Hours	
ASSA ABLOY	EMZ8-DM	Padde Z8 series double monitored electromagnetic lock 1100kg	For double timber or aluminium doors	
		Electric Double Maglock & Monitored	 Fire rated 4-Hours	
Dormakaba	SL30DBL	Dormakaba Cobolt electronic side load lock 100kg	For timber or aluminium doors	
		Electric lock, Fail Secure & Monitored		
Dormakaba	SL30SGL	Dormakaba Cobolt mini electronic side load lock 100kg	For timber or aluminium doors	
		Electric lock, Fail Secure & Monitored		

12.4. Electronic Lock Door Hardware

Brand/Supplier	Part number	Item Description	Notes	Item Picture
ASSA ABLOY	1820/1905/70SC	Lockwood square end plate handles with outer LED indicator 1820/70SC outside lever with cylinder LED indicator concealed fixing SC 1905/70SC inside lever visible fixing SC (NO LED) Cardax or CATS electrically operated doors	For single or double timber doors or wide style aluminium doors  (for internal doors only) Fire rated 4-Hours	
ASSA ABLOY	1820/1922/70SC	Lockwood square end plate handles with LED indicators 1820/70SC outside lever with cylinder LED indicator concealed fixing SC 1922/70SC inside lever with LED indicator visible fixing SC Cardax or CATS electrically operated doors	For single or double timber doors or wide style aluminium doors  (for internal doors only) Fire rated 4-Hours	
ASSA ABLOY	4811/4905/70SC	Lockwood square end narrow style plate handles with outer LED 4811/70SC outside lever with cylinder LED indicator concealed fixing SC 4905/70SC inside lever visible fixing SC (NO LED) Cardax or CATS electrically operated doors	For single or double narrow style aluminium doors (for internal doors only)	
ASSA ABLOY	4811/4912/70SC	Lockwood square end narrow style plate handles with LED indicators 4811/70SC outside lever with cylinder LED indicator concealed fixing SC 4912/70SC inside lever with LED indicator visible fixing SC Cardax or CATS electrically operated doors	For single or double narrow style aluminium doors (for internal doors only)	

12.5. Door Closer Hardware

The following Door closers are to be installed on all mechanical doors (except where not required – e.g. individual offices), electronic strikes and electronic mortise locks

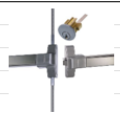
Brand/Supplier	Part number	Item Description	Notes	Item Picture
Allegion	1461SV	LCN standard arm or parrelle arm door closer EN 1-6 in silver	For single and double timber and aluminium doors	
			 Fire rated 4-Hours	
Allegion	1460TSV	LCN slide arm door closer EN 1-6 in silver	For single and double timber and aluminium doors	
			 Fire rated 4-Hours	
Dormakaba	TS83SIL	Dormakaba TS83 standard arm door closer in silver	For single and double timber and aluminium doors	
			 Fire rated 4-Hours	
Dormakaba	TS93GSIL	Dormakaba TS93G "PUSH SIDE" door closer EN 1-5 in silver	For single and double timber and aluminium doors	
			 Fire rated 4-Hours	
Dormakaba	TS93BSIL	Dormakaba TS93B "PULL SIDE" door closer EN 1-5 in silver	For single and double timber and aluminium doors	
			 Fire rated 4-Hours	
Dormakaba	RTS853F	Dormakaba RTS85 EN 3 non hold open concealed transom closer	For single and double timber and aluminium pivot doors	
		For internal doors up to 950mm wide and 110kg in weight	 Fire rated 4-Hours	
Dormakaba	RTS853HO	Dormakaba RTS85 EN 3 with hold open concealed transom closer	For single and double timber and aluminium pivot doors	
		For internal doors up to 950mm wide and 110kg in weight	Has Hold Open feature	
			NOT suitable for Fire Doors	
Dormakaba	RTS854F	Dormakaba RTS85 EN 4 non hold open concealed transom closer	For single and double timber and aluminium pivot doors	
		Non Hold Open for Fire Doors up to 950mm wide and 110kg in weight	 Fire rated 4-Hours	
Dormakaba	RTS854HO	Dormakaba RTS85 EN 4 with hold open concealed transom closer	For single and double timber and aluminium pivot doors	
		For internal doors up to 950mm wide and 110kg in weight	Has Hold Open feature	
			NOT suitable for Fire Doors	
Dormakaba	RTS855F	Dormakaba RTS85 EN 5 non hold open concealed transom closer	For single and double timber and aluminium pivot doors	
		Non Hold Open for Fire Doors up to 1250mm wide and 110kg in weight	 Fire rated 4-Hours	
Dormakaba	RTS855HO	Dormakaba RTS85 EN 5 with hold open concealed transom closer	For single and double timber and aluminium pivot doors	
		For internal doors up to 1250mm wide and 110kg in weight	Has Hold Open feature	
			NOT suitable for Fire Doors	
Dormakaba	BTS75SSNHO	Dormakaba BTS75 EN 1-4 in ground floor spring non hold open SS cover	For single and double timber and aluminium pivot doors	
		For doors up to 110mm wide and 120kg in weight	Has Hold Open feature	
			NOT suitable for Fire Doors	

