DOCUMENT CONTROL

Document Name	**UWA Design and Construction Standards: Security Services - F**
Document Status	Final version
Version No.	4.0
Date of Issue	1st October 2023
Endorsement Body	To be determined
Owner	Director, Campus Management
Author(s)	The Standards have been developed by Campus Management with the assistance of UWA staff, external consultants, contractors and colleagues from other education institutions.
Contact Person	Associate Director Capital Projects, Campus Management

COPYRIGHT

This document is the property of The University of Western Australia and may not be copied as a whole or in part without the approval in writing of the Associate Director Capital Works, Campus Management.

Table of Contents

1 Introduction

1.1 PURPOSE

The *UWA Design and Construction Standards* (the *Standards*) outline UWA's expectations for its built forms in order to achieve consistency in the quality of the design and construction of those built forms. They are aligned with the *UWA's Campus MasterPlan 2020* planning principles and UWA's requisites for aesthetic appeal, maintainability and environmental sustainability, while ensuring that there is sufficient scope for innovation and technological advancements to be explored within each project.

The Standards are intended for use by any parties who may be involved in the planning, design and construction of UWA facilities. This includes external consultants and contractors, UWA planners, designers and project managers as well as School and office staff who may be involved in the planning, design, maintenance or refurbishment of facilities. These Standards also provide facility managers, maintenance contractors and other service providers with an understanding of UWA services in order to assist in the maintenance and operation of facilities.

1.2 SERVICES

The UWA *Design and Construction Standards for* ***Security Services*** (this document) are a part of *UWA Design and Construction Standards* set of documents (the Standards). The Standards are divided into the following service documents for ease of use, but must be considered in its entirety, regardless of specific discipline or responsibilities:

A	Building and Architecture
B	Mechanical Services
C	Electrical Services
D	Communication Services
E	Hydraulic Services
F	**Security Services (this document)**
G	Fire Services and Fire Safety Engineering
H	Structural Works
I	Civil Works
J	Irrigation Services
K	Sustainability
L	Vertical Transport

1.3 RELATED DOCUMENTS

1.3.1 University Documents

The Standards are to be read in conjunction with the following relevant University documents:

- UWA General Preliminaries Document
- UWA Specification for As-Constructed Documentation
- Relevant UWA planning and policy documents such as the *UWA Campus MasterPlan* and associated documents related to Cultural Heritage, Landscape, Environmental Sustainability, Infrastructure and Space Policy
- Relevant UWA operational and maintenance documents such as preferred vendors lists, room data sheets, operational and maintenance manuals, etc.
- Other documents as referenced within the *UWA Design and Construction Standards*.

1.3.2 Relevant Legislation

The planning, design and construction of each UWA facility must fully comply with current relevant legislation, including but not limited to:

- Relevant Australian or Australian / New Zealand Standards (AS/NZS),
- National Construction Code (NCC),
- Occupational Safety and Health (OSH) legislation,
- Disability Discrimination Act (DDA),
- Accessibility Aspiration Design Factors,
- Local Electricity Supply Authority Regulations, and
- Local council and authority requirements.

1.3.3 Manufacturer Specifications and Data Sheets

All installation must be carried out in accordance with manufacturer specifications and data sheets to ensure product performance over its intended life and so as not to invalidate any warranties.

1.3.4 Project Specific Documentation

Requirements specific to a particular project, campus or other variable, will be covered by project specific documentation, such as client briefs, specifications and drawings. These Standards will supplement any such project specific documentation.

The Standards do not take precedence over any contract document, although they will typically be cross-

referenced in such documentation.

Extracts from the Standards may be incorporated in specifications, however it must remain the consultant's and contractor's responsibility to fully investigate the needs of the University and produce designs and documents that are entirely 'fit for purpose' and which meet the 'intent' of the project brief.

1.4 DISCREPANCIES

The Standards outline the University's generic requirements above and beyond the above mentioned legislation. Where the Standards outline a higher standard than within the relevant legislation, the Standards will take precedence.

If any discrepancies are found between any relevant legislation, the Standards and project specific documentation, these discrepancies should be highlighted in writing to the Associate Director Capital Projects, Campus Management.

1.5 DEPARTURES

The intent of the Standards is to achieve consistency in the quality of the design and construction of the University's built forms. However, consultants and contractors are expected to propose 'best practice / state of the art' construction techniques, and introduce technological changes that support pragmatic, innovative design.

In recognition of this, any departures from relevant legislation, or the Standards, if allowed, must be confirmed in writing by the Associate Director Capital Projects, Campus Management.

Any departures made without such written confirmation shall be rectified at no cost to UWA.

1.6 PROFESSIONAL SERVICES

For all works, it is expected that suitably qualified and experienced professionals are engaged to interpret and apply these Standards to UWA projects. Works cannot be carried out by unqualified and unlicensed consultants or contractors.

Campus Management (CM) administer the online contractor safety induction. All consultants and contractors working at UWA will have to obtain an Authority to Work. Operations and Maintenance (Contractor Compliance) within CM administers the Authority to Work process via Rapid Global.

1.7 STRUCTURE OF DOCUMENT

This document is structured into 4 parts:

Part 1 Introduction (this Section)

Part 2 General Requirements – outlines the general requirements or design philosophies adopted at UWA

Part 3 Checklist for project team (if applicable) – checklist of items for consideration at various stages of a project

Part 4 Specifications (if applicable) – materials specifications and/or preferred lists for materials, processes or equipment used by UWA.

