University of Otago

Building Technologies – Standards Suite

CHAPTER 5: ELECTRONIC SAFETY & SECURITY (ESS) SYSTEMS STANDARD

DOCUMENT CONTROL

1) Document Identification

File Name	UoO_BTSS_ CHAPTER 5: ELECTRONIC SAFETY & SECURITY (ESS) SYSTEMS STANDARD
Version	4.1
Document Owner	IT INFRASTRUCTURE TEAM

2) Preparation

Action	Name	Role / Function	Date
Prepared by:	Phil Earl, Cas Olckers	Torque IP	2021-Jun-11
Reviewed by:	Mike Stacey, Douglas Harre	Torque IP	2021-Aug-05
Prepared by:	Cas Olckers	Torque IP	2021-Nov-19

3) Release

Version	Date Released	Change Notice	Remarks
1.0	11 June 2021	New document written; Standards broken down into 7 chapters making up a new UoO Building Technologies – Standards Suite of documents. This document is Chapter 1 of 7	Draft For client review and benchmark for final issue
2.0	19 November 2021	Notes applied in relation to workshop held on 14 October 2021	Draft For client review and benchmark for final issue
3.0	18 February 2022	Input from property team	Draft For client review and benchmark for final issue
4.0	4 March 2022	Issue for Implementation	

Version	Date Released	Change Notice	Remarks
4.1	21 March 2022	Add reference to the Labelling Standard Chapter (Chapter 8)	For Release

4) Contribution (C) and Distribution (D) List

Name	C/D	Organisation	Title
Wallace Chase	D	University of Otago	Head of IT Infrastructure
Young Cho	C	University of Otago	Manager Network Services
Mike Harte	D	University of Otago	Director of ITS
Tanya Syddall	D	University of Otago	Director Campus Development
Dean Macaulay	D	University of Otago	Director Capital Development
Stephen Duncan	C	University of Otago	Network Solutions Architect
Rob Wilks	C	University of Otago	Building Information and Compliance Manager
Michael Porter	D	University of Otago	Property Services Facilities Manager
Shane Montague-Gallagher	C/D	University of Otago	Security Systems Coordinator
Geoff Burns	C/D	University of Otago	Deputy Proctor
Paul McNamara	C/D	University of Otago	Emergency Management and Business Continuity Coordinator

BUILDING TECHNOLOGIES STANDARDS SUITE INDEX

This document is only one chapter of the University of Otago Building Technologies Standards Suite.

The Building Technologies Standards Suite consists of the following chapters (chapter highlighted refers this document):

Acknowledgements

The University of Otago, New Zealand, acknowledges with thanks the assistance and contribution of a number of organisations, institutions, statutory bodies, and individuals in the preparation of these Standards. In particular, the assistance of the following parties is acknowledged:

Torque IP and University of Otago IT Staff

CONTENTS

1. DOCUMENT PURPOSE

This document is CHAPTER 5: ELECTRONIC SAFETY & SECURITY (ESS) SYSTEMS STANDARD and forms part of the University of Otago Building technologies Standards Suite.

Its purpose is to provide design consultants and contracts the guidance that shall be followed when either designing, installing, maintaining, or performing changes to a University of Otago Access Control, Duress, and Intercom systems.

1.1. Document sponsor

This document has been developed and is controlled by the University of Otago (hereafter referred to as UoO).

The contractor or designer shall adhere to the latest published edition of all standards and technical documents for all responses and construction work. Should a conflict exist between the standards or any scope of work, the contractor shall notify the consultant or University of Otago Proctor's Office of any conflict and seek clarification prior to continuation.

All queries, errors, omissions, or suggestions related to this document are to be directed to:

The Proctor's Office

University of Otago

PO Box 56
Dunedin 9054
New Zealand

Email: deputy.proctor@otago.ac.nz.

1.2. Outcome statement

By using this document and relative standards, designers and contractors will meet the University of Otago's standards for the safety, design, installation, and support of Electronic Safety & Security systems environments that the University manages and operates.

1.3. Chapters

The Building Technologies Standards Suite covers the following Information and Communication Systems. Each system is presented as a separate chapter:

- Chapter 1 – Introduction to Building Technologies Standards Suite
- Chapter 2 - Cabling Infrastructure Pathways Standard

- Chapter 3 - IT Infrastructure – Generic Cabling Systems Standard
- Chapter 4 - IT Infrastructure – Passive Optical LAN Cabling Standard
- Chapter 5 - Electronic Safety and Security (ESS) Systems Standard
- Chapter 6 - Closed Circuit Television (CCTV) System Standard
- Chapter 7 - Audio Visual (AV) Cabling Standard
- Chapter 8 – Labelling Standard

2. USING THIS DOCUMENT

This document shall be read in conjunction with all other Chapters in the BUILDING TECHNOLOGIES STANDARDS SUITE that carry other relevant information regarding the installation of ESS systems, including but not limited to Pathways, Equipment rooms, Cabinets, GCS, POL, AV, CCTV, and documentation requirements.

The design consultant, contractor and University staff shall refer to CHAPTER 1: INTRODUCTION TO BUILDING TECHNOLOGY STANDARDS for an overview of the standards suite requirements.

3. REFERENCED DOCUMENTS

3.1. UoO REFERENCE DOCUMENTS

The following documents to be referred to:

- Installation Specification for Gallagher Access Control System at University of Otago (Rev v01 dated February 2016)
- Closed Circuit Television (CCTV) Security Systems Policy (https://www.otago.ac.nz/administration/policies/otago676292.html)

3.2. STANDARDS

Installation of the Electronic Safety & Security systems shall be carried out in compliance with the relevant standards detailed below.

Should a conflict exist between respective above-mentioned standards and/or with specifications documents, the order above shall dictate the order of precedence in resolving conflicts. This order of precedence shall be maintained unless a lesser order document has been adopted as code by a local or central government entity or as determined by University of Otago.

All the above-mentioned documents listed are believed to be the most current releases of the documents, however it is the responsibility of the contractor to determine and adhere to the most current versions of related standards at the time of installation.

3.2.1. New Zealand Standards

Standard	Standard Description
AS/NZS 2201.1:2007	Intruder alarm systems – Client's premises – Design, installation, commissioning, and maintenance
AS/NZS 2201.5:2008	Intruder alarm systems – Alarm transmission systems
NZS 4301.3:1993	Intruder alarm systems – Detection devices for internal use
NZS/AS 2201.2:1992	Intruder alarm systems – Central stations
NZS/AS 2201.4:1990	Intruder alarm systems – Wire-free systems installed in client's premises

Standard	Standard Description
Ministry of Justice	Private Security Personnel and Private Investigators Act 2010
NZS 4512:2021	Fire detection and alarm systems in buildings
NZS 4514:2009	Interconnected smoke alarms for houses
AS/NZS 3000:2007	Electrical Wiring Rules
AS/NZS 3604:2011	Timber-framed buildings
NZS 4219:2009	Seismic Performance of Engineering Systems in Buildings

3.2.2. UoO's Service Provider Standards

Standard	Standard Description
Confidential February 2016 (Revision v01)	Installation Specification for Gallagher Access Control System at University of Otago

Should a conflict exist between respective above-mentioned standards and/or with specifications documents, the order above shall dictate the order of precedence in resolving conflicts. This order of precedence shall be maintained unless a lesser order document has been adopted as code by a local or central government entity or as determined by University of Otago.

All the above-mentioned documents listed are believed to be the most current releases of the documents, however it is the responsibility of the contractor to determine and adhere to the most current versions of related standards at the time of installation.

3.3. WEBSITES

http://www.legislation.govt.nz/

http://www.otago.ac.nz

http://www.telepermit.co.nz/PtcSpecs.html

3.4. LATEST REVISIONS

The users of this document shall ensure that their copies of the above-mentioned New Zealand Standards and the New Zealand Building Code are the latest revisions. Amendments to referenced New Zealand and Joint Australian/New Zealand Standards can be found on http://www.standards.co.nz.

4. DEFINITIONS AND ABBREVIATIONS

For the purposes of this document the following definitions and abbreviations shall apply.

4.1. Definitions and Abbreviations

Term	Definition
Application Specific Cabling	System manufacturers design
As built	Final set of drawings produced at the completion of a construction project, including all changes made to the original construction drawings
ACID	Access Control and Intruder Detection Systems
ACS	Access Control System
BMS	Building Management Systems
Building backbone cabling	Cable that connects the building distributor to a floor distributor
Campus	An area or site which contains several University buildings, and includes the grounds in which a cabling system is installed
Campus backbone cabling	Cable that connects the campus distributor to the building distributor(s)
Campus distributor	Distributor from which the campus backbone cabling starts
Category 5 (Cat 5)	For the purposes of this document, cabling components which provide a permanent link that, when tested, do not meet AS/NZS 11801-1 Class D performance
Category 5e (Cat 5e)	For the purposes of this document, cabling components which provide a permanent link that, when tested, meet AS/NZS 3080 [AS/NZS 11801-1] Class D performance
Category 6 (Cat 6)	A definition of cabling components which provide a permanent link that, when tested, meet AS/NZS 11801-1 Class E performance

Term	Definition
Category 6A (Cat 6A)	A definition of cabling components which provide a permanent link that, when tested, meet AS/NZS 11801-1 Class E_A performance
Catenary wire	A wire supported at two points kept under mechanical tension to provide a support to which cabling may be fastened.
CCTV	Close Circuit TV system
Channel	End to end transmission path connecting two pieces of application specific equipment (includes patch cords and work areas cables)
Clear working spaces	A ventilated working space allowing quick unrestricted egress or escape in the event of emergency
Consolidation Point	Connection point in the horizontal cabling subsystem between a floor distributor and a telecommunications outlet
Contractor	Where the term "Contractor" is used within this document it shall be interpreted as the "Communications Contractor".
Deputy Proctor	A person also acting at UoO security manager.
Designer	A person who plans the look, or workings, or both, of something prior to it being made, by preparing drawings or plans
Distributor	The term used for a collection of components (such as patch panels, patch cords) used to connect cables
Distributed Intelligence	This is when the security control panel will be able to still operate when disconnected for the rest of the ESS LAN (Local Area Network)
EDR	Emergency Door Release Unit
Enclosure	A housing for accommodation of equipment and cabling that includes mounting rails and protective panels
EPS	Emergency Phone Stations – External and internal stations used by staff, students, contractors, or visitors to escalate a security duress or panic situation to Campus Watch

Term	Definition
Equipment footprints	The vertical and horizontal planes occupied by a piece of equipment in normal operation
ESMS	Electronic Security Management System (Gallagher System)
ESS	Electronic Safety & Security Systems
Generic cabling system (GCS)	Structured telecommunications cabling system, capable of supporting a wide range of standardised applications. Standards based design
HBUS	Provides an interface between the Security Control Panels and field devices i.e., card readers, panic system inputs, BMS inputs, outlets to electronic locks, strobe lights etc.
Horizontal cabling	Cable connecting the floor distributor to the terminal equipment outlets
IDS	Intruder Detection Systems
Installer	A person that places or fixes equipment or machinery in position ready for use. The party(s) responsible for the supply, installation, testing and warranty of cabling systems
Integrator	A person that places or fixes active IT equipment e.g., network switching, Wireless Access Points, servers, desktop computers etc. in position and configures, programs them ready for use. The party(s) responsible for the supply, installation, testing and warranty of active equipment systems
INTS	Intercom Systems
Manufacturer	A person or company that makes cabling goods for sale
NVR	Network Video Recorder
Power over Ethernet	Power over Ethernet (PoE) is a technology for wired Ethernet local area networks (LANs) that allows the electrical current necessary for the operation of each device to be carried by the generic cabling system rather than by power cords. Typical uses include VoIP phones, WAPs, IP CCTV cameras, or lighting.