Dormakaba	BTS75SSHO	Dormakaba BTS75 EN 1-4 in ground floor spring with hold open SS cover For doors up to 110mm wide and 120kg in weight	For single and double timber and aluminium pivot doors Has Hold Open feature NOT suitable for Fire Doors	
Dormakaba	BTS804HO	Dormakaba BTS80 EN 3 in ground heavy duty floor spring with hold open For doors up to 950mm wide and 300kg in weight	For single and double timber and aluminium pivot doors Has Hold Open feature NOT suitable for Fire Doors	
Dormakaba	BTS805HOSS	Dormakaba BTS80 EN 5 in ground heavy duty floor spring with hold open For doors up to 1100mm wide and 300kg in weight	For single and double timber and aluminium pivot doors Has Hold Open feature NOT suitable for Fire Doors	
Dormakaba	BTS806HOSS	Dormakaba BTS80 EN 6 in ground heavy duty floor spring with hold open For doors up to 1400mm wide and 300kg in weight	For single and double timber and aluminium pivot doors Has Hold Open feature NOT suitable for Fire Doors	
Dormakaba	BTS80F4	Dormakaba BTS80F EN 4 in ground heavy duty fire rated floor spring SS cover Non Hold Open for Fire Doors up to 1100mm wide and 300kg in weight	For single and double timber and aluminium pivot fire doors  Fire rated 4-Hours	
Dormakaba	BTS80F5	Dormakaba BTS80F EN 5 in ground heavy duty fire rated floor spring SS cover Non Hold Open for Fire Doors up to 1400mm wide and 300kg in weight	For single and double timber and aluminium pivot fire doors  Fire rated 4-Hours	
Dormakaba	BTS80F6	Dormakaba BTS80F EN 6 in ground heavy duty fire rated floor spring SS cover Non Hold Open for Fire Doors up to 1400mm wide and 300kg in weight	For single and double timber and aluminium pivot fire doors  Fire rated 4-Hours	
Dormakaba	EMB804	Dormakaba EN 4 in ground Electromagnetic Hold Open fire rated floor spring Hold Open for Fire Doors up to 1100mm wide and 300kg in weight	For single and double timber and aluminium pivot fire doors  Fire rated 4-Hours	
Dormakaba	EMB805	Dormakaba EN 5 in ground Electromagnetic Hold Open fire rated floor spring Hold Open for Fire Doors up to 1400mm wide and 300kg in weight	For single and double timber and aluminium pivot fire doors  Fire rated 4-Hours	
Dormakaba	EMB806	Dormakaba EN 6 in ground Electromagnetic Hold Open fire rated floor spring Hold Open for Fire Doors up to 1400mm wide and 300kg in weight	For single and double timber and aluminium pivot fire doors  Fire rated 4-Hours	

12.6. Panic Bar and Exit Hardware

Dorma Kaba to be used where required. Must be Satin Chrome and one of the following – depending on door type installed:

Brand/Supplier	Part number	Item Description	Notes	Item Picture
Dormakaba	ED22MFSS	Dormakaba ED22M single panic bar with mortice lock SSS Can be installed with outside handle and security cylinder for access if required	For single timber doors  Fire rated 4-Hours	
Dormakaba	ED22EOFSS	Dormakaba ED22E single panic bar exit only SSS	For single timber doors  Fire rated 4-Hours	

Dormakaba	ED2227EOFSSS	Dormakaba ED2227 top & bottom locking panic bar exit only SSS	For single or double timber doors  Fire rated 4-Hours	
Dormakaba	ED22DPFSSS	Dormakaba ED22 2-door panic bar kit exit only SSS	For single or double timber doors  Fire rated 4-Hours	
Dormakaba	ED22DPNLFSSS	Dormakaba ED22 2-door single and top & bottom locking panic bar with keyed cylinder for entry SSS	For single or double timber doors  Fire rated 4-Hours	
Dormakaba	PHA201	Dormakaba PHA2000 single point panic exit only bar in silver Max door weight 200kg and width 1000mm	For single timber or aluminium doors  Fire rated 4-Hours	
Dormakaba	PHA203	Dormakaba PHA2000 3-Point locking panic exit only bar in silver Max door weight 200kg, width 1000mm & height 2270mm	For single or double timber or aluminium doors  Fire rated 4-Hours	
Dormakaba		Dormakaba PHA2000 3-Point double door locking panic exit only bar in silver Max door weight 200kg, width 1000mm & height 2270mm	For double rebated timber or aluminium doors  Fire rated 4-Hours	
Dormakaba	PHT05	Dormakaba PHT outside locking lever handle in silver	Suitable for the UNSW security key system cylinders  Fire rated 4-Hours	

12.7. Auxiliary Locks and Hardware

Brand/Supplier	Part number	Item Description	Notes	Item Picture
BiLock	A7589QCP	BiLock 2-position push lock in chrome plate Used for the upper lectern hinged cover	CATS Lecterns	
Allegion	SCL25636	Schlage CL1000 square backed cupboard lock in satin chrome plate Used for the lower lectern hinged cupboard door(s)	CATS Lecterns	
Carbine	CLH-RNC	Electrical / switch cabinet L-Handle in chrome plate (Keyed to UNSW key)	UNSW Orange Switchboards	
Lock Focus	A/HL8P	Electrical / switch cabinet L-Handle in chrome plate (Padlock)	UNSW Orange Switchboards	
Dormakaba	1234SC	Dormakaba double door sequence door selector	For double timber or aluminium doors  Fire rated 4-Hours	
Dormakaba	2300	Dormakaba BTS floor spring sealing compound for external or wet area doors		
SELECTLOK	1107SBB04	Padlockable swing handle - UNSW Switchboard Cabinets	Orange Switchboards IP65, 316 Stainless 13mm padlock shackle	

D&D LOKKBOLT	LB118BX-LA	Lockable bolt for secondary doors on external gates.		
		NOTE: Must be this model, as other models cannot be rekeyed onto UNSW cylinders.		
The Cyber Lock Key System is specified to be installed on all new desk and pedestal systems. UNSW Locksmiths cannot guarantee keys or service for any other systems. Master keys are only provided to Security for emergencies, as too many would compromise security. If you have trouble obtaining these locks, consult UNSW Locksmiths. All locks use a Cyber Lock key, and additional keys can be requested via Archibus using the numbers on the lock/key.				
Cyber Lock	A-601	CL Square back drawer lock.	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	A-602 A-603-SF A-603	CL Multi Drawer lock CL Multi Drawer lock - single flange CL Multi Drawer lock - double flange	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	A-604	CL Push lock	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	A-605	CL Tambour lock	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	A-201	CL Filing Cabinet lock	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	A-629	CL Slam lock	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	A-621	CL Showcase lock	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	552R / 553R	CL Flush Handle lock	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	A-607	CL Cam lock	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	
Cyber Lock	CL856	CL Combination locker lock.	Cabinets/Drawers/ Lockers/Pedastals/ Cupboards	

****for Lockers, preference is to install access control – Gallagher. Otherwise mechanical locks as per the above (pin codes not recommended. Nor will they be supported/maintained by the UNSW Locksmith)**

12.8. Rooms controlled by access control

Any door that has access control installed is to be keyed to the Security Master key system; this key system is restricted to security personnel only. For rooms that have multiple doors and access control installed on a single door, each door to that access-controlled room must be keyed to the Security Master key system.