1.8 DEFINITIONS

For the purpose of this document, the following definitions apply:

Can: Implies a capability of possibility and refers to the ability of the user of the document, or to a possibility that is available or might occur.

May: Indicates the existence of an option.

Shall: Indicates that a statement is mandatory.

Should: Indicates a recommendation.

2 General Requirements

2.1 PREFERRED SECURITY CONTRACTORS (PSC)

Any security works required for the installation or modification of security systems at UWA shall occur by a short list of UWA PSC. The current PSC list may be obtained from Campus Management.

The PSC shall:

- Be a Gallagher Channel Partner who is authorised and qualified to install, programme, commission and maintain the Gallagher systems.
- Have several qualified installers with the required ACA and/or electrical licences and a Gallagher accredited training certificate.
- Have several qualified installers with the required ACA and/or electrical licences and the Avigilon training to work with the UWA Video Surveillance System (VSS).
- Comply with all relevant UWA processes and procedures in the delivery of their works.
- Have qualified and licensed WA Security Agents, Consultants, Technicians and Installers in accordance with the Security and Related Activities (Controls) Act.
- Comply with all statutes, regulations and by-laws relating to the protection of the environment.
- Carry out the work under the contract in such a manner that the security of the premises is maintained at all times.
- Supply, cut in and install the locking hardware devices to complete the project requirement except where otherwise stated.

2.2 DESIGN REQUIREMENTS AND TECHNICAL PRINCIPLES

2.2.1 General

The operational design and control of the electronic security system will be determined in liaison with UWA Security and the appropriate School or stakeholders.

The security design should be based on a Security Risk Assessment in accordance with *HB 167:2006 Security Risk Management*.

The Security System shall provide a building auto lock-down feature at close of business each day and shall monitor the status of the buildings perimeter after hours. All building time schedules are to be verified on a building-by-building basis.

The electronic security systems shall be capable of performing the following functions:

- Access Control
- Intruder Alarm
- Alarm Monitoring and Management

- Systems Interfacing

Building main entry doors shall be kept to a minimum, preferably one location only per building. Main-entry doors should be automatic sliding doors, including electronical access control. All building perimeter doors shall include electronic access control.

Fire escape doors which are used to exit a building, must have an audible (low level) door held open alarm.

Doors in exit paths may have Hold Open devices to fix the doors in an open position and allow the free flow of traffic during normal hours.

Access to sensitive areas (e.g., animal laboratories) and hazardous areas (e.g., laser, biochemistry, radiation and pathology laboratories) must be strictly controlled by the use of Electronic Access Control.

The cardholder management for access control is the responsibility of the School or Section occupying the building or area.

2.2.2 Security Principles and Design Philosophy

The ESS shall enable the efficient and effective operation of UWA facilities and must be designed to operate in a manner that supports the facilities operational management approach and philosophy.

The following security principles and design philosophy shall be applied during the design and construction of new buildings and facilities:

- The UWA Security Standards, as outlined within this document.
- The defined practices, policy and procedures that support the operational security of the buildings and facilities.
- The functions and duties to be carried out from the security control room.
- The security controls required to manage movement between various precinct, and security areas across the campus environment.
- Application of Security in Depth principles to enable the School or Section to effectively Deter, Detect, Delay, Monitor and actively Respond to any security incident or emergency event.
- The principles of Crime Prevention Through Environmental Design (CPTED).
- Implementation of a risk management-based approach to ensure that known security risks and threats are actively identified, assessed, and effectively treated.

2.2.2.1 Security Design Guiding Principles

Overview

The ESS to be installed as part of the new buildings and facilities shall be capable of integration into the existing UWA security platforms, and as such the design, structure, configuration, and hardware selection for the ESS to be installed shall comply with the following Guiding Principles:

1. Based on a fully integrated ESS solution with layered architecture.
2. Communicate using the UWA LAN supporting all ESS hardware.
3. The ESS and all subsystems shall be built on an 'Open Platform' as far practicable.
4. The ESS and all subsystems shall be 'Vendor Agnostic' to the greatest extent possible.
5. The ESS design shall support redundancy and resilience across all systems the maximum extent possible and to facilitate future expansion.
6. Security sub-system hardware platforms, such as Controllers, DGPs (Data Gathering Point), etc. should be non-proprietary, independent of the manufacturer headend software wherever possible.
7. All security sub-systems must be capable of local, redundant, operation independent of the system headend.
8. The ESS design shall provide a flexible platform to facilitate future systems' migration and interface to the system headend.
9. Existing systems or equipment shall be integrated into or transitioned to the new ESS infrastructure wherever possible, rather than expanding aging or outdated infrastructure.
10. Systems' specifications shall be based on functional performance reflective of the *UWA Approved Equipment List (Section 4.1)*.
11. All systems shall be software based, running on generic Commercial Off-The-Shelf (COTS) hardware, rather than proprietary hardware, where practicable with specific lead times or availability in WA.
12. All system interfaces to the ESS shall be High Level Interfaces (HLIs), employing a Flat Interfacing Architecture without intermediate subsystems, where achievable.
13. ESS selection must include a mature distribution network, with local support and training programs in place for:
    - Approved supply and distribution network for support of the product.
    - Certified installer and maintenance provider program.
    - Certified training and support program.
    - Lifecycle replacement and ongoing maintenance support.