Term	Definition
Power Over SCS or GCS cabling	Power over structured telecommunications cabling (application specific cabling) or power over generic cabling (non-application specific cabling)
Permanent link	Transmission path between the telecommunications outlet and the floor distributor
Proctor's Office	The UoO security office is being managed by the Proctor's office. The security office is also known as the Campus Watch.
RAS	Refuge Area Stations
SCP	Security control panel which is part of the ACID system
Service Distributor (SD)	Equivalent to distributor 1 in ISO/IEC 11801-1
Service Outlet (SO)	Equivalent to a TE Outlet in ISO/IEC 11801-1
Single vendor system	A system provided by a single vendor to help reduce operational, configuration, and management complexity
Site	See **Campus**
Structured Cabling System	Specific cabling solution designed with a set of cabling and connectivity products that are constructed (engineered) according to standardised rules to facilitate specific connectivity requirements e.g., Nurse Call (Staff Assist). Legacy design.
Suitably qualified person	A person with the professional qualifications and experience in the industry to undertake the design and supervision of the works
Terminal Equipment Outlet (TEO)	Fixed connecting device which provides and interface to the terminal equipment. N.B. The term telecommunications outlet is used in some other parts of the ISO/IEC 11801 series, while the term terminal equipment outlet is used within AS/NZS 11801-1 and this document.
UoO	University of Otago
URI	Universal Reader Interface

Term	Definition
Velcro™	A proprietary form of Hook & Loop fastener/cable tie
VMS	Video Management System

5. ESS: OVERVIEW

5.1. Purpose of this standard

The purpose of the standard is to guide the following stakeholders in terms of ESS (Electronic Safety and Security) systems designs, installation, maintenance, and upgrades:

- ESS Design consultants
- ESS Project Managers
- Architects
- UoO Project Team
- UoO Proctor's office
- UoO Facilities management
- UoO ITS team

It is still important that this document shall be read in relation to related industry standards, manufacturer warranty requirements and industry best practice.

5.2. Electronic Safety & Security (ESS) Systems

University of Otago has main campuses located in Dunedin, Christchurch, and Wellington. Rest of the UoO sites are considered remote sites located in various parts of New Zealand.

The Electronic Security System (ESS) forms an integral part of the overall staff, student, and asset safety management system.

The ESS comprises of:

- Access Control and Intruder Detection systems (ACID): Gallagher system and other
- Monitoring / Integration of 3rd party systems:
    - Panic/Duress Systems: Refuge Area Stations (Talk-A-Phone)
    - PA and Intercom systems: Informacast
    - Building Management System (BMS)
    - Lift phones and fire alarms

5.2.1. ESS requirements

The following is high level requirements in terms of the ESS:

- All ESS head end also needs to be connected to the applicable building or communications rack UPS network
- UPS network to allow for a 2-hour battery backup power supply.
- All ESS requires Building Consent through UoO and the applicable local City Council.

5.2.2. ACID system overview and requirements

The Access Control System consists out of:

- 2No virtual servers located in the Dunedin campus Data Centre which is for backup purposes
- Gallagher Security Management System at the Campus Watch Control Room
- Dual technology card readers
- 162 controllers and associated door licences - Currently deployed
- V8.2 firmware version
- The Dunedin campus has a centralised control room monitoring ACID alarms. Remote sites are integrated into the main building ACID systems
- The Gallagher system is also connected to:
    - Hazardous alarms are connected into the Gallagher
    - Panic alarms and Refuge Area Stations (RAS)
    - Avigilon CCTV
    - Staff assist call buttons inside toilets.
    - Fire Alarm Systems
    - Super Low Freezer Alarms
- Doors are to be fitted with maglocks. Other types of locks can only be fitted with the explicit approval of the Deputy Proctor.

The following is current issues and future requirements:

- Controllers inside cabinets – Inconsistency in controller installation, locations, and positioning

- Need to define the placement of the controllers within telecommunication spaces or risers
- Gallagher 6000 series controllers to replace all existing older controllers by end of 2021
- The monitoring of fridges and remote sites potentially needs to be phased out over time, but remain at this stage till further notice from UoO
- Duress systems needs to be scenario specific i.e., after hours and during calls hours alarms escalation to be escalated accordingly etc.

Older version Gallagher (Cardax) card reader and keypad unit:

Newer version Gallagher card reader and keypad unit (T20):

- All new teaching spaces, or any teaching spaces undergoing a refit/refurb, MUST have Gallagher access control fitted. The reason for this is to enable electronic booking systems to maximise the use of spaces without the need for staff to lock/unlock doors etc. especially after hours.
- The naming convention for Gallagher equipment. UoO had repeated issues with the names in the Gallagher system not corresponding to the naming convention of the building – they are supposed to be the same (with a v minor variance which we all know about)

5.2.3. Monitoring and integration of and to 3rd party systems

5.2.3.1. Panic/Duress and Life Safety Emergency systems overview and requirements

The Panic/Duress System consists out of:

- Refuge Area Stations (RAS) deployed throughout the campus
- Emergency Phone Stations (EPS) deployed throughout the campus
- The following schedule provides a summary of Refuge Area Station (RAS) AND Emergency Phone Stations (EPS) types, quantities, and links to further technical information:

Item	Device Name	Device Description
1	Emergency Phone Stations (EPS) - TalkAPhone WEBS-MT/R (Towers)	Towers / Wall mount devices have an emergency button, pressing these contacts a pre-programmed number http://talkaphone.com/products/webs-mtr/ • Intercom buttons have dedicated copper for PBX connectivity These devices are connected to Informacast, that platform is used to send broadcast messages to these
2	Emergency Phone Stations (EPS) - TalkAPhone ETP-WM (Wall mount Stations)	Towers / Wall mount devices have an emergency button, pressing these contacts a pre-programmed number: https://talkaphone.com/products/etp-wm/ • Intercom buttons have dedicated copper for PBX connectivity These devices are connected to Informacast, that platform is used to send broadcast messages to these

Item	Device Name	Device Description
3	Emergency Phone Stations (EPS) - TalkAPhone WEBS-PA-1 (Broadcast Speakers)	Indoor paging units: https://talkaphone.com/products/webs-pa-1/ These devices are connected to Informacast, that platform is used to send broadcast messages to these
4	2Talk SIP	Haywards Hall for connecting to their PA system • These were purchased as part of a building project - this was due to there being no standard for devices to be used for broadcast speakers This gateway provides a connection to Informacast so that it can send a broadcast message to PA speakers that are installed in that hall
5	Refuge Area Stations (RAS) - TalkAPhone VoIP 600 (Safe Refuge)	Safe Refuge Emergency phones were installed starting with G401 Mellor Labs, F614 Commerce Building and H402 St Davids II from 2017 onwards: https://talkaphone.com/products/voip-600/ • These use SIP to connect to Cisco Call manager and use SIP to make outbound calls via a pre-programmed number. While these are branded as TalkAPhone devices, these are not connected to Informacast and instead are essentially "telephones" Safe Refuge Phone Configuration (TalkAPhone VoIP 600)
6	Valcom Model VIP-120A-IC	Valcom's Round Ceiling Speaker. Vendor's website works intermittently at: https://valcom.com/Products/speaker_ts/ceilspkrs.htm
7	Valcom Model VOP-410A-IC	Valcom's Metal Wall speaker. Vendor's website works intermittently at: https://valcom.com/Products/speaker_ts/metalwall.htm

UoO currently has 2 previous Refuge Area Stations and Emergency Phone Station models in use, which is not connected to the newer Informacast system. They are connected to Webscontact system from TalkAPhone:

- Viacom
- 2Talk units

The above-mentioned system is in use till gradually migrated to the Informacast.

The following is current issues and future requirements:

- The Refuge Area Station and Emergency Phone Stations buttons are connected to the ACID monitoring and the CCTV system but not working. This needs to be rectified.

The Emergency Phone System activations will then prompt instances (different types of notifications) to be escalated the various Membership Groups (Students, staff, contractors etc.), as per the Notification Groups, via the Informacast Fusion network.

The emergency notifications are controlled by the Emergency Management and Business Continuity Coordinator and documented in the Emergency Event Notification Procedure.

5.2.3.2. PA and intercom systems overview and requirements

The PA System consists out of:

- 95 internal speakers driven by the Informacast Fusion system
- The colleges have an Informacast connected speaker inside their foyers only with the rest of the college speakers connected to a 3rd party system (Velcom)
- The internal intercoms are Aiphone (various models) video intercoms and connected to a standalone base station, in the applicable building where the door (gate station(s)) is/are located

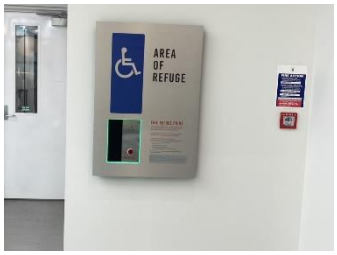
The following is current issues and future requirements:

- Speakers are not installed as communicated (Campus Development)
- Intercom needs to be addressed as part of new built or renovation projects
- New intercoms need to be driven by Informacast
- Speakers need to be multi-purpose
- Volume needs to be centrally managed.

External Emergency Phone Station / Emergency Phone: Example 1:

Internal/External Emergency Phone Station: Example 1:

Internal Refuge Area Station: Example 1:



5.2.3.3. BMS systems overview and requirements

The BMS system consists out of:

- BMS server is hosted on a VM in the UoO data centres
- The BMS software is called Desigo CC
- The BMS provides inputs to the Gallagher system via clean contacts.

The following is current issues and future requirements:

- The BMS system needs to be monitored by the Gallagher system. The interface will be from BMS controller to the nearest Gallagher Access Control and Intruder Detection systems control panel.

5.2.3.4. Room booking systems overview and requirements

The room booking systems to meeting rooms and lecture theatres are all managed through a separate room booking system, managed by the UoO AV team. This room booking system is required to interface with the Gallagher system to allow for lecture theatres and meeting rooms (which might have access-controlled doors) doors to:

- unlock automatically when booked
- lock when no movement is detected, and the booking session timeframe has been completed

6. DESIGN, INSTALLATION AND MAINTENANCE CRITERIA

6.1. Criteria for use

The designer and contractor shall refer to sources and publications outlined at the beginning of this document for general design, installation, and maintenance guidance.

6.2. ESS Exclusions

Refer to the Design and Coordination section for exclusions.

Related ESS systems that are outside the scope of these standards include:

a) Network equipment, such as servers and switches that are connected to the Campus Watch
b) Wireless LAN equipment
c) Radio based carrier interface
d) Generic Cabling Systems (cabling associated to ethernet connections and associated hardware (patch panels, cabinets etc.)

6.3. Existing ESS

ESS that has been provided in accordance with earlier standards will be retained in service unless there is sufficient justification for replacement of the ESS as part of an upgrade or redevelopment, or if the ESS performance is inadequate.

Any existing ESS that is deemed to be retained by the University or project manager shall be tested to the appropriate performance specification. If the link fails, it shall be either:

a) Replaced
b) Brought up to this specification
c) Removed from service if no longer required

6.4. New ESS systems

The following schedule provides a summary of the various new ACID components deployed at UoO:

Component	Location	Make	Model	Use
Virtual Server	UoO Campus Data Centre	VMWare (version 2016)		Hosting the ESMS (Electronic Security Management System) Based at 444 and 325 CD Failover clustering Downtime only 2 minutes

Electronic Security Management System (ESMS)	Campus Watch Control Room	Gallagher Commend Centre	FT (8.2). – Updates required annually	The standard features available with the Commend Centre: *https://products.security.gallagher.com/security/nz/en_NZ/products/software/command-centre/p/C201311* The following additional features are required through the Command centre: • VMS integrations • REST APIs and other tools for integration into other systems • Visitor Management • Elevator integrations • Key cabinet integrations • Third party readers including biometric • Locker Management • Car Park Management • Tag boards • Intercom integrations • Additional licenses (e.g., door, fence, carpark, competencies, workstations etc) • Additional credentials The ESMS is also responsible for

Component	Location	Make	Model	Use
				monitoring alarms at all UoO campuses nationally.
Cabinets	ICT rooms and ICT risers	Gallagher	Dual Cabinet 8A PS	Hosting SCP's, HBUS modules
Security Control Panels	ICT rooms and riser locations	Gallagher	C6000 series controllers	Interface between the ESMS and field devices i.e., card readers, panic system inputs, BMS inputs, outlets to electronic locks, strobe lights etc.
HBUS Modules	ICT rooms and riser locations	Gallagher	4H and 8H	Provides an interface between the C6000 controllers and field devices i.e., card readers, panic system inputs, BMS inputs, outlets to electronic locks, strobe lights etc.