Additionally, any access-controlled door that incorporates a fixed leaf, secured by a drop bolt or similar device, adjacent to an active swing leaf shall have the fixed leaf secured and keyed to the UNSW restricted key system. The restricted key and associated lock barrel shall be supplied and installed by the UNSW Locksmith. Refer to Section 12.1: Mechanical Locks.

The drop bolt shall be installed on the inside/secure side of the room, opposite the side on which the access control card reader is installed, so that it cannot be accessed or operated from the entry side of the door.

The drop bolt shall be of an extended-length type, suitable for the door construction and installation. The installation and fixing method shall ensure that through-fixings, screws and associated hardware do not interfere with, penetrate, compress or otherwise compromise the smoke seals located at the bottom of the door.

Any service door (not limited to), Plant Room, access to a roof space, Cleaners room. IT Communications room are all to be access controlled.

12.9. Keys

For any project that has a new door – whether it be a small refurbishment or a new building, Security Systems are to be notified in order to rekey the affected doors.

For Large projects – new buildings/refurbished buildings. Up to 12 weeks is required for locks to be changed – this period includes the Locksmith to survey the area, liaise with the occupants in regard to key requirements, build and configure the new key master system, building of barrels, cutting of keys, handing out new keys to building occupants and changing of lock barrels to new master key system.

For smaller refurbs – up to 50 locks. 8 weeks is required for locks to be changed – this period includes the Locksmith to survey the area, Liaise with the occupants in regard to key requirements, build and configure key master system, building of barrels, cutting of keys, handing out new keys to building occupants and changing of lock barrels to new/extension of existing master key system.

Failure to provide sufficient notice will result in delays.

Appendix A: Example of a Gallagher Equipment Programming Commissioning Sheet

INSPECTION AND TEST CHECKLIST FOR: GALLAGHER CONTROLLER COMMISSIONING		
Controller Name		Controller C7000 Controller
Controller Location		
IP Address		
MAC Address		
GPO Details		
Network Port Details		

H-BUS Expansion - Bus 1				Testing			Comment
Serial No	Type	Unit Name	Location	Date Tested	Online	Tamper	

H-BUS Module							
Serial No		Final Name (as per UNSW)	Terminated Date	Initials	Test Date	Initials	Comments
	<i>Reader 1</i>						
	<i>Reader 2</i>						
	<i>Reader 3</i>						
	<i>Reader 4</i>						
	<i>Reader 5</i>						

	Reader 6					
	Reader 7					
	Reader 8					
Inputs	Input 1					
	Input 2					
	Input 3					
	Input 4					
	Input 5					
	Input 6					
	Input 7					
	Input 8					
	Input 9					
	Input 10					
	Input 11					
	Input 12					
	Input 13					
	Input 14					
	Input 15					
	Input 16					
	Input 17					
	Input 18					
	Input 19					
	Input 20					
	Input 21					
	Input 22					
	Input 23					
	Input 24					
Outputs	Output 1					
	Output 2					
	Output 3					
	Output 4					
	Output 5					

	Output 6						
	Output 7						
	Output 8						

Final Acceptance		
		APPROVED (YES/NO)
COMMISSIONING TECHNICIAN		
UNSW REPRESENTATIVE		

Appendix B: Example of a Gallagher Equipment Programming Commissioning Sheet

UNSW Power Supply Commissioning			
Controller Details			
Controller Type		8H Module	Yes/No
Network port Details		MAC Address	
IP Address		Location	
Number of doors connected			
Power Supply Details			
Power Supply Quantity			
Volts (Loaded)		Volts (unloaded)	
Battery Details			
Battery Date		Battery Size	
Alarms			
AC Fail	Yes/No	Battery Low	Yes/No
Installation Details			
Installation company		Technician	
Date of test		Technician Signature	
UNSW Contact (PM)		Signature	
Units supplied from this Power Supply:			
Comments			