Security Communications Network (SCN)

The ESS shall utilise the UWA Local Area Network (LAN) to support all ESS installed equipment.

UWA security systems are configured onto the UWA LAN using Security Group Tags (SGT's). For Campus Management there are two (2) SGT's, these being:

- sda_devices_cm_bms – this group is used for all Building Management System (BMS) devices
- sda_devices_cm_security – this group is used for all VSS & security devices

All new security devices that are to be connected to UWA network are to be coordinated with UWA UniIT for approval by the Network Administrator.

All new security devices that are to be installed within the communications racks are to be coordinated with UWA UniIT for approval by the Network Business as Usual (BAU) Manager.

All configuration and connection of security equipment to the UWA LAN shall be completed by preferred communication services contractor as per UWA preferred contractors list.

Refer to *UWA Design and Construction Standards – Communications Services* for design criteria related to the UWA LAN.

Vendor Agnostic Systems, Non-Proprietary, Systems & Support

All ESS shall be 'Vendor Agnostic' in that they may be sourced, installed, and maintained, by multiple, unrelated vendors. This is to facilitate a competitive procurement process, as well as competitive ongoing support and maintenance for the installed systems.

The ESS shall have a mature distribution and support program in operation, with a 3x appropriately trained and certified, licensed Security Integrators / Organizations, local to WA, who are certified by the system manufacturer to supply, install and maintain the system.

The program must support market competition for the lifecycle support and maintenance of the product and minimise the risk of non-competitive supply chains / system support. Evidence of distribution and support program, including a list of trained and certified Security Integrators within WA with demonstrated experience shall be provided to UWA.

Open Platform Systems

The electronic systems shall be based on 'open standards' and 'protocols.

All ESS shall be built on an 'Open Platform' so that HLIs can be easily developed and supported to integrate the separate security sub-systems.

Non-Proprietary Equipment

The ESS shall make maximum use of non-proprietary equipment, where suitable equipment is available in the

Australian marketplace and can be supplied and supported by multiple service providers.

Systems and equipment supplied under these works must be non-proprietary, common platform system.

Lifecycle Replacement & Maintenance

The ESS shall allow for flexibility in the procurement of ongoing maintenance and support for its full lifecycle. This shall include the ability to obtain preventative, reactive/corrective and or comprehensive maintenance from multiple services providers, including but not limited to ongoing support from the manufacturer.

Facilitation of Future Systems' Migration

All ESS shall be selected and designed in a manner to facilitate future systems migration. These include considerations for remaining serviceable life, product life cycle and systems architecture.

This is specifically relevant for ESS to be installed within existing buildings and facilities.

Integrating Existing Systems into New Systems

Taking into consideration existing systems' serviceable life and product life cycle factors, all existing systems shall be integrated into or transitioned to the current ESS infrastructure wherever possible, rather than expanding aging or outdated infrastructure.

That is, existing systems shall be modified, or upgraded, to enable them to be integrated with the current ESS, rather than 'dumbing down' the new systems to integrate with the existing.

Server Virtualisation (Software versus Hardware)

In as far as it is achievable, all ESS head-end systems shall be software-based running on COTS servers, rather than proprietary hardware-based or standalone solutions.

Multiple physical servers shall be 'virtualised' to operate on a single Virtualised Server Environment (VSE) and to avoid the need for installation of multiple or separate server hardware platforms. Virtual server solutions shall be provided to maximize system resilience and redundancy and minimise proprietary hardware platforms.

Proprietary hardware / server configurations shall be kept to a minimum where possible. Any existing ESS required to be upgrade or expanded as part of new installation works shall be virtualised and migrated to the new site-wide VSE.

Systems/Network Redundancy/Resilience and Spare Capacity

The design shall provide sufficient head-end systems' redundancy, network redundancy, and spare capacity, to ensure that the complete ESS solution is resilient and has provision for future expansion.

The design of all ESS must consider redundancy and resilience in the security communications and support infrastructure, including power supplies, communications paths, and hardware redundancy such that single

points of systems and services failure are otherwise avoided where practical to do so and the systems are able to be available for 24/7/365 operation.

Performance Based Specifications & Proven Technology

The selection of ESS and equipment shall be based on performance requirements, rather than a specific make or model, although specifications will be based on pre-approved systems or products as noted in *Approved Equipment List (Section 4.1)*.

Proven Technology

Where UWA has a preferred or proven security system, the procurement methodology shall allow for tenderers to offer alternatives that meet the Performance Specifications provided that the performance quality and standard can be satisfactorily demonstrated e.g., live test or shoot-out. This will enable UWA to make an informed decision whether to select the specified or alternative equipment, based on actual performance.

Where existing proven technology is installed onsite, preference should be given to match existing equipment make/model for consistency of service maintenance and operation.

Specified Products

Where reference is made to a specific brand, make or model number, this reference shall be used as a minimum benchmark for product performance, quality, functionality, design, and fitness for purpose.

Alternate items may be offered as an equivalent, provided that the above criteria are met, and the performance can be satisfactorily demonstrated.

Full details of any proposed alternatives and sufficient information, live testing, etc. to satisfactory demonstrate that any alternative equivalent is better in quality and performance, as well as technical specifications, shall be provided.