Component	Location	Make	Model	Use
Car Readers	Card readers are deployed the following access-controlled door locations: • ICT rooms • Buildings ground level perimeter entrances • Between reception and staff only spaces • Labs – Computer and Science (PC1 And PC2 labs) • Lifts • Timetable Spaces – Lecture Theatres • Accommodation Buildings (including restricted spaces)	Gallagher	• T15 Multi Tech • T11 Multi Tech • T20 Multi Tech • T30 Multi Tech • Gallagher Mobile Readers i.e., Health Sciences	• T15 Multi Tech – Internal staff only area doors, and lifts • T11 Multi Tech – Internal student area doors, Perimeter pedestrian and vehicle gates • T20 Multi Tech Terminal – Main building entry doors, Services deliver doors, ICT Rooms • Eccles Bldg – Use Mifare Readers – Only exception • Use mobile function via 802.15
Door locks	Electronic locks are deployed the following access-controlled door locations: • ICT rooms • Buildings ground level perimeter entrances • Between reception and staff only spaces • Labs	• Assa Abloy / Lockwood • Abloy / Lockwood • Assa Abloy / Lockwood • Assa Abloy / Lockwood • Assa Abloy / Lockwood	• 3570 • 3582 • Z4 • Z2 • Z8	• for standard size doors (or equivalent • for narrow back applications (or equivalent). • for standard size doors (or equivalent) • for narrow frame applications (or equivalent) • for over standard size doors (or equivalent)

7. SYSTEM REQUIREMENTS

7.1. General

Product specifications, general design considerations, and installation requirements are provided in this written document. Any quantities, cable routes, locations, types, and installation details for the specific project, shall be detailed on associated services layouts, design specifications and project specific scope of works documents.

The access control system (ACS) shall generally include but not be limited to the following equipment:

- ESMS - Electronic Security Management Software.
- Controllers (Main Controller and/or Field Controller and I/O expanders).
- Card Readers.
- Request to exit buttons.
- Emergency Door Release (EDR).
- Electronic locking hardware.
- Cabinets, cabling, power supplies and batteries (as defined in the electronic system section).
- Credentials (access cards or key fobs); and
- Intercoms.

The contractor shall design, furnish, and install all equipment, accessories and material required for a complete turnkey solution.

7.2. System functionality – Access Control System (ACS)

All security access-controlled doors will be provided with an appropriate lock. An Emergency Door Release (EDR) unit shall be provided at all doors where the locking hardware is not capable of this.

The ACID shall connect to the fire alarm panel. As such, during a fire alarm condition the ACID, in conjunction with the fire alarm system interface, shall release the security on doors as noted on any services layouts. The security contractor to refer to the Fire safety/evacuation engineer's report for detail and to include the detail in security as built documentation.

All door entry and exit methods shall be recorded in the system event database. The door shall be monitored for both door open/closed, and door unlocked/locked using concealed monitor switches appropriate for the door installation. Door position switches shall be installed in the door jamb separated from the lock. Should a door be left unlocked or open after a pre-set time, an alarm shall be generated reporting the condition. The door open/unlocked warnings shall provide an audible warning at the door.

Should a valid request to access a door be generated and access not taken, it shall be possible to ignore the request (not record it as an event) and automatically re-secure the door after a pre-set time. When a valid access through a door is undertaken, the door shall immediately re-secure on closing.

Any delayed unlocking shall adhere to the following requirements:

- Must be approved under the building consent process and included into the fire safety summary in the design document
- Delay must be >15 seconds
- Fire relay must take precedence over the timer delay relay mechanism
- Must include signage to indicate it is a delayed opening door/gate

7.3. System functionality – Intruder Detection Systems (IDS)

The Intruder Detection Alarm System's main function is to detect any unauthorised movement in selected areas. Motion detection is achieved by directional and 360 degrees dual technology Passive Infrared and Microwave combination detectors. Glass break detectors are also required in the areas covered by intruder detection motion detectors, but only in the ground areas or areas easily reachable from the ground level.

The Intruder Detection devices are connected directly to the Electronic Access Control System to allow for a combines Access Control and Intruder Detection system.

The following alarms to be escalated via the ACID, to authorised UoO personnel for appropriate levels of escalation and reaction:

- Any unauthorized movement detection
- Door forced open
- Door propped open
- Authorised access card/pin holders accessing areas during unauthorized times

The SMS (Security Management Software) and server is located within the 444 and 325.

The following is achieved by the front-end user terminals inside the security control room:

- Reporting
- Access card management
- Intruder alarm system alarm management
- Intruder alarm pin management.

7.4. Electronic Security Management System

At minimum the SMS shall provide a single overarching platform for the programming, administration, control and monitoring of the access control and the intrusion detection system. The SMS shall also provide a single integrated platform to any other security sub-systems.

The SMS shall support full deployment over virtual computer platforms, cloud computing environments and clustered server implementations, deployed throughout UoO.

The SMS shall be implemented and connected to the UoO ACID (Access Control and Intruder Detection) server architecture. The SMS shall support multiple concurrent UoO network connections from different workstations or operators.

The SMS shall be scalable to support the UoO sites, from small (requiring only 1 controller) to large (requiring 100+ controllers).

The SMS shall be capable of a similar scale for users (1 – 100,000+). Full capacity details shall be detail inside the tender response.

7.4.1. Distributed Intelligence

If the SMS is not running for whatever reason, the field hardware shall continue to function at full capacity, including authentication of all users. No alarms, tamper events or security logging information will be discarded, unless the field hardware buffer becomes exhausted.

Each controller shall be capable of storing up to 100,000 user records, along with all necessary lists to be able to apply permissions and qualifying considerations in real time, even if the SMS is offline or non-operational.

In the case that a controller goes offline, the SMS shall notify the UoO security control room operator, of the incident but then suffer no system-wide drop in overall performance, other than an inability to control or monitor the entities stored on or connected to the specific offline controller.

7.4.2. Integration & Support of Other Applications

The SMS application shall allow integration to a variety of proprietary and third-party systems and applications such:

- Intruder detection systems.
- Access control systems.
- CCTV video surveillance systems.
- Intercom systems.
- Duress systems; and
- Building management systems.

The ESMS application shall act as a central hub for the coordination of activities and events within and between any disparate systems at the UoO Main Security Control room. The ESMS application shall provide a single point of operation for the most typical types of control and monitoring security activities on site.

7.4.3. User Management

The ESMS application shall store information about users of the electronic security system. A user is defined as a person with either card access or PIN access at a card reader or system keypad.

The ESMS shall regard a cardholder/user as a global entity which spans all controllers. Under no circumstances should a single cardholder need to be individually programmed into separate controllers. The ESMS shall automatically and seamlessly send the cardholder programming details to all controllers without operator intervention.

The ESMS shall update in real-time the location of cardholders as they access different areas. It shall be possible to type in the name of the area to filter the list of users in that area.

7.4.4. Remote Monitoring

The contractor shall set the system up to be capable of being monitored and supported remotely either via direct or a set of network configurations (i.e., firewall rules, port-forwarding, etc.). Should the site use a fibre optic cable for external communications (VoIP) and there is no access to a dedicated PSTN connection for remote monitoring, then a battery backed Cellular connection shall be installed for any power outages.

7.4.5. Alerts & Notifications

The ESMS shall support the automatic sending of emails and SMS text messages as a result of defined events or alarms. The ESMS shall allow operators to define the contents of the email or ESMS text message. Dynamic text, such as the details of an alarm, is to be automatically entered by the ESMS, along with any static text defined by the operator.

The SMS shall support sending emails by specifying an SMTP server and any relevant authentication credentials that may be required by the SMTP server. In addition, the ESMS shall support sending emails over an encrypted SSL connection to the SMTP server.

The SMS shall keep a history of all sent messages including the type of message (SMS text or email), the time and date they were sent, the recipient, any retry attempts and so forth.

The SMS shall include comprehensive alarm management functionality to allow any kind of security or access event to be trapped and brought to the attention of an operator via a monitoring station or some other person via text messaging or email.

7.4.6. Logging & Reporting

The ESMS shall include an event log that records every event that takes place on any controller and from within the software itself. This log is to allow events to be viewed in real-rime or used to view historic events that have already occurred within the system.

The event log shall be capable of purging low-risk event details from the log on a set schedule e.g., 31 days, to avoid system lag and performance impacts.

The ESMS shall include a comprehensive audit log, detailing every change that was made to the system programming, who made the change and when it was changed.

The ESMS shall include basic reporting features throughout the application.

7.5. Security Enclosures

The security enclosures shall contain all central security related equipment with preferably one cabinet assembly, or where needed, multiple cabinet assemblies.

The security enclosures shall be modular style wall mounted cabinets manufactured from powder coated steel. Doors are to be full hinged and are to include door locks. All locks shall be keyed alike but not be the manufacturer's standard. Two sets of keys are to be provided to the project manager on completion of the project. Cabinets shall be sized to ensure good cableways and that the board is regular in shape. Within the cabinets provide slotted cable trunking, of appropriate size, for cable management and house all cables within. All internal cables shall be fully labelled.

All panels shall include tamper protection for the front and back of the panel. The front panel shall be tamper protected for door open and the rear panel for removal of cabinet from the wall.

The terminations of cables shall be made into DIN rail type connectors or directly onto the controller boards. All equipment and connectors within the security panels shall be suitably labelled and identified. Equipment and battery enclosures shall be protected to at least IP 31 degree of protection.

A plan sleeve shall be provided on the inside of the panel door for holding installation information including:

- A sketch for the floor layout showing the location of all field hardware.
- Wiring diagrams for all equipment associated with the panel.
- Door configuration information.
- Controller configuration details such as IP address.

A minimum of 20% spare capacity shall be provided for future expansion in each cabinet.

Each cabinet shall be earthed in accordance with AS/NZS 3000.

7.6. Controllers and IO (Input/Output) Expanders

7.6.1. Controllers

The control of doors and lifts shall be carried out by distributed intelligent micro-processor-based units capable of operating independently and shall be capable of operating properly during loss of communications with any main controller or ACID (Access Control and Intruder Detection) server.

Each controller shall be capable of controlling the required number of doors and lifts and record all valid and invalid access attempts. Local records shall be transferred to the respective central ACID server for analysis and archiving. The controllers shall be programmed from a central panel but once programmed, shall operate independently with changes only as instructed from the central panel.

All controllers shall be connected via the UoO security LAN (IP address blocks, gateways, and Network masks to be confirmed with UoO ITS Infrastructure prior to installation) to facilitate communications between units and back to the central security panel, as required even under power fail conditions. Refer to section 2 for the existing configuration for UoO's access control and intruder detection system IP address range details.

The controllers shall, after a power failure, return to the same state as before the power failure. Should the solution proposed run over an Ethernet LAN, then all components (including network switches) shall survive a power failure for a minimum of 8 hours to match the capability of using an RS485 LAN.

For all electronically controlled doors a separate door lock and a separate door closed signal is required.

7.6.2. IO Expanders

Gallagher FT high density IO (In and Output) modules will be required, to extend FT controllers to the following in and outputs:

- Duress systems in the Staff room, Dispatch etc.
- Mains and battery failure in in the Plant rooms.
- Fire alarms.
- Walk-in Freezers (An external warning light and siren to be located above the door external to the freezer)
- Areas where hazardous chemicals are used

All the GBUS expanders needs to be replaced with HBUS expanders.

Output signals to be escalated to:

- Campus Watch
- Local siren / Strobe

7.7. Card Readers

Card readers shall be proximity type, dual tech (125 kHz and 13.75 MHz) and contain a beeper and multicolour LED, which can be hosted and/or locally controlled and be able to generate a signal to enable the controller to identify lost communication and thereby generate an alarm.

The card readers shall be able to provide high reliability, consistent read range and have low power consumption. Card readers should not be proprietary to the access control system.

The associated reader specifications are:

- Readers must comply with at least IP54 environmental protection rating.
- A vandal-resistant enclosure meeting an IP65 rating shall be provided in external installations and inside the following UoO areas / Buildings:
    - Plant spaces
    - Basement card parks

- Where there are card readers on both sides of a controlled door, they must be wired separately to show direction of movement.
- Card reader physical dimensions shall be no wider than 53mm to allow mounting on door jambs where no suitable solid wall exists.