Appendix C: Equipment List

Brand/Supplier	Part Number	Description	Notes
Gallagher	C400101	Controller 7000 Enhanced Controller	
Gallagher	C300182	8 H Module	
Gallagher	C300470	Gallagher FT T15 Multitech Reader	Black
Gallagher	C300460	Gallagher FT T20 Multitech Reader	Black
Gallagher	C200100	Gallagher Single Cabinet	
Gallagher	C200105	Dual Cabinet 8A PS	
Gallagher	C200440	Power Supply	8A
Gallagher	C300688	HBUS 16 I/O	
Gallagher	C300684	HBUS 8/4 I/O	
Gallagher	C300680	HBUS 8 Input	
Gallagher	C300660	HBUS 8 In 2 Out Door Module	URI
Sprint	D115G	Break glass unit	Green in colour
Powerbox	PBB2S137	Powerbox 13.8VDC 7Amp Power Supply with Battery Charging, AC Fail and Low Battery Monitoring	
Powerbox	PBB2SWMB	Powerbox Wall Mounted Enclosure - WMBB-C-S-D	
Axis Intercom	I8016-LVE	(for Help Point)	Housing to be supplied by Cunneen Signs through UNSW
SMART	1001 (SD/001)	Fixed Duress button	Desk mounted/Wall mounted *Duress buttons to include White Trifoliate labels 'Emergency Duress'
SMART	XALK01/ZB5AS844/ZENL1121	Fixed Duress (Part No includes Pushbutton (yellow, Mushroom (Red) and Mount)	Waterproof for wet areas
Inovonics	EN42X	Wireless Duress	Monitoring individual duress zones and Battery Low alarm of receiver
Lockwood	3570ELM0SC	Mortice	For wooden doors
Lockwood	6782ELSS	Mortice (extended backset)	For Aluminum doors
Lockwood	3782ELSS	Mortice	For Aluminum doors
Lockwood	LC8810	Transfer Hinge	
Lockwood	LC8810	Transfer hinge (lead cover)	
Lockwood	LC881	Transfer hinge (lead cover)	
Lockwood	1801 Plate/70 Lever /SC	Entry Hardware	Key Override
Lockwood	1820 Plate/70 Lever/SC	Entry Hardware	Key override + LED
Lockwood	1905 Plate/70 Lever/SC		Internal Plate
Lockwood	20020NA Plate/96 Lever/SS	Entry Hardware	Left-Handed Key override + LED
Lockwood	20020NA Plate/96 Lever/SS	Entry Hardware	Right-Handed Key override + LED
Lockwood	20105NN Plate/96 Lever/SS	Entry Hardware	Internal left-handed
Lockwood	20105NN plate/96 lever/SS	Entry Hardware	Internal Right-handed
Lockwood	4811/70SC	Door Handle	
Padde	EMZ8SM	Maglock	External single doors
Padde	EMZ8DM	Maglock	External double doors
Padde	EMZ4SM	Maglock	Internal single doors
Padde	EMZ4DM	Maglock	Internal double doors
Padde	ES9000	Strike	*Must seek approval prior to install
Sentrol	1078C	Reed Switch	
Sprint	SPRL3761	Touchless Exit Button	
Paradox	525D/DG466	PIR	360 degree
Axis	P3285-LV	CCTV Camera	Indoor Dome
Axis	P3285-LVE	CCTV Camera	External Dome
Axis	5676-E MK II.	CCTV Camera	PTZ
Axis	P3735-PLE	CCTV Camera	Multidirectional Camera
Axis	Q6300-E, Q6125-LE	CCTV Camera	Multidirectional Camera to be used with PTZ
Axis	Q6135-LE	CCTV Camera	PTZ for Multidirectional Camera
Axis	M3086-V	CCTV Camera	Dome camera for lift cars
Axis	P4705-PLVE 2 MP/P4707-PLVE 5MP	CCTV Camera	Multi Head Dual Camera