2.2.2.2 Engage in collaborative design process

While this document sets out the proposed technical requirements for the ESS to be provided as part of a new development or refurbishment it must be recognised that it will have unique functional, operational and design requirements. It is therefore required that the Security Consultant engage in a collaborative design process with:

- Client designated representatives
- The designated project manager.
- The lead design consultant.
- Other engineering design consultants, i.e., electrical, and mechanical.
- Other specialist consultants, i.e., fire engineer, Building Code Assessment (BCA) Consultant, Environmentally Sustainable Design (ESD) Consultant and the like.

2.2.2.3 Services Coordination

The design of the ESS is to be coordinated with Architectural and other Engineering Services, this shall include:

- The size and location of Security Equipment Rooms and equipment rooms and plantrooms for other services.
- The route for distribution of services across the facility to maximise the use of common services trenching and avoid services clashes.
- The route for distribution of services within each building to maximise the use of common services infrastructure and avoid services clashes.
- The location and layout of equipment to ensure:
    - Equipment is collocated as required.
    - Equipment is located considering the Architectural layout construction methodology.
- The interface between the ESS and other Engineering Services.

2.2.2.4 No Remote Access

The ESS for UWA buildings and facilities shall be interconnected across the UWA LAN and shall not provide any means for remote access to the ESS.

2.2.2.5 Durability and Design Life

The ESS shall have adequate durability to achieve a normal industry standard design life, without requiring undue maintenance. The systems and equipment should also:

- Be the current and supported versions for each system.
- Have a life span of a minimum of 10 years supported by an established development program.
- Be based on use of open protocols that allow interface between systems
- Operate on the latest currently available and supported operating systems.

All associated cabling and power systems shall be designed for minimum design life of 20 years. Minimum design life for any batteries associated with the system shall be 5 years.

2.2.2.6 Redundancy & Resilience Across System

ESS design and supporting shall be based on “enterprise level” design principle.

Redundancy measures shall allow systems and equipment to continue to function and remain operational for use despite individual failures in system hardware and software. This shall include the elimination to the greatest extent possible of single points or single systems of failure at the core systems level.

The electronic security systems will include appropriate redundancy measures to all systems and equipment to ensure the facility can function in a 24-hour campus environment. Redundancy measures may include practices such as:

- Virtual servers and processing.
- Redundant servers.
- Watchdog monitoring software and auto-changeover systems.
- Redundant network design.

Redundancy and resilience shall also include:

- Security equipment installed within communications rooms that are to be sized to accommodate current and future capacity, and to enable seamless upgrade or replacement of systems in parallel with the existing.
- Be incorporated into the design of ESS support infrastructure, such as:
    - Uninterruptible Power Supply (UPS) power supply at main equipment locations.
    - Dedicated, clean air-conditioned communications rooms.
    - Battery back-up power.
- Redundant, virtualised severs with high availability.
- Distributed System Architecture
- Embedded system health monitoring and self-reporting of all ESS faults.

2.2.2.7 ESS Communications Network – Ethernet (TCP/IP)

All ESS shall include Ethernet (TCP/IP) based communications and be provided via the UWA LAN.

Communications between local field equipment and field / end devices shall also, to the greatest extent possible, be TCP/IP based communications (i.e., where supported by the system manufacturer). This shall utilise a certified structured cabling systems and support use of field terminated Cat-6 RJ-45 for direct connection of security field devices, i.e., no outlets required in field or at end devices.

2.2.2.8 Systems Assurance & Health Monitoring

System assurance and health monitoring shall be imbedded throughout the ESS.

The ESS must self-monitor the health and status of all its systems with automated fault diagnosis, monitoring and reporting of all system components. The ESS assurance and health monitoring functions must regularly pole and test all its components, systems and communications interfaces for correct operation and automatically report any loss of operation, system error or fault.

The assurance / health monitoring must provide proactive detection, monitoring and reporting of system faults to protect against loss of operation or system failure due to a fault or error not having been identified. The

monitoring function must clearly log, identify, and annunciate any system faults to the user and include a real-time reporting function for integration with the ESS reporting engine.

2.2.2.9 System Flexibility, Capacity, and Future Planning

The security services must, to the maximum practical extent, be designed for flexibility and adaptability for future upgrades and expansions. The design must allow for changes to the new building or facility or the services with minimal disruption to the operation of the building or facility and at a minimum cost.

Equipment distribution, capacity and spatial planning shall allow for future expansion of the ESS without the need for building expansion, system redundancy, or service interruption throughout the systems lifecycles.

Spare capacity must be provided to both installed spare system capacity (e.g., bandwidth, slots, inputs, licenses, and the like), and spare physical space for additional components, wiring, conduits, panels, room within racks and the like. A 20% spare capacity is generally acceptable across the ESS and equipment.

Installed spare system capacity must be installed at the time of construction and available for immediate use without any requirement for additional equipment, apart from the stipulated field components.

Future Planning

All services reticulation routes from equipment locations, i.e., equipment rooms, to field equipment and all areas of each building shall provide access for distribution of future services.

Provide for the following provision of space for future expansion:

- All incoming and outgoing cabling infrastructure to a building or area must be able to accommodate future expansion.
- All internal building infrastructure for distribution of cabling including services risers, cable trays, and the like must allow for future expansion.
- All equipment racks, cabinets, enclosures, and panels must allow for future expansion.
- All security services rooms and cupboards must have space for future expansion.