7.7.1.1. Card reader locations

Card readers to be located in the following buildings or areas:

UoO Area	Immediate area where an electronic access controlled is required
Faculties	Receptions – Main entry door
Faculties	Reception – Reception counter and waiting areas
Faculties	Staff Only areas – Main entry and exits
Faculties	Lab entry and exit points
Faculties	Fire stair entry and exit point
Faculties	Lifts
Faculties	Communal areas - Corridors
Faculties	Lecture Theatres – perimeter entry and exit points
Faculties	Meeting rooms and small lecture spaces – Main entry and exit points
Faculties	Perimeter entry and exit points – Ground level, lower ground, level 1 (balcony areas) and main entry to building services plant room areas
Faculties	Engineering and labs where hazardous equipment and substances are managed
Cafes and recreation building and areas	Fire stair entry and exit point
Cafes and recreation building and areas	Lifts
Cafes and recreation building and areas	Lift Foyers
Cafes and recreation building and areas	Lecture Theatres – perimeter entry and exit points

UoO Area	Immediate area where an electronic access controlled is required
Cafes and recreation building and areas	Meeting rooms and small lecture spaces – Main entry and exit points
Cafes and recreation building and areas	Perimeter entry and exit points – Ground level, lower ground, level 1 (balcony areas) and main entry to building services plant room areas
Cafes and recreation building and areas	Areas where high risk activities being undertaken i.e., rock climbing
Cafes and recreation building and areas	Gym main entry and exit points
Cafes and recreation building and areas	Point of Sales
Student Accommodation	Receptions – Main entry door
Student Accommodation	Reception – Reception counter and waiting areas
Student Accommodation	Staff Only areas – Main entry and exits
Student Accommodation	Fire stair entry and exit point
Student Accommodation	Lifts
Student Accommodation	Lift Foyers
Student Accommodation	Communal areas - Corridors
Student Accommodation	Meeting rooms and small lecture spaces, whanau spaces and games rooms – Main entry and exit points
Student Accommodation	Perimeter entry and exit points – Ground level, lower ground, level 1 (balcony areas) and main entry to building services plant room areas
Student Accommodation	Areas where high risk activities being undertaken i.e., rock climbing
Student Accommodation	Gym main entry and exit points
Administration Buildings	Receptions – Main entry door
Administration Buildings	Reception – Reception counter and waiting areas

UoO Area	Immediate area where an electronic access controlled is required
Administration Buildings	Staff Only areas – Main entry and exits
Administration Buildings	Fire stair entry and exit point
Administration Buildings	Lifts
Administration Buildings	Lift Foyers
Administration Buildings	Communal areas - Corridors
Administration Buildings	Perimeter entry and exit points – Ground level, lower ground, level 1 (balcony areas) and main entry to building services plant room areas
Administration Buildings	Point of Sales

7.8. Electronic Locks

7.8.1. Electric Mortice Lock

Electric mortise locks shall be:

- Assa Abloy/Lockwood 3570 for standard size doors (or equivalent); and
- Assa Abloy/Lockwood 3582 for narrow back applications (or equivalent).

The Security consultant and/or Security contractor shall ensure that the locks used are compliant with the door manufacturer's approved locks, which will comply with maintaining the fireproof rating integrity of the applicable fire door.

All mortise locks shall have:

- 12/24VDC fail safe with full locked, latch, and hub monitoring. The internal handle shall also be connected to the controller via way of micro switch, recording the request to exit.
- Hinge transfers shall be Assa Abloy EA280 (or equivalent).
- Each lock shall be individually fused and fail safe; and
- All locks shall meet the required fire specification rating.

Electric mortise locks shall control the locking of the outside (non-secure side) handle. The internal handle shall provide free egress. Releasing the lock shall cause the door to remain latched.

7.8.2. Electromagnetic Lock

Electromagnetic locks (EML) shall be:

- Assa Abloy/Lockwood Z4 for standard size doors (or equivalent).
- Assa Abloy/Lockwood Z2 for narrow frame applications (or equivalent).
- Assa Abloy/Lockwood Z8 for over standard size doors (or equivalent).
- Assa Abloy/Lockwood Z8 weather-resistant unit for outdoor/external applications (or equivalent).
- FSH MEM2400 for lightweight frame applications (or equivalent).

All EMLs shall:

- Be monitored.
- Be 12V DC fail safe.
- Each lock shall be individually fused.
- Meet the required fire specification rating.
- Always be mounted internal to the building (unless specifically for an outdoor application), in such a way that no cabling is exposed or visible.
- Have a certified minimum holding force of 600kg in secured position, and the magnets shall be specifically designed so they do not become permanently magnetised over time.
- Shall have a Z plate fitted for standard doors of 1980mm in height; and
- Shall have a U bracket fitted for frameless glass doors.

Where double door EMLs are detailed on drawings, incorporate two EML devices into a single housing.

The Security consultant and/or Security contractor shall ensure that the locks used, are compliant with the door manufacturer's approved locks, which will comply with maintaining the fireproof rating integrity of the applicable fire door.

7.8.3. Electric Strike Locks

Electric strike locks shall be:

- Assa Abloy/Lockwood ES2000 (or equivalent) for standard size internal doors.

All strike locks shall:

- Be 12V DC fail safe with full strike locked and door latched monitoring.
- Be of stainless-steel construction.
- Be individually fused.
- Meet the required fire specification rating; and
- Have a certified minimum holding force of 680kg in secured position, and be endurance tested to exceed 1,000,000 strike operations.

The Security consultant and/or Security contractor shall ensure that the locks used, are compliant with the door manufacturer's approved locks, which will comply with maintaining the fireproof rating integrity of the applicable fire door.

7.8.4. Electronic Drop Bolt

Electronic Drop Bolts (EDB) shall be:

- Assa Abloy/Lockwood IB25 (or equivalent).

All EDB shall:

- Be 12/24V DC fail safe.
- Be monitored.
- Have magnetic auto alignment.
- Individually fused.
- Be of stainless-steel construction; and
- Meet the required fire specification rating.

The Security consultant and/or Security contractor shall ensure that the locks used, are compliant with the door manufacturer's approved locks, which will comply with maintaining the fireproof rating integrity of the applicable fire door.

7.8.5. Hook Locks

Electrical hook locks shall be:

- Assa Abloy/Lockwood ES6000 (or equivalent).

All hook locks shall have:

- 12/24V DC fail safe.

- 700kg holding force.
- Each lock shall be individually fused and fail safe; and
- All locks shall meet the required fire specification rating.

7.8.6. Request to Exit (ReX)

Request-to-Exit (ReX) buttons shall be touch sensitive wall switches that can be used for the following applications at minimum:

- Used in conjunction with the access control system to perform function of an exit button.
- Used as a remote door release switch at a reception desk.
- Ease of operation for everyone requiring accessibility assistance.

All ReX buttons shall operate on voltage 12-16V DC and have current consumption not greater than 50mA in operation. They shall be IP65 rated in external installations.

7.8.6.1. Motion detection (Contact less) ReX buttons

The motion detection activated ReX buttons shall comply with the following requirements:

- Comply with her requirements stated under the above-mentioned section (7.8.6).
- IP67 rated.
- Dual colour LED.
- Output timer selectable: >1 and <= 10 seconds.
- Input voltage: 12v DC.
- Output: isolated NO and NC; 1A 30V DC.

7.8.6.2. Fire safety requirements in relation to ReX buttons:

The following is required, in relation to ReX's, to comply with the Code of Practice for Electromechanical Controlled Locking devices on Egress doors: June 2018:

- Allow enough time for the user to move from REX to door and open it.
- The button operation requires a single button press and release and then door to be physically opened and not a continual button press and door to be manually opened at the same time.

- Button is required to be green.
- Any Rex more than 900mm and less than 1500mm away from an access-controlled door shall be clearly marked with a sign at the door indicating direction and location of the ReX; and
- ReX' shall not exceed 1350mm above floor finish level.

7.8.7. Emergency request To Exit / Emergency Door Release (EDR) Units

Emergency Door Release (EDR) units shall be flush mounted, where possible. On activation, a signal shall be sent to the local Gallagher Controller. The operation of the unit is to be monitored by UoO's Campus Security. At each break glass unit, provide an audible sounder that is operated when the Emergency Door Release (EDR) is operated and remains operable until the alarm is deactivated.

Where located on a secure egress door (i.e., card reader access in the direction of exit), the unit shall be fitted with an additional stopper cover, which emits a local audible sounder when lifted. Any additional stopper cover shall not affect the system operation or monitoring. The security contractor shall provide all details to the project manager, consultant, UoO representative, for approval prior to implementation.

Emergency Door Release (EDR) units shall be IP65 rated in external installations.

7.8.7.1. Fire safety requirements in relation to Emergency Door Release (EDR) buttons:

This section should also be read in relation to C/AS 2 Section 3.15.2.

The following is required, in relation to Emergency Door Release (EDR)', to comply with the Code of Practice for Electromechanical Controlled Locking devices on Egress doors: June 2018:

- Cut the power supply to the lock and magnetic hold opens.
- The magnetic lock and magnetic hold open to remain in the fail-safe position till the Emergency Door Release (EDR)' have been manually re-set.

- Emergency Door Release (EDR)' changing NC state to NO state to another relay, who connected to a lock power in NC state, needs to be detailed in building consent application i.e. an Emergency Door Release (EDR) connected to the access control panel in NC state i.e. and monitored for circuit resistance change i.e. changing to NO state, needs the access control panel output to door lock power to also change from NC to NO state – this is not applicable to this design and will need to be issued by the installer if this is the methodology required;
- The Emergency Door Release (EDR)' must be green and clearly marked as an emergency device.
- The Emergency Door Release (EDR)' can be an additional input to an alarm panel i.e., to sound the door buzzer if activated, but not cause the Emergency Door Release (EDR) to malfunction.
- The Fire alarm relay shall not replace the Emergency Door Release (EDR). The Emergency Door Release (EDR) is still required even if the electromagnetic lock power supply feed is connected through a fire alarm relay.
- The Emergency Door Release (EDR)' may be protected by a cover that has a clear cover and is not lockable and has clear instructions to remove cover.
- The Emergency Door Release (EDR)' protected cover being Opaque/faded, shall allow for the covers to be replaced with minimal cost and time impact.
- Electromechanical lock operations will not avoid panic fastening to open the doors.
- No Emergency Door Release (EDR) is required when panic fastening is in place.
- Any Emergency Door Release (EDR) more than 900mm and less than 1500mm away from an access-controlled door shall be clearly marked with a sign at the door indicating direction and location of the Emergency Door Release (EDR); and
- Emergency Door Release (EDR)' shall not exceed 1350mm above floor finish level.

7.9. Intercoms

7.9.1. Intercom general characteristics

The following general characteristics is required as a minimum in terms of intercoms system deployed at UoO:

- Must be compatible with the building main ACID (Gallagher) and CCTV (Avigilon).
- Must use TCP/IP protocols.
- Must have the ability to integrate over a SIP system if needed.

- Must be IP65 rated and or suitable for the environment it will be deployed in.
- Video and voice enabled

7.9.2. Intercom locations

The following areas / buildings will require intercom gate stations:

- Perimeter doors leading into buildings

Intercom base stations will be in the following buildings and areas:

- Receptions
- Entrance ways
- Building upper Levels

7.9.3. Gate stations

Gate stations shall have the following characteristics as a minimum:

- Suitably rated for the environment it is deployed - As a minimum IP65 for external and IP45 for internal deployments
- LED lid push to talk button
- Internal microphone to allow for audible experience to users and legible voice level feedback for base station operators, where external noise levels may exceed standard ambient noise levels
- LCD display for hearing impaired users
- Brail text on housing for visual impaired users
- Sun and rain cover
- Vandal proof wall fixing screws
- 5MP internal camera with day night compatibility
- Ventilated
- Volume control with auto reset after gate opening activated

7.9.4. Base stations

Base stations shall have the following characteristics as a minimum:

- Suitably rated for the environment it is deployed - As a minimum IP65 for external and IP45 for internal deployments
- LED lid push to talk button
- Internal microphone to allow for audible experience to operators and legible voice level feedback for gate station users, where external noise levels may exceed standard ambient noise levels
- LCD display to indicate:
    - Intercom location
    - Date
    - Time
    - 10" display with UHD quality
    - Volume control
    - LCD back light control
- Internal memory storage up to 7 days voice and video footage

7.10. Public Address Systems

7.10.1. Sound

7.10.1.1. Audio Frequency response

The PA and Paging system need to provide a minimum of 250 Hz to 5 kHz and 20 Hz to 20kHz frequency response to allow for the successful reproduction of speech.

7.10.1.2. Sensitivity

The sound will not exceed 95 dB SPL at the listener's ear and no less than 75dB or the sound will be 15dB and no more than 20dB above the ambient noise levels. This is to ensure the PA system does not get lost or being unintelligible.

7.10.2. Design and configuration

The PA contractor shall design and install sound which will accommodate the space dimensions, expected ambient noise levels for the various areas within the age care facility and also factoring the different surfaces composition. Smaller dispersion angle speakers or more speakers to be considered if the planned speaker dispersion angles cannot meet the required level of sound above ambient noise levels.