Maintainability

The ESS shall be designed to allow maintenance activity to all equipment to be carried out without significant disruption to existing systems equipment. Particular attention shall be given to ensuring the accessibility and serviceability of all equipment, including the systems equipment shall be installed in areas such as communications rooms and no equipment shall be installed in ceiling spaces, electrical and mechanical plantrooms or other areas that are difficult to access.

Equipment shall also be laid out in equipment racks and equipment panels and the like to provide a logical layout of equipment and be consistent across the facility.

The system shall be designed such that in the event of refurbishment / maintenance works, the main system

equipment and distributed control equipment in other areas remain fully operational.

2.2.2.10 Local Environmental Conditions

All ESS equipment installed shall take into account local environmental conditions for new buildings and facilities.

Pending the locality, new buildings and facilities may be subject to a number of environmental conditions and factors that will require specific design solutions to be implemented to address the impact that these elements have in:

- Reducing the effective life cycle of the systems and / or equipment.
- Requirement for higher than usual routine maintenance.
- Damage that would require extensive breakdown repair service.

The environmental conditions and factors include:

- Heat and humidity
- Cyclonic conditions
- Heavy seasonal rainfall
- Lightning
- Soil conditions
- Dust and particulates

2.2.3 Overview of Security Systems

This section describes the security system technologies that are used throughout UWA. These technologies assist in mitigating security and safety related risks whilst supporting the management of security operations. The UWA security systems include:

- Security Management System (SMS)
- Electronic Access Control System (EACS)
- Intrusion Detection System (IDS)
- Video Management System (VSS)
- Intercom System
- Automatic Barriers
- Electronic Key Management Systems (EKMS)
- Wired/Wireless Duress Systems

2.2.3.1 Security Management System

The Security Management System (SMS) provides the overall management of alarms and the Graphical User Interface (GUI) that the security operators use for the management and control of the above systems.

To enable all systems to be fully integrated, the SMS and associated systems communicate over the UWA Local Area Network (LAN).

2.2.3.2 Electronic Access Control System

The Electronic Access Control System (EACS) is an integral component of the SMS to assist in the control and monitoring of authorised access through nominated doors and barriers. Restricted areas will be controlled by card readers and unlocked with authorised access cards.

The EACS will monitor nominated doors for attempted unauthorized entry, forced door, door ajar and other alarms and report these to the SMS for logging and alarm notification.

The EACS will also monitor the status of all doors connected to the system and tamper alarms as fitted to vulnerable control equipment and remote panels. In the event of an alarm or tamper, the EACS will report this status to the SMS which will be displayed on SMS workstations.

The EACS will be interfaced to the Fire Alarm System to automatically unlock nominated fire doors in the event of a building fire alarm.

2.2.3.3 Intrusion Detection System

The Intrusion Detection System (IDS) will be installed as an integral component of the SMS to ensure a fully compatible and cost effective solution is configured. The IDS shall provide all necessary interfaces to manage the arming and disarming of detection devices.

The primary purpose of the IDS is to monitor the building for detection of the varying forms of breaches including:

- Forced entry at perimeter and selected internal doors
- Forced entry to equipment enclosures and panels
- Monitoring of systems cabling to detect any unauthorised tampering
- Activation/de-activation of individual alarm zones by way of keypad devices (or combined card reader and keypad devices)
- Monitoring of detection devices include but are not limited to:
    - Recessed door contacts (reed switches)
    - Duress buttons
    - Movement detection devices (PIR's and VSS VMD)
    - Inputs from other systems (e.g. fire alarm panel outputs).

The IDS will be configured within the SMS to facilitate the monitoring of all spaces within the building and to initiate responses, with priority given to life threatening situations.

2.2.3.4 Video Surveillance System (VSS)

The Video Surveillance System (VSS) will be implemented to provide coverage of the following areas:

- Main vehicle entry/exit points
- External areas of buildings
- Building entry/exit points
- Internal building spaces used after hours (including foyers and main corridors within buildings)
- High risk/value areas
- Additional areas as identified in consultation with end users

The VSS will be designed to assist in identifying persons at key access points, verifying alarms, detecting suspicious behaviour and assisting in post incident investigations.

The VSS comprises the following components:

- Fixed VSS cameras
- Pan Tilt Zoom (PTZ) cameras
- Network Video Recorders (NVR's)
- VSS Workstation software
- Display Monitors

The VSS design will be based on using a majority of fixed cameras with a limited number of PTZ cameras to support security operations.

VSS Coverage Functions and Objectives

Camera function and views shall be generally provided in accordance with the table below as based on AS/NZS 62676.4. This table is based on a camera viewing a 1.8 metre person standing at the location of the primary point of the camera view.

FUNCTION	DENOTED AS	DESCRIPTION
Observation	O	To enable characteristic details of an individual, such as distinctive clothing to be seen, whilst allowing a view of activity surrounding an incident. Image height = 25% of field of view
Recognition	R	To enable the operator to determine with a high degree of certainty whether or not an individual shown is the same as someone they have seen before. Image height = 50% of field of view.
Identification	I	To enable identification of an individual beyond reasonable doubt. Image height = 100% of field of view.

The key VSS coverage areas shall be as follows:

COVERAGE	AREA / LOCATION	TARGET SPEED	OBJECTIVE
Observe	All vehicle entry points	0-20km/h	Observe and provide description of vehicle occupants
	Building Perimeter coverage	Walking Speed	Observe and provide description of pedestrians on building perimeter
	General Sitewide coverage	Pedestrians - Walking Speed Vehicles - 0-20km/h	Observe and provide description of pedestrians and vehicles within general campus areas such as carparks, forecourts, external grounds of campus etc.
Recognise	Building Internal areas	Walking Speed	Identify and provide description of occupants within building common areas such as inside libraries, external to lecture theatres, building lobbies, lifts and lift lobbies.
Identify	Building perimeter entry/exit points (including emergency exits)	Walking Speed	Clear recognition of staff, students and visitors entering and existing building perimeter points
	Help Call Point Locations	Walking Speed	Clear recognition of staff, students and visitors using a Help Call Point
	Specialist / Restricted Spaces (i.e. labs)	Walking Speed	Clear recognition of staff, students and visitors entering and existing the specialist or restricted space. Exact application of VSS coverage is to be determined based on the use of the specialist space.
	Communications Rooms and Data Centres	Walking Speed	Clear recognition of staff and maintenance personal entering Communications Rooms and Data Centres
	Plant Rooms	Walking Speed	Clear recognition of staff and maintenance personal entering Plant Rooms

All cameras will be recorded on Network Video Recorders at high resolution and retained for a minimum period of thirty-five (35) days. The VSS system is interfaced to the SMS to allow VSS footage to be automatically displayed on an alarm monitor in the event of an SMS alarm and/or event.

2.2.3.5 Intercom System (Help Call Points)

Intercoms (Help Call Points) shall be implemented at strategic locations to provide intercommunications between the public (staff, students, visitors and contractors) and the UWA Security Control Room.

All new Help Call Point intercoms shall be Avigilon H4 Video Intercoms.

Existing analogue Jacques Help Point Intercoms shall be retrofitted with an Analogue-to-IP convertor to allow intercoms to communicate via the UWA LAN. Intercoms shall be configured to utilise Microsoft Teams to make calls.

When activated the intercoms shall dial the security emergency number to call the Security Control Room phones for response, and the control room able to open gates remotely via Gallagher.

Help Call Points are to be located in areas where students are expected to be after hours (i.e. areas where student access is anticipated 24/7).

Help Call Points must be located along Walk safe routes with adequate lighting. A Detection level of VSS coverage shall be provided on routes to the Help Call Point.

A VSS camera shall be installed within the vicinity of the Help Call Point to provide Identification level VSS coverage.

2.2.3.6 Intercom System

All new standalone intercoms shall be Avigilon H4 Video Intercoms to provide clear voice communication and/or video transmission the Avigilon Client on a workstation within the select area. The type and model shall suit the environment and the intended use as required by the project.

These intercoms are usually used for standalone operation to a specific building or area to enable a door to be unlocked from the Avigilon Client (where available), or to the Security Control Room phones / Avigilon Client workstation, to enable unlocking of doors or gates remotely via Gallagher.

2.2.3.7 Automatic Barriers

Automatic barriers (including vehicle and pedestrian barriers) will be implemented for a variety of reasons, including but not limited to:

- Avoiding unauthorised vehicle access
- Enabling high throughput access
- Providing suitable access for people with disabilities.

Automatic barriers will generally be required to interface with the EACS so that they can be automatically locked/unlocked and controlled by local card readers.

Automatic barriers include:

- Vehicle Bollards
- Boom gates
- Bio airlocks

2.2.4 Security Zones

To ensure security services are applied in a consistent manner throughout UWA, a standard approach to security technologies must be applied. Although each building/area will have its own unique security risks, the security measures identified in this section shall be applied as a minimum.

2.2.4.1 Zone 1A - Public Space (external to buildings)

These areas include external landscape areas, external roads, driveways, car parks and paths etc., where little, if any, control or security can be enforced due to the open nature.

To assist in the security operations of these areas, general VSS surveillance and recording shall be provided, along with strategically located help call points (intercoms). Although 100% VSS coverage of these spaces is not feasible, VSS coverage of key walkways, car parks and campus entry/exit vehicle and pedestrian ways shall be provided.

The application of Crime Prevention Through Environmental Design (CPTED) principles shall be adopted to assist in reducing anti-social behaviour wherever possible.

The level of lighting for all public spaces shall be of a level to provide for the safe and secure passage of vehicles and pedestrians at all times. Lighting for VSS shall be designed in coordination with lighting designers to ensure light levels are appropriate for the effective operation of the VSS within internal and external areas.

The landscaping is to be such that it minimises hiding places or obstructs views of the buildings' perimeter by natural surveillance or VSS.

Refer the following table for the minimum security controls to be applied to Zone 1A Public Space (external).

SECURTY ZONE	EXAMPLE SPACES/BUILDINGS	MINIMUM SECURITY CONTROLS TO BE APPLIED
Public Space (External)	• Internal roadways • Open air carparks • Public Circulation spaces external to buildings	**VSS** Coverage for Observation to external areas Coverage for Detection Level at all Help Call Points Licence Plate Recognition (LPR) for carpark entrances (applied on a project-by-project basis) **Help Call Points**

SECURTY ZONE	EXAMPLE SPACES/BUILDINGS	MINIMUM SECURITY CONTROLS TO BE APPLIED
		All walk-safe areas and congregation areas **EACS** Card readers and boom gates for restricted area carparks (applied on a project-by-project basis)

2.2.4.2 Zone 1B- Public Spaces (Internal to buildings)

These areas include building entry foyers and all other spaces accessible to the public during normal opening hours. These spaces shall be designed so that the building can be automatically secured after hours. After-hours access shall be available through main entry doors, via an authorised access card.