7.10.2.1. Zoning and applicable telecommunication spaces

Speakers will be zoned according to the various PA zones. Speakers should also be set up to allow for priority between fire activation system shutdown (not announcements because it will be driven by the dedicated fire detection and evac system), standard announcements, background music.

7.10.3. Power Amplification

2 options are required for the PA system sound amplification:

- Traditional Analogue centrally amplified system with Analogue to IP interface; and
- IP Digital PA system with distributed amplified system.

The PA contractor shall ensure that the transformers they select at the speakers will match the speaker voice coil impedance to ensure the power of the transformer do not exceed the speaker's maximum power capacity.

The PA contractor shall ensure that the circuit connections are correctly polarized to avoid reduced sound, no sound or sound distortion.

The sound amplifiers to be sized to ensure the planned circuit will not exceed 80% of the amplifier load capacity or 25% to 50% more capacity than the sum of all the speaker power combined connected to the amplifier. The PA contractor should also take a 1dB loss per speaker transformer, when calculating number of speakers required.

The PA system based on the analogue option will be a centralised powered system with a constant voltage in mind with planning speaker sizing, placemen etc. Amplifiers also needs to be located in the applicable communications room, applicable to the PA Zone.

The PA Contractor shall consider the following when sizing the amplifier capacity:

- Sum of wattage taps
- Sum of cable power loss
- Future growth – At least 25%

7.10.4. Speakers

7.10.4.1. Speaker layout

Square patterns inside TV lounges and dining halls and inline patterns for corridors.

7.10.4.2. Speaker spacing and orientation methodology

The following will apply with regards to speaker spacing:

- Edge to edge: Distance spacing = 2r (r = base coverage) – This is required in hallways
- Minimum overlap: r x 1.414 (for square layout) - This is applicable to TV rooms and dining halls

The spacing between speakers will be 2 x (Edge to Edge methodology) the ceiling to floor distance in areas where the ambient noise levels are less than 70dB. Areas with ambient levels more than 70dB will required for the speakers to be spaced 1.732 x ceiling to floor height (in case of hexagon pattern layout). It will be the responsibility of the PA Contractor to do the final design and issue to the ICT consultant for approval.

Wall mount speakers shall be no less than 2.4 meters and no more than 3.7 meters from the floor level and will not directly face another opposite side wall speaker.

Wide dispersion speakers should be avoided due to the system's primary function is speech reinforcement of the PA system with background music being regarded as a secondary function.

Speakers in hallways shall be mounted as follow:

- Ceiling mount versions:
    - 1st speaker shall be 2.4 meters from start of hall and end of hall
    - Installed at hallway junctions
    - Spaced at 2 x ceiling to floor height distance
- Wall mount:
    - Bi-directional at 6.1 from hall, start and end
    - 8 meters intervals alternating between the hallway walls

7.10.4.3. Speaker phasing

The speakers will be al tuned to be in phase.

7.10.4.4. Network Speaker technical requirements

Analogue Speaker System

The following schedule provides a summary of the analogue speaker's minimum technical requirements:

Item	Technical Category	Minimum Requirements
1	Max Sound Pressure Level (SPL)	95dB

Item	Technical Category	Minimum Requirements
2	Frequency response	45Hz to 20kHz
3	Maximum Coverage Pattern	130 degrees
4	Built in amplifier and capacity	6W Class D

Digital Speaker System

The digital speakers are based on the AXIS C2005 Network Ceiling Speaker or similar system.

The following schedule provides a summary of the digital speaker's minimum technical requirements:

Item	Technical Category	Minimum Requirements
1	Audio steaming	1 way (optional 2 way if needed)
2	Max Sound Pressure Level (SPL)	95dB
3	Frequency response	45Hz to 20kHz
4	Maximum Coverage Pattern	130 degrees
5	Built in amplifier and capacity	6W Class D
6	Network Security	• Password protection. • IP address filtering. • HTTPS encryption. • IEEE 802.1X network access control. • Digest authentication. • User access log. • Centralized certificate management
7	Supporting Open SSL	Yes

Item	Technical Category	Minimum Requirements
8	Supported network protocols	• IPv4/v6. • HTTPS, • QoS Layer 3 DiffServ. • SFTP. • CIFS/SMB. • SMTP. • Bonjour. • UPnPTM. • SNMP v1/v2c/v3 (MIB-II). • DNS. • DynDNS. • NTP. • RTSP. • RTP. • TCP. • UDP. • IGMP. • RTCP. • ICMP. • DHCP. • ARP. • SOCKS. • SSH. • NTCIP. • SIP
9	VoIP	• Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems, if needed in future. • Peer to peer or integrated with SIP/PBX. • Supported SIP features: secondary SIP server, IPv6, SRTP, SIPS, SIP TLS, DTMF (RFC2976 and RFC2833), NAT (ICE, STUN, TURN) • Supported codecs: PCMU, PCMA, opus, L16/16000, L16/8000, speex/8000, speex/16000, G.726-32
10	Audio Synchronisation	Yes
11	Memory	256 MB RAM, 256 MB Flash
12	Power	Power over Ethernet

Item	Technical Category	Minimum Requirements
13	Ethernet	100BASE-TX
14	Safety Wire Kit	Yes

The speakers need to be connected, via the PA system VLAN, to the to the audio management system inside the Campus Security Control Room.

7.10.5. IP to Analogue Zone Convertor/Bridge

The PA system IP (Digital) to Analogue Convertor/Bridge is required if the client wishes to proceed with the analogue speaker option.

7.10.5.1. System Requirements

The PA system IP (Digital) to analogue convertor/bridge is based on the AXIS C8033 Network Audio Bridge, AXIS C8210 Network Audio Amplifier or similar.

The following schedule provides a summary of the IP (Digital) to Analogue Convertor/Bridge's minimum technical requirements:

Item	Technical Category	Minimum Requirements
1	Audio streaming	2-Way
2	Power Supply	PoE
3	Audio encoding	• AAC LC 8/16/32/48 kHz, • G.711 PCM 8 kHz, • G.726 ADPCM 8 kHz, • Axis μ-law 16 kHz, • WAV, • MP3 in mono/stereo from 64 kbps to 320 kbps.
4	Network Security	• Password protection. • IP address filtering. • HTTPS encryption. • IEEE 802.1X network access control. • Digest authentication. • User access log. • Centralized certificate management
5	Supporting Open SSL	Yes

Item	Technical Category	Minimum Requirements
6	Supported network protocols	• IPv4/v6. • HTTPS, • QoS Layer 3 DiffServ. • SFTP. • CIFS/SMB. • SMTP. • Bonjour. • UPnPTM. • SNMP v1/v2c/v3 (MIB-II). • DNS. • DynDNS. • NTP. • RTSP. • RTP. • TCP. • UDP. • IGMP. • RTCP. • ICMP. • DHCP. • ARP. • SOCKS. • SSH. • NTCIP. • SIP
7	VoIP	• Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems, if needed in future. • Peer to peer or integrated with SIP/PBX. • Supported SIP features: secondary SIP server, IPv6, SRTP, SIPS, SIP TLS, DTMF (RFC2976 and RFC2833), NAT (ICE, STUN, TURN) • Supported codecs: PCMU, PCMA, opus, L16/16000, L16/8000, speex/8000, speex/16000, G.726-32
8	Audio Synchronisation – Unicast and Multicast	Yes
9	Memory	256 MB RAM, 256 MB Flash
10	Power	Power over Ethernet

Item	Technical Category	Minimum Requirements
11	Ethernet	100BASE-TX
12	Event Actions	• Play audio clip, • Send SNMP trap, • File upload via HTTPS, • Notification via email, HTTPS, and TCP, • External output activation.

7.10.5.2. Network integration

Analogue Speaker System

The IP to Analogue Bridge to be located inside the applicable PA Zone communications room inside the cabinet on a shelf. The IP to Analogue Bridge is patched to the PA Contractor supplied and installed network switch (This option might change if the client decides to supply, configure, and install the network switching equipment).

The IP to Analogue Bridge is connected to the associated sound amplifier, which is connected to the analogue speakers.

The IP to Analogue Bridge is connected back to the PA Microphone and Console Unit and also the PA Microphone and Console Unit and the Audio Management System, via the PA System switching network.

Digital Speaker System

Each Digital Speaker is connected to the PA Contractor supplied and installed network switch (This option might change if the client decides to supply, configure, and install the network switching equipment).

The IP Digital Speakers are also connected to the PA Microphone and Console Unit and also the PA Microphone and Console Unit and the Audio Management System, via the PA System switching network.

7.10.6. PA Microphone and Console Unit

7.10.6.1. Speech reinforcement

The PA contractor to allow for speech reinforcement to be governed at the PA Microphone and Console Unit to allow for the following:

- Stable system.
- Intelligible; and
- Acceptable level of loudness.

7.10.6.2. System Requirements

The PA Microphone and console unit is based on the 2N Sip or similar system.

The following schedule provides the minimum system requirements:

Item	Technical Category	Minimum Requirements
1	Minimum multi cast zones	12
2	2-way communications enabled	Yes
3	Web based management access enabled (HTTPS)	Yes
4	Power Supply	PoE
5	IP PBX compatibility via SiP	Yes
6	Pre-recorded massages	Yes

7.10.6.3. Network integration

Analogue and Digital Speaker System Options

The PA Microphone and Console Unit is patched to the PA Contractor supplied and installed network switch (This option might change if the client decides to supply, configure, and install the network switching equipment).

The PA Microphone and Console Unit is connected back to the Audio Management System, via the PA system switching network.

7.10.7. Audio Management System

7.10.7.1. System overview

The system shall be located inside Campus Security. Dedicated and authorised UoO staff (i.e., directly connected to the authorised users in Informacast such as Incident Management Team, Proctor, Deputy Proctor, Campus Watch controller and possibly specific roles In the Senior Leadership Team) will have the ability to schedule announcements and also monitor any speaker issues (if the system is fully digital) and report to the security provider for accurate maintenance response. The manager will also have the ability to schedule background music and sound levels (if fully digital).

7.10.7.2. System Requirements

The Audio Management System is based on the AXIS Audio Manager Pro or similar system.

The following schedule provides the minimum system requirements:

Item	Technical Category	Minimum Requirements
1	Licence	Unlimited
2	PC hardware requirements	Intel® Core™ i3-7100T
3	PC software requirements	Microsoft Windows 10 IoT 2016 LTSB
4	Audio streaming	• Stereo/mono from 32 kbps to 320 kbps, • Unicast and Multicast, • MPEG-1 Audio Layer 2 (MP2) • Support for internet radio via secure URL
5	VoIP	• G.711u, • G.711a • Support for Session Initiation Protocol (SIP) for integration with Voice over IP (VoIP) systems • Peer to peer or integrated with SIP/PBX.
6	Supported protocols	• IPv4&6, • HTTPS, • DNS, • NTP, • RTP, • RTSP, • TCP, • UDP, • DHCP, • SIP, • mDNS, • M3U
	Security	Multiple user access levels with password protection
	Event triggers	• HTTP commands triggering • Playback scheduler

The PA Contractor to allow for a PC as an option if the client is not supplying the management PC.

7.10.7.3. Network integration

Analogue and Digital Speaker System Options

The PA Microphone and Console Unit is patched to the PA Contractor supplied and installed network switch (This option might change if the client decides to supply, configure, and install the network switching equipment).

The PA Microphone and Console Unit is connected back to the Audio Management System, via the PA system switching network.

7.11. System Warranty

The cabling solution is to be supported with a vendor's warranty for a period of not less than 5 years.

7.12. Legacy systems

The ESS design shall consider the interface requirements of legacy equipment in existing installations. If any discrepancies are noted, they should be highlighted in writing to the University or its representative.

8. DESIGN REQUIREMENTS

8.1. General

1. The design consultant shall be responsible for a thorough and accurate design to enable installers to provide a correct installation, testing, commissioning, and functional system as described in the design specification and as per this standard.
2. The Designer shall also provide a fully coordinated design to allow for a fully integrated, and operational system.
3. Detailed design shall specifically include but not necessarily be limited to the following:
    a. Design of individual systems that make up the electronic security systems as described herein including system layout, selection of materials, design of system operation, working methodology, selection of hardware and equipment.
    b. Design of fixing and support details.
    c. Design of seismic details.
    d. Design of all hardware and installation required to comply with fire rating and smoke sealing requirements of the fire specification and standards.
    e. Design of trimming and flashing details for penetrations through roofs/walls associated with these systems.
    f. Detailed co-ordination of electronic security systems with building works, and other building services.
    g. Maintaining of any existing services and integration of existing services with new as specified.