Building perimeter doors shall be configured to meet the intended entry/exit requirements. Typically, perimeter doors can be categorised as:

- Main entry/exit door - these are generally automatic sliding doors leading to a main building foyer
- Emergency egress door - provides free handle egress from a building structure with no external access
- General access door - unlocked from both sides during normal opening hours and secure from the outside after-hours
- Restricted access door - secure from the outside at all times.

If after-hours access is required through a perimeter door that provides access into a public space, then the door shall be provided with an external card reader. Access via key shall be limited.

Other than the main entry automatic sliding door(s), all perimeter doors shall be configured so that they can be automatically locked from the outside whilst providing free handle egress. These doors shall remain locked from the outside (fail-secure) in the event of a building fire alarm, providing access via key override only.

Where toilet facility doors are located on a building perimeter, they shall be provided with electronic access control to restrict public access after-hours.

VSS coverage in these areas shall include:

- Identification at all building entry points including main entry points and fire stairs
- General VSS surveillance shall be provided to spaces that are accessible by staff and students.

The objective of VSS in these spaces is to have a facial record of all persons entering the building and the ability to identify their movements once inside the building via general observation camera coverage.

Any area that is accessible by students 24/7 shall be provided with general VSS surveillance.

Refer the table below for the minimum security controls to be applied to Zone 1B Public Space (internal).

SECURTY ZONE	EXAMPLE SPACES/BUILDINGS	MINIMUM SECURITY CONTROLS TO BE APPLIED
Public Space (Internal)	• Administration office (public/student facing) i.e. student services area, student hub • Cafes, cafeteria's and food services areas • Tavern • Amenities	**VSS** Coverage for Observation to external and internal areas for general coverage of the building. Coverage for Identification: • Main entry to each building i.e. internal building foyer airlock area • Ground floor fire stairs door to external (internal side of door) **SMS/EACS/IDS** Building Main entry doors: • Card readers for entry (after-hours) • Automatic doors on building main entry • Arm/Disarm card reader applied on project-by-project basis Fire stairs: • Doors configured for general egress during the day (free handle) , and emergency egress only afterhours, via electric mortice locks and emergency break glass General: • Monitoring of door forced via reed switch • Motion detection via Video Motion Detection (VMD) on VSS (after-hours monitoring only) • Duress push buttons in staff and student areas, and amenities • Under desk duress buttons public facing counters and interface areas **Intercom System** Applied on project-by-project basis depending on building function

2.2.4.3 Zone 2- Semi-Controlled Spaces

The shared private spaces within buildings are areas which are generally off limits to public access and include areas such as:

- Student and Staff only facilities
- Common teaching venues/spaces
- Laboratories

Entry /exit doors leading into semi-controlled spaces shall be provided with electronic access control.

Swing doors must be provided with an electronic mortise lock and door closer. If sliding doors are used they must be motorised with appropriate controls to prevent the door from opening each time a person approaches the door.

VSS coverage in these areas shall include:

- Observation coverage of the external areas of the building
- Identification at all building entry points including main entry points and fire stairs
- Identification coverage of lift lobbies and within lift cars
- General VSS surveillance shall be provided to spaces that are accessible by students after hours.

Any area that is accessible by students 24/7 shall be provided with general VSS surveillance.

Depending on the use, risk and/or sensitivity of the area, areas may be required to be separately armed and disarmed from the rest of the buildings. Internal movement detection may be required.

Vertical Access

The security controls used for vertical access must be based on the access provisions for each stair or lift. Stairs and lifts may provide access to different security zones and therefore may need to be provided with suitable controls to manage access into those spaces.

Stairs can generally be categorised into one of the following:

- Emergency egress stair
- Internal movement stair

Where an emergency egress stair is not intended to provide internal movement, the stair doors shall be secure at all times providing emergency egress only, as required and in accordance with the *National Construction Code (NCC)*. All emergency egress doors shall be provided with an audible alarm and appropriate signage. Audible door alarms must be shunted in the event of a fire alarm.

Stair doors that provide access into controlled / restricted spaces shall be provided with an electronic mortise lock (configured as fail safe) and card reader, to restrict access onto the floor. Re-entry provisions shall be applied in accordance with the *NCC*.

Lifts that provide access into controlled / restricted spaces shall be provided with electronic access control. A card reader shall be incorporated into the lift to provide floor selection as programmed.

The Lift contractor will be required to provide additional cores in the Lift Trailing Cable for power and communications cabling to the lift car card reader.

Low Level Interface (LLI) connections shall be provided between the EACS and the Lift Control Unit to provide control of floor selection.

Lift call card readers shall be provided where lift usage is restricted to a specific group(s). This includes:

- Restricted lifts (e.g. staff only) located in non-restricted areas
- General lifts that open out to the public (externally).

When lift access is in “secure” mode the lift will only be able to be called when an authorised card is presented to the lift call card reader. This will prevent unauthorised access into the lift.