8.2. Aesthetic design

In all cases the ESS shall be designed and installed in a manner that is suitable for the building and not in conflict with the environment.

8.2.1. Heritage buildings

The contractor shall refer to the UoO BTSS CHAPTER 1: INTRODUCTION for all heritage building requirements.

8.3. Environmental considerations

The contractor shall refer to the UoO BTSS CHAPTER 1: INTRODUCTION for all environmental considerations.

8.4. Design Documentation

For ESS designed and installed at UoO campuses, items generally considered to be in scope include the following:

1. A formal scope of works document detailing all components, actions, responsibilities, accountabilities, and co-ordination applicable to the ESS deployment for respective projects.
2. Undertake a design process in accordance with NZ Construction Industry Council CIC Guidelines.
3. Layout drawings and schematics detailing the construction of the ESS encompassing:
    a. ACID (Access Control and Intruder Detection) and CCTV servers
    b. ESS main and field controllers
    c. Associated risers and comms room/plant room locations
    d. Applicable cable pathways etc.
4. Subject to specific project-based scope documents, further items that may need to be included:
    a. Catenaries and conduits routes from the supplied cable trays.
    b. Penetration locations and sizing through the floor, wall, and structural beams.
    c. System interfacing i.e., Fire detection system, BMS, etc.
    d. Automated doors.
    e. Remote ESS monitoring and remote access requirements.
    f. Servers, backup systems and connection to uninterruptible power supplies (UPS).

g. Local Area Network (LAN) and Wireless Local Area Network (WLAN) routing and switching requirements i.e., ACID and CCTV servers' connections to field controllers and CCTV cameras, RFID tags connection to the ACS (Access Control System)

h. ESS PSU (Power supply units) power load requirements.

i. Wireless equipment, including access points, controllers, RFID tagging etc.

j. ESS BUS communication cabling and expander modules.

8.5. Design Coordination

Where the ESS work is dependent upon or carried out in conjunction with other works (such as building, structured cabling or electrical works), the security contractor shall coordinate security installation activities with the project manager and UoO's Facilities Management team with respect to:

- Liaison with all members of the building services design and respective project management teams, and other contractors or system providers as required.
- Attendance at meetings called by the main contractor, architect, engineers, or other members of the project team.
- Use of the works site and access facilities.

8.5.1. Design - Scheduling of the works and site construction resources and utilities

- Interface with structured cabling, electrical, mechanical, fire and lift service contractors; and
- Reinstatement and remediation of building surfaces and/or groundworks.

Refer to Annexure A: Coordination schedule.

8.5.2. Electrical Services

Co-ordination with electrical services includes the following:

- Mounting requirements for any electrical feeds, isolators or socket outlets required by the ESS.

- Any shared services routes ensuring that all installed cabling meets separation and segregation requirements pertaining to electrical safety and system performance; and
- Any integration with building lighting systems.

8.5.3. Generic Cabling Systems (GCS)

Co-ordination and liaison regarding:

- Any electronic security hardware to be mounted in ICT cabinets and communication room spaces i.e., inside the telecommunication rooms and ICT risers.
- Shared support systems to ensure adequate reticulation space for system cabling.
- Hardware mounting in any shared equipment rooms/spaces. Care is required to ensure any free-standing cabinet doors can open unimpeded by security panels within the rooms.
- The provision of any telecommunications outlets or network connectivity required for the SCPs of field controllers.
- The provision of any cabling for CCTV cameras; and
- UPS'.

All cabling installed by the structured cabling contractor for CCTV cameras shall be fully terminated and tested prior to use.

Refer to UoO BTSS CHAPTER 3: IT Infrastructure – Generic Cabling Systems Standard in relation to GCS (data cabling)

8.5.4. Fire Protection Services

Co-ordination and liaison regarding:

- Any communication interface requirements detailed between the ACS and the fire detection/evacuation system, to allow free egress in the event of a fire evacuation; and
- The provision of volt-free relay contacts to release any Magnetic Hold Open devices (MHO), where applicable

- The security contractor/Security consultant to allow for the Statement of Coordination (Refer to Annexure B for the performa), to be completed and included in the design specification and/or the security contractor shop drawings and system proposal – The statement of coordination will be required during the consent stage of a project
- Any coordination required in relation to Passive Fire Systems.

8.5.5. Lift/Vertical Transport Services

Co-ordination and liaison regarding:

- Any integration with any lift car or vertical transport systems. The security contractor shall be responsible for coordinating the level of integration, the type of integration, the equipment to be used and any required programming, commissioning, and testing.

8.5.6. Mechanical Services

Co-ordination and liaison regarding:

- The positioning of any mechanical ventilation or cooling equipment ensuring that it does not impact on the operation of the ESS; and
- Any integration with the Building Management System (BMS), deployed throughout UoO – Refer to section 5.2.3.3

8.5.7. Building Works

Co-ordination with construction services and builders may be required for any of the following:

- Identification, sizing and marking out of all penetrations required for the ESS system cabling.
- Sealing/flashing of all services penetrating any portion of the external skin of the building e.g., cladding, roof, floor, etc.
- Construction of equipment rooms, panel housings, entry facilities and required floor and ceiling bundling, sealing, including any passive ventilation, etc.
- Construction of all communications risers.
- Access panels in ceiling for cable ladders and other equipment requiring access for maintenance and servicing.

- Removal and reinstatement of tiles in ceilings, roof cat walks and platforms, cranage and access for plant erection.
- Placing, casting in and protection of conduits within any structural wall, floor, or ceiling space.
- Responsibilities pertaining to the cleaning of equipment rooms and riser locations.
- Signage on doors for security system spaces and all communications riser cupboards.
- Utilisation of door jambs and window frames for cable pathways in areas where wall access is not available.
- Details of weight of equipment and services clearances required.
- Structural bracing and support required in floors, walls and ceilings for SCPs, field controllers and cameras; and
- Installation of any electronic or magnetic locks on doors and frames.

8.6. Battery Backup and Power Supplies Design

1. The electronic security system (ESS) shall be provided with sufficient battery capacity to allow the system to operate normally for duration of at least eight (8) hours.
2. Battery back-up power supplies shall be provided within each security enclosure. The supplies shall be sized such that the load on one power supply does not exceed 75% of the power supply rating.
3. In sizing the batteries consideration shall be given to the minimum equipment operational voltage, cable voltage drops and battery end-of-life voltage. Following factors shall be allowed for in battery sizing:
    a. Ageing - 1.25.
    b. Design Margin - 1.10.
    c. Design ambient temperature - 25oC.
    d. Per cell cut off voltage – DC supplies 1.8V PC; and
    e. Per cell cut off voltage – UPS supplies 1.7V PC.
4. Provide fused dim rail mounted outputs such that each major device or door is individually fused, boards are to incorporate LED indication.

5. As access control controllers are less tolerant to low voltage than the locks, either a separate battery backup supply or a suitable DC-DC convertor shall be provided such that the access control controllers remain fully operational even though the locks may have released due to low voltage.
6. The systems shall comprise:
    a. Batteries.
    b. Battery charger.
    c. Inverter and DC-DC convertors.
    d. Main's voltage monitor.
    e. Audible and relay On Battery alarm.
    f. Audible and relay fault alarm.
    g. Controls; and
    h. Output distribution panel incorporating load protection and output fuse boards.
7. Low battery, mains and system failures shall all be monitored by the ESS and escalated to the UoO Security control room.
8. The security system shall be capable of recharging the battery back-up batteries from empty to full charge over a period of twenty-four (24) hours.
9. The minimum power supply current available for battery charging shall also exceed the value derived from the battery capacity in Amp hours multiplied by 1.2 and divided by the re-charge period in hours.
10. Batteries shall be maintenance-free sealed lead-acid type with a minimum design life of 5 years at a potential ambient temperature of 50o Celsius. Batteries shall be labelled with the date of installation and service schedule requirements detailed within the handover documentation.

8.7. Uninterruptable Power Supply (UPS) design

1. A UPS will be required to provide battery back up to any associated network equipment, if not already covered under a new project or a renovations project.
2. Final approval of any UPS should be sought from the client representative prior to ordering. UoO reserves the right to supply any such network equipment at their own cost. In the event the client does provision such hardware the contractor shall detail system power consumption details and issue it to UoO.

3. Refer to UoO BTSS CHAPTER 3: IT Infrastructure – Generic Cabling Systems Standard in relation to UPS power.

8.8. Network Equipment design

1. Any network equipment required to facilitate the complete operation of the ESS system shall be detailed in the security contractor's tender submission (unless otherwise tagged out in the scope of works of drawing layouts).
2. All network equipment shall be 19" rack mountable and be mounted into an ICT cabinet. Equipment shall be sized to accommodate all cameras specified plus an additional 25% expansion.
3. Final approval of any network equipment should be sought from UoO IS representative prior to ordering. UoO reserves the right to supply any such network equipment at their own cost. In the event UoO does provide such hardware, the security contractor shall detail any specific requirements to allow the system to function correctly.

8.9. Fire safety integration design requirements

8.9.1. Fire safety requirements for Rex buttons

The following is required, in relation to ReX's, to comply with the Code of Practice for Electromechanical Controlled Locking devices on Egress doors: June 2018:

- Rex buttons to comply with the following:
    - Allow enough time for the user to move from REX to door and open it.
    - The button operation requires a single button press and release and then door to be physically opened and not a continual button press and door to be manually opened at the same time.
    - Button is required to be green.
    - Any Rex more than 900mm and less than 1500mm away from an access-controlled door shall be clearly marked with a sign at the door indicating direction and location of the ReX; and
    - ReX' shall not exceed 1350mm above floor finish level.

8.9.2. Emergency Request to Exit (EMReX) buttons/ Emergency Door Release (EDR) Units

EDR units shall be flush mounted, where possible. On activation, a signal shall be sent to the local intelligent controllers. The operation of the unit is to be monitored by the local nurse station and also the security control room. At each break glass unit, provide an audible sounder that is operated when the Emergency Door Release (EDR) is operated and remains operable until the alarm is deactivated.

Where located on a secure egress door (i.e., card reader access in the direction of exit), the unit shall be fitted with an additional stopper cover, which emits a local audible sounder when lifted. Any additional stopper cover shall not affect the system operation or monitoring. The security contractor shall provide all details to the project manager, consultant, UoO, for approval prior to implementation.

Emergency Door Release (EDR) units shall be IP65 rated in external installations.

8.9.3. Fire safety requirements for Emergency Door Release (EDR) buttons

The following is required, in relation to Emergency Door Release (EDR)', to comply with the Code of Practice for Electromechanical Controlled Locking devices on Egress doors: June 2018:

- Cut the power supply to the lock and magnetic hold opens.
- The magnetic lock and magnetic hold open to remain in the fail-safe position till the Emergency Door Release (EDR)' have been manually re-set.
- Emergency Door Release (EDR)' changing NC state to NO state to another relay, who connected to a lock power in NC state, needs to be detailed in building consent application i.e. an Emergency Door Release (EDR) connected to the access control panel in NC state i.e. and monitored for circuit resistance change i.e. changing to NO state, needs the access control panel output to door lock power to also change from NC to NO state – this is not applicable to this design and will need to be issued by the installer if this is the methodology required;
- The Emergency Door Release (EDR)' must be green and clearly marked as an emergency device.
- The Emergency Door Release (EDR)' can be an additional input to an alarm panel i.e., to sound the door buzzer if activated, but not cause the EDR to malfunction.
- The Fire alarm relay shall not replace the Emergency Door Release (EDR). The Emergency Door Release (EDR) is still required even if the electromagnetic lock power supply feed is connected through a fire alarm relay.

- The Emergency Door Release (EDR)' may be protected by a cover that has a clear cover and is not lockable and has clear instructions to remove cover.
- The Emergency Door Release (EDR)' protected cover being Opaque/faded, shall allow for the covers to be replaced with minimal cost and time impact.
- Electromechanical lock operations will not avoid panic fastening to open the doors.
- No Emergency Door Release (EDR) is required when panic fastening is in place.
- Any Emergency Door Release (EDR) more than 900mm and less than 1500mm away from an access-controlled door shall be clearly marked with a sign at the door indicating direction and location of the Emergency Door Release (EDR); and
- Emergency Door Release (EDR)' shall not exceed 1350mm above floor finish level.

8.9.4. Access controlled doors fire detection system release schedule

The following schedule provides a template and example of fire system and emergency release interfacing detail, with the access control system, in relation to the magnetic hold opens and access-controlled doors, part of the emergency egress routes, which needs to be included by the Security Consultant and/or Security contractor prior to construction and as part of the Consent stage:

Door Number	Area	Magnetic Door Hold Open	Door Lock Type	Method of Release	Connected to the Fire Protection System relay?	Fail security / Fail safe functionality
###	###	Yes	Handle and push plate	Magnetic hold opens power supply is connected through fire relay and releases on fire signal	Yes	Fail safe
###	###	No	Electronic Mortise Lock	Fire relay is connected to access control panel which allow for the lock to be energised to allow for the door to be free handle to exit	Yes	Fail secure

Door Number	Area	Magnetic Door Hold Open	Door Lock Type	Method of Release	Connected to the Fire Protection System relay?	Fail security / Fail safe functionality
###	###	No	Electrical Striker Lock	Emergency door release button is connected as a closed loop circuit to access control panel. Activating the button will allow for the access control panel to energise the door lock to allow for free handle to exit	Yes	Fail safe

9. INSTALLATION AND MAINTENANCE REQUIREMENTS

9.1. Maintenance - General requirements

All maintenance performed on any component of the system must be recorded in the schedule kept onsite by the client.

The installer must carry out the maintenance routine as required by the manufacturer and record the maintenance in the schedule. The O&M manual shall be stored in a secure place with a register logging access and return of the manual by the technician.

Any onsite spares required to meet the ongoing system maintenance and support requirements shall be supplied as part of the project scope.

9.2. Commissioning requirements

9.2.1. Client Inspections

UoO's Proctor will nominate a representative which might make periodic inspections of the project in progress.

Upon completion of the project, UoO's nominated representative will perform a final inspection of the installed electronic security system. The final inspection will be performed to validate that the electronic security system is installed as defined in this specification, as detailed within scope of works document and drawing packages.

9.2.2. Manufacturer Inspections

Any system manufacturers shall undertake site inspections to level required to qualify the electronic security systems for a manufacturer warranty. Manufacturer inspections shall be considered part of the security contractor's project scope incurring no additional costs to the client. These inspections shall be arranged by the security contractor, notifying the project manager and security consultant of inspection dates and times.

Evidence is to be provided for all manufacturer inspections in the form of a declaration of conformance confirming compliance with respective manufacturer system requirements.

9.2.3. Testing and Commissioning

The electronic security system shall be commissioned in accordance with the manufacturer's instructions and client operational requirements. All commissioning shall be completed by personal trained in the setup and operation of the installed system.

Prior to sign off, the electronic security system shall be fully tested by the contractor to ensure the system is functioning as specified and as intended. System testing shall incorporate the following aspects at minimum:

- Review all work for completeness against wiring diagrams, as-builts and shop drawings. This included checks of all cable and component labelling.
- Visual check of all terminations and test the continuity of all connections and conductors in cables, prior to energising equipment.
- Test full system operation under mains failure, ensuring battery hold up and recharge times comply with specification requirements.
- Test each alarm input, card reader and output device for correct operation. These include the below at a minimum:
    - Each alarm initiating device.
    - Each card reader for valid, invalid and 'lost 'cards.
    - End of line supervision for each input.
    - Equipment tamper alarms.
    - All features and functions of the system as specified herein.
- Test the generations of system alerts and notifications, and the associated distribution to staff.
- Ensure the correct focusing and alignment of all cameras.
- Test all third-party system interfaces including but not limited to:
    - CCTV
    - Intercom
    - Lifts
    - Fire Evacuation
    - Lighting
    - Building Management Systems

A commissioning plan shall be submitted to the security consultant for review and approval prior to commissioning commencement. Full commissioning reports on system operation must be provided at practical completion and signed by contractor. A copy of this commissioning report must be left on site as part of the final documentation.

9.2.4. Training

Prior to handover of the electronic security system, the contractor shall undertake a full training session with the client's nominated staff.

The training session shall include at minimum:

- System overview and layout; inspection and explanation of each of the system components.
- Networks and transmission equipment overview.
- System operation and functionality.
- An overview of all features provided by the system.
- Basic maintenance and trouble shooting.

- Basic system adjustments.
- System pre-sets.
- Addition and removal of users (and key fobs) from the system.
- Setup and amendment of system schedules.
- System alerts and notifications.
- System reporting.

The contents and makeup of the training session shall be approved by the client prior to delivery to staff. All training material shall be included as part of the final documentation.

9.2.5. Practical Completion

This contract or installation shall be deemed complete at the date the main contract has been deemed practically complete. All testing, commissioning and readiness for normal operation shall be complete and the installation under this contract at this point shall be considered 'handed over' to the client and the defect free liability period shall commence.

9.2.6. Final Acceptance

Final completion shall mean the end of the defects liability period or when defects notified during the defect's liability period have been made good, whichever occurs last.

9.2.7. Documentation

For all work undertaken on site, the following shall be provided at a minimum to the project manager for review by a nominated client representative, prior to completion/client acceptance:

- Contractor and supplier contact details.
- Bill of materials listing the products and materials used, including manufacturer details and product codes.
- Details of all system licences and support entitlements.
- Full commissioning reports and system schedules detailing all controller interfaces.
- System testing report signed and dated by the contractor.
- As-Built drawings showing locations of all installed hardware and associated labelling.
- System schematic drawings.
- Time and date stamped digital photos of completed works covering installed cabling and equipment.
- Manufacturer's declaration of conformance and warranty certificates.
- Contractor sign-off letter detailing any associated installation warranty.
- Ongoing servicing and system maintenance requirements and details of any associated maintenance plan.
- System operation and training material.

All documentation shall be provided in both hard and soft copy format. A bound, type written hard copy shall be left onsite, available for onsite maintenance requirements. The soft copy shall be provided on a USB flash drive. As built drawings shall be provided in AutoCAD and in PDF format, or as otherwise agreed with the project manager.

This information shall be compiled and supplied to the project manager or nominated representative within two weeks of the practical completion of the works.

9.2.7.1. Shop Drawings and Product Technical Data

Technical data sheets and shop drawings shall be submitted by the successful contractor for review. This shall include a complete solution design and installation drawings, along with data sheets, performance specifications, test data and product samples:

- Requested for architectural approval.
- Required to implement the specified solution.
- That shall be reasonably requested by the project manager, architect or consultant detailing any work to be undertaken by other trades.

This required package of work shall be referred to as "Shop Drawings".

The contractor shall submit shop drawings along with a schedule detailing any/all deviations from the specification and design. Failure to comply with this requirement, shall result in the contactor being responsible for complete rectification to meet the design and specification at their cost regardless of whether a review has been carried out or not.

The contractor's submission shall present sufficient detail to allow verification that the proposed equipment and solution can be installed, maintained, operated, and modified to meet the system design requirements. The contractor shall ensure that they have made allowance for a fully functioning solution that has included the total site dimensions, any adjusted dimensions or actual dimensions that can reasonably be expected to be encountered onsite. All dimensions shall be metric. The solution shall allow for ease of serviceability, while maintaining security of all equipment supplied or installed. The contractor shall ensure that they coordinate with other trades, all design requirements, including finishes and material specified by other consultants including but not limited to lift, architectural, structural, mechanical, and electrical consultants.

Submitted technical data and shop drawings shall be submitted in the format required by the main contractor. All shop drawing submissions shall be reviewed within 15 working days of their receipt, unless otherwise specified and any adjustments required shall be identified using "clouds". All adjusted shop drawings shall be resubmitted as a clean new revision for review or acceptance.

9.2.7.2. Operation and Maintenance Manuals (O&M)

The contractor shall submit documentation to enable the client to operate and maintain all equipment deployed as a part of this contract. Documentation shall include any details allowing the client to make adjustments, alterations or additions to the supplied solution and shall have the ability to expand beyond the solution deployed.

All supplied documentation (written, pictorial, audio, or video) shall be in English. All material supporting the installed solution shall be succinct and written in a manner that allows the client's non-technical personnel to understand and use. The compilation of the manual shall be undertaken by a suitably qualified person, capable of detailing the overall systems architecture, operation, and any other required information to provide the client the ability to understand and operate the installed solution.

O&M manuals shall be submitted to the ICT/ELV consultant for approval prior to final acceptance.

9.2.7.3. As Built Drawings

Prior to practical completion, prepare and publish as-built documentation and manuals. Document the design as per NZCIC Construction Design phase requirements for Electrical Ancillary Services. Submit the documentation for review and approval.

As–built documentation shall be submitted to the ICT/ELV consultant for approval prior to final acceptance.

9.2.7.4. Maintenance Schedules

A maintenance schedule shall be provided detailing the manufacturer's maintenance routine and recommended system tests or activities to ensure optimal system performance.

The schedule will be required to ensure ESS inspection, maintenance and system reporting will be allowed for to meet Building Warrant of Fitness status.

9.3. Installation Requirements

9.3.1. In Scope

2. The supply, installation, commissioning, and documentation of an access control system including:
    a. Card readers.
    b. Request to exit buttons (ReX).

c. Emergency break glass/Emergency Request to Exit units (Emergency Door Release (EDR)).

d. Electronic locking hardware.

e. Security controllers, power supply units and battery backup supplies; and

f. SMS (Security Management Software) and server for the ACID (Access Control and Intruder Detection) system server,

3. The supply and installation of the duress systems and integration with the ACID
4. The supply, installation, commissioning, and documentation of internal and external IP Video Intercoms.
5. High level integration between the access control, CCTV, intercoms, RAS, PA systems and BMS
6. The supply, installation, commissioning, and documentation of ESMS, inside the both the Campus Distributors at 444 and 325.
7. The supply and installation of all internal building minor pathways including catenary wires, conduits, and flush boxes. This includes any precast conduits and flush boxes in precast AFS walls.
8. The supply of access control key fobs, access cards and wrist bands, in quantities as detailed in the ICT consultant's Design specification hardware schedule/Bill of materials.
9. The supply, installation, commissioning, and documentation of local security hardware in UoO facilities.
10. The supply and installation of major cable pathways (applicable to maintaining existing ESS).
11. The supply of any patch cords required by the ACS, IDS, Duress, or intercom systems in the Communications rooms (applicable to maintaining existing ESS).
12. The supply and installation of horizontal cabling for internal IP cameras or intercoms (applicable to maintaining existing ESS).
13. The supply and installation of any UPS to support the ACID, if it is an existing UPS are already installed by the security contractor and requires maintenance/replacement.
14. Access control integration with the fire evacuations system.
15. Supply and installation of any magnetic hold opens.
16. Access control integration with the lift system.

17. ACS integration with BMS
18. The supply and installation of data network backbone cabling intercoms (applicable to maintaining existing ESS).
19. The supply and installation of any underground pathway's intercoms (applicable to maintaining existing ESS).
20. The fire stopping of all major penetrations will be completed by a specialist 3rd party contractor intercom (applicable to maintaining existing ESS).

9.3.2. Out Of Scope

1. The supply, installation, and commissioning of any PoE network switches required by the access control or intercom.
2. The supply and installation of major cable pathways as defined in the Electrical Services Cable Access Layouts (applicable to new projects or renovation projects).
3. The supply of any penetrations through concrete floors, walls, or ceilings.
4. The supply and installation of the Communications Earth Terminals.
5. The supply and installation of any electrical socket or permanent connections required for the security system.
6. The supply and installation of horizontal cabling for internal IP cameras or intercoms (applicable to new projects or renovation projects).
7. The supply and installation of telecommunication outlets for the access controller Ethernet connectivity.
8. The supply of any patch cords required by the access control, Duress, or intercom systems in the Communications rooms (only applicable to new or renovation projects).
9. The supply and installation of any ICT cabinets for mounting of ESS headend equipment i.e., ACID server, etc.
10. The supply and installation of an IP phone system.
11. The supply and installation of any UPS to support the ACID, unless existing UPS are already installed by the security contractor and requires maintenance. The security contractor shall provide power consumption details to the data contractor to allow appropriate sizing of any ICT cabinet UPS.

12. The fire stopping of major fire cell penetrations will be completed by a specialist 3rd party contractor (applicable to new projects or renovation projects), but minor works it will be completed by the security contractor and also certified by the security contractor that the required fire cell separation fire stopping has been achieved and fire cello is maintained after the fire stopping has been applied.
13. The supply and installation of data network backbone cabling intercoms (applicable to new projects or renovation projects).
14. The supply and installation of any underground pathway's intercoms (applicable to new projects or renovation projects).

9.4. ESS Warranty Requirements

The system and hardware performance of any ESS shall comply with the associated suite of joint Australian & New Zealand standards.

Fundamentally the ESS and related infrastructure, shall be installed in a manner achieving a minimum of 5-year performance warranty, from the installed product vendor.

The warranty shall be facilitated by the contractor and will be established between UoO and the manufacturer directly.

The contractor shall maintain current certified installer status with the manufacturer meeting all training and onsite installation requirements for the duration of the project to ensure the provision of a minimum 5-year system performance warranty by the system manufacturer.

The abovementioned warranty excludes Generic Structured Cabling (Data cabling connecting ESS to the TCP IP network) and cabling systems (Data cabinets). These items are covered under UoO BTSS CHAPTER 3: IT Infrastructure – Generic Cabling Systems Standard.

The contractor must provide all licenses and warranties pertaining to hardware supplied. Register warranties in the name of the client with manufacturers as appropriate. Retain copies of warranty documentation delivered with components and equipment. Warranty periods shall commence at practical completion or at acceptance of installation if acceptance is not concurrent with practical completion.

Warranty documentation shall be submitted to the ICT/ELV consultant for approval prior to final acceptance.

9.5. Installation and Maintenance Defects Liability

The minimum defect liability period for any work under this contract shall be two years or 24 calendar months from the date of issue of a Practical Completion Certificate. Multi-staged projects shall have a practical completion certificate issued at the end of each stage and this shall mark the commencement of the defect free period. In the defect's liability period, 'maintenance' shall include the inspections, maintenance and reporting required for the BWoF process.

Rectification work, including replacement or making good shall include:

- Any damage caused during the installation or because of repairs that arise post hand over during the defect's liability period; and
- Any product defect that is uncovered post practical completion during the defect liability period.

Any repaired and/or replaced component shall be supported by new test results and documentation being furnished by the contractor for inclusion in the manual. These shall provide evidence that the replaced component has not impacted on the day-to-day operation of the system and that it is functioning to the original requirement and system deployed.

All warranties of replaced equipment during the defect's liability period shall have their warranty extended by a further 12 months and the contractor shall supply serial numbers and details to the client for inclusion in the manual.

Any component failure that is considered critical (e.g., prevents the overall solution from functioning) shall be repaired with 48 hours of written notification, any other non-critical component failure shall be rectified within 5 working days following written notification. Should the contractor fail to comply with the written request, the client reserves the right to engage a suitably qualified alternative contractor or supplier to complete the work without further notification and deduct the costs from any outstanding amount due or payable to the contractor. Should the costs be more than any outstanding amount then the client has the right to recover these costs from the original contractor. Any such action enforced due to lack of response by the contractor shall not impede any of the responsibilities required by this specification and associated designs.

The contractor shall maintain current certified installer status with the manufacturer including all training requirements, for the duration of the project. The contractor shall staff the installation crew with the appropriate number of trained personnel in accordance with the respective manufacturers' contract agreement.

The contractor shall be fully conversant and capable in the design, installation, and commissioning of security systems such as but not limited to:

- Electronic access control systems.

- Intrusion detection systems.
- Closed circuit television (CCTV) and video management systems (VMS).
- Intercom systems.

Only companies who have the following credentials shall be considered for this contract:

- Current channel partner or certified agent and installer of the proposed systems offered.
- Hold a current Company License under the Private Security Personnel and Private investigators Act.
- Use only staff members that hold current 'Certificates of Approval' under the Private Security Personnel and Private investigators Act.
- Use a technician with a minimum qualification of NZQA Level 3 – Electronic Security. There shall not be more than a ratio of one trainee/labourer per qualified technician.
- Use staff trained and certified in the design and installation of the chosen manufacturers' system; and
- The contractor shall have a local office and be able to provide onsite support and technical assistance within 2 hours of notification of a system fault.

The project manager and/or consultant reserves the right to conduct any enquiries it deems necessary with any supplier, manufacturer, or training provider in order to verify the validity of the current status of any qualification, certification and authorisation claimed by the contractor and/or employees of the company. Any person, including subcontractors or a contractor engaged by the company is deemed to be an employee of the company.

The accredited contractor is to provide photocopies or softcopies of the above items to the Project Manager as part of their tender response.

9.6. Site Restoration

The ESS contractor shall ensure that any required restoration work is completed to UoO's satisfaction onsite. This includes leaving work areas clean and tidy, regardless of what the previous area condition were. Any ambiguity relating to roles and responsibilities must be resolved with the UoO project manager before installation commences.

9.7. Battery Backup and Power Supplies Installation

Mount the power supplies and batteries as part of the security panels. Provide ventilation for the power supplies. Ensure that the batteries are seismically restrained and that the batteries cannot short onto any metal associated with the cabinet under earthquake conditions. The batteries shall be arranged on proprietary purpose-built non-corroding stands for easy access of any one cell without the need to disturb other cells.

Low battery, mains and system failures shall be connected as inputs to the access control system to be monitored by the security system.

9.8. General Cable Installation Practices

All cabling shall be installed in accordance with the following requirements:

- Cabling shall be installed in accordance with manufacturers' recommendations and best industry practices.
- Any minimum specified bending radius and maximum hauling tension for cabling shall be maintained at all times.
- Ensure segregation from low and high voltage cabling at all times in accordance with AS/NZS 3000 and specific manufacturer requirements.
- Cabling shall be concealed and make use of ceiling, wall, or floor voids at all times where this is possible.
- All cabling shall be supported at intervals no greater that one meter.
- Cables shall be kept away from extremes in temperature.
- All cables shall be correctly rated for the environment in which it is installed.
- No more than 24 cables shall be installed on any one catenary wire and security cabling shall not share catenary wires with any other services. Cables shall be secured at approximately 300mm intervals.
- Where installed within cable trays and baskets, cables are to be loosely strapped to the entry and exit of the tray/basket and at all directional changes.
- Any point where cabling exits a cable tray or cable basket, the cabling shall have protection from sharp edges fitted.
- Cables shall be installed in continuous lengths from origin to destination (no joins) unless specified otherwise.
- Cables shall be installed above fire-sprinkler and systems and shall not be attached to the system or any ancillary equipment or hardware. The cabling system and support hardware shall be installed so that it does not obscure any valves, fire alarm conduit, boxes, or other control devices.
- Cable tray and cable basket used for extra low voltage (ELV) cabling shall not be utilised for low voltage (LV) cabled services i.e., 230v/400v.
- Cables shall not be attached to ceiling grid or lighting support wires. Where light support for drop cable legs is required, the contractor shall install removable clips to support the cabling.

- Any cable damaged or exceeding recommended installation parameters during installation shall be replaced by the contractor prior to final acceptance at no cost to client.
- Cabling shall be installed and run perpendicular to the building axis.
- Where installed within framed walls, cabling shall drop vertically through wall cavities to the final location to allow for future servicing and cabling replacement.

All cabling utilised by the ESS shall be stranded copper unless otherwise stipulated by the manufacturer of the selected product.

Cabling installed for card readers shall meet the following requirements:

- All readers shall be wired with a dedicated cable.
- All reader cables shall be shielded and terminated within the control cabinet at one end and the screw terminals of the control logic board at the other end. The shield shall only be terminated at each control cabinet end.

Cabling installed for door hardware shall meet the following requirements:

- All monitoring devices and remote release shall be wired with cables of a minimum aggregate size of 1mm².
- All power to mortise locks shall be wired with cables of a minimum size of .75mm² twin.
- Each door monitoring cable shall be 8 core cable.
- All cable termination points at the doors shall be soldered and sleeved with clear heat shrink.
- All EOL termination points at field devices shall be soldered and sleeved with clear heat shrink.
- If magnetic door locks are used an 'auto-twin' cable must be run that is a minimum of 2mm². The auto-twin cable for every secured doorway is cabled back to the control cabinet for that zone.

9.9. Network Connections

Where the security LAN utilises RS485 protocol to communicate, the cabling shall be shielded Category 6 (S/STP) and a different colour to that used for the structured cabling system. LAN isolator shall be installed on all Master controllers.

Where the security LAN utilises Ethernet to communicate; the controllers Ethernet interface will be linked by the site's structured cabling infrastructure to a separate security Ethernet LAN. Cross connects will occur between the patch panel and the Ethernet switching infrastructure housed in the ICT cabinets/floor distributors inside telecommunication rooms.

9.10. Patch Cords

Refer to the UoO BTSS CHAPTER 3: IT Infrastructure – Generic Cabling Systems Standard, for patch cord details.

A APPENDIX A: Services Coordination

A.1 Table

1.1 Annexure A: Services Coordination

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
ACS (Access Control System)	ACS: Supply and install ACS hardware	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Architectural	Architectural: Confirm door locks with architect door schedule	☐	☒	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐
Architectural	Architectural: Comfirm card reader and camera colours, positions and set outs with architect	☐	☒	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
Architectural	Architectural: Comfirm card reader and camera colours, positions and set outs with architect	☐	☒	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐
CCTV	CCTV: Supply and install CCTV equipment	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Telecommunication Spaces	Telecommunication Spaces: Confirm and coordnate spacing with architect and UoO	☐	☒	☐	☐	☒	☐	☐	☐	☐	☐	☐	☒
Electrical	Power: Issue rack power load to electrical for UPS provision	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
Electrical	Power: Confirm security head end equipment power load with electrical contractor for UPS supply and installation	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Electrical	Power: Confirm power loads to electrical for locks and SCP PSU GPOs	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
GCS (Generic Cabling Systems)	GCS: Confirm SCP locations with data contractor for data cabling supply and installation	☐	☒	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
GCS (Generic Cabling Systems)	GCS: Confirm camera and SCP locations with data contractor for data cabling supply and install	☐	☒	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐
IDS (Intruder Detection System)	IDS: Supply and install IDS equipment	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Networking	Network: Supply and install UoO approved switches	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒
Networking	Networking: Supply networking requirements to UoO	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
Networking	Networking: Confirm IP address blocks with UoO for applicable service devices	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒
Networking	Networking: Confirm routing details and requirements for applicable service with UoO	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒
GCS (Generic Cabling Systems)	Patching: Comfirm ports with UoO to be patched	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
GCS (Generic Cabling Systems)	Patching: Supply patch leads (patch panel and device end)	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
GCS (Generic Cabling Systems)	Patching: Intall patch leads (patch panel and device end)	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐
Telecommunication Spaces	Racks: Confirm rack ID and location within rack for security head end equipment installation	☐	☒	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐
Telecommunication Spaces	Racks: Equipment rack weight to be issued for wall and floor reinforcement	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Reticulation	Reticulation: Supply and installation of cable trays	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
Reticulation	Reticulation: Supply and installtion of primary path under ground and above ground conduits and ducts	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Reticulation	Reticulation: Supply and installation of catenary and secondary path conduits	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Reticulation	Reticulation: Provide wall and floor penetration details to main contractor for implementation	☐	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
Reticulation	Reticulation: Provide wall and floor penetration details to main contractor for implementation	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Seismic restraining	Seismic restraining: Seismic restraining cable trays and primary overhead ducts	☒	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐
Seismic restraining	Seismic restraining: Seismic restraining equipment cabinets	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

SOW Category	SOW Details	Electrical Contr.	Security Contr.	Main Building Contr.	Generic Cabling Systems Contr.	Architect	Mech	Hydr	Fire prot.	Fire safety	Structural	Civil	UoO
Telecommunication Spaces	Telecommunication Spaces: Confirm and coordnate spacing with architect and UoO	☐	☒	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐
Telecommunication Spaces	Wall prep: Confirm cabinet sizing, weight and setouts with arch for wall preparation	☐	☒	☒	☐	☒	☐	☐	☐	☐	☐	☐	☐
		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

1.2 Annexure B: Statement of Coordination

The following statement of coordination is required, as per PN22, for electronic access-controlled doors, part of the fire egress routes:

The Design Coordination Statement is to be provided to the Building Consent Authority and is intended to accompany the documents submitted in the building consent application.

The Acceptable Solution Fire Report prepared by [FIRE ENGINEER DETAILS] titled [TITLE OF THE FIRE REPORT], Version [VERSION], dated [DATE], has been reviewed for egress requirements.

I believe on reasonable grounds that the 'relevant elements' of the fire safety summary and associated plans have been incorporated into the design of the electromechanical locking devices as described in this document and the design, and that this design ensures that the locking devices will comply with the building code requirements.

Signed:

[Designer]

[Date]