Refer the table below for the minimum security controls to be applied to Zone 2 Semi-Controlled Space.

SECURTY ZONE	EXAMPLE SPACES/BUILDINGS	MINIMUM SECURITY CONTROLS TO BE APPLIED
Semi-Controlled Space	• Lecture theatres (large and small) • Computing Labs • Library rooms • Studio rooms • Seminar rooms • Simulation rooms • Galleries • Guild • Vertical transport (lifts) and fire stairs • Gymnasiums	**VSS** Coverage for Observation (where applicable): • External building areas for general coverage of the building (where applicable to standalone buildings) • Internal areas for general coverage of the building corridors and circulation spaces. Coverage for Identification (where applicable): • Main entry to each building i.e. internal building foyer airlock area • Ground floor fire stairs door to external (internal side of door) • Inside lift cars (full internal coverage) No VSS coverage within rooms. **SMS / EACS** Building main entry doors and entry to semi-controlled rooms/spaces: • Card readers for entry • Free handle egress generally applied. Push to exit and breakglass required where automatic doors are used. • Electronic locking (preference electric mortice lock) on entry doors. Other locks applied on project-by-project basis • Doors configured for controlled access • Doors interfaced to room booking (where applicable) General: • Monitoring of door forced via reed switch for all controlled doors • Duress push buttons in staff and student areas, and amenities • Under desk duress buttons public facing counters and interface areas **IDS**

		To be applied on a project-by-project basis: • Arm/Disarm card reader • T20 codepads for arming/disarming of building or select rooms • PIRs for motion detection • Reed switches to external doors **Intercom System** Applied on project-by-project basis depending on building function

2.2.4.4 Zone 3 - Controlled Spaces

Controlled spaces are similar to semi-controlled spaces but are generally used by a more limited group of UWA personnel. Ideally these spaces should be located within a semi-controlled space. All individual semi-controlled spaces shall be restricted to authorised persons only by either key or electronic access control.

Depending on the use, risk and/or sensitivity of the area, areas may be required to be separately armed and disarmed from the rest of the overall buildings and internal movement detection may be required.

VSS coverage in these areas shall include:

- Observation coverage of the external areas of the building
- Identification at all building entry points including main entry points and fire stairs
- Identification coverage of lift lobbies and within lift cars
- General VSS surveillance shall be provided to spaces that are accessible by staff and students during both business hours and after hours.

Student Housing and Accommodation

Within student housing, individual bedrooms shall be provided with “wire-free” (offline) locking units with inbuilt card readers, which can read the UWA access cards. Access privileges shall be managed by Gallagher.

Main entry doors leading into student housing shared and common areas shall be provided with electronic access control, with card readers enabled to update the student’s UWA access card with system information such as the assignment of access privileges, battery status of offline doors and lost/cancelled/blacklisted card information, etc.

Refer the following table for the minimum security controls to be applied to Zone 3 Controlled Space.

SECURTY ZONE	EXAMPLE SPACES/BUILDINGS	MINIMUM SECURITY CONTROLS TO BE APPLIED
Controlled Space	• Staff only spaces i.e. administration (non public / student facing), school staff offices • Storerooms (general and high value storage) • Student Accommodation (General circulation spaces, common areas, amenities, accommodation rooms) • Workshop spaces (power tools) • Glasshouses • Central Plant	**VSS** Coverage for Observation (where applicable): • External building areas for general coverage of the building (where applicable to standalone buildings) • Internal areas for general coverage of the entry foyers circulation spaces (ground floor only) Coverage for Identification (where applicable): • Main entry to each building i.e. internal building foyer airlock area • Ground floor fire stairs door to external (internal side of door) • Inside lift cars (full internal coverage) Coverage for storerooms: • Observation within store rooms (project-by-project basis on value of goods within store room) • Identification on Entry points **SMS/EACS** Building Main entry doors and entry to controlled rooms / spaces: • Card readers for entry • Free handle egress generally applied. Push to exit and breakglass required where automatic doors are used • Electronic locking (preference electric mortice lock) on entry doors. Other locks applied on project-by-project basis • Doors configured for controlled access • Monitoring of door forced via reed switch for all controlled doors **IDS** To be applied on a project-by-project basis (pending building function): • T20 codepads for arming/disarming of building or select rooms • PIR's for motion detection • Reed switches to external doors **Wireless Access Control (student accommodation only)** • Gallagher hotspot reader in building foyer • Wireless lock to student accommodation units doors

		• Wireless hubs within corridors **Intercom System** Applied on project-by-project basis depending on building function

2.2.4.5 Zone 4 – Restricted Spaces

Restricted spaces are similar to controlled spaces but are generally used by a small group (3 or less people) or an individual. Ideally these spaces should be located within a controlled space. All individual restricted spaces shall be restricted to authorised persons only, with all entry /exit doors leading into restricted spaces provided with electronic access control.

VSS coverage in these areas shall include:

- Observation coverage of the external areas of the building
- Identification at all building entry points including main entry points and fire stairs
- Identification coverage of lift lobbies and within lift cars
- General VSS surveillance shall be provided to spaces that are accessible by staff and students during both business hours and after hours.

Application of additional VSS coverage for specific areas to be applied on a project-by-project basis to fulfill specific building functions.

Depending on the use, risk and / or sensitivity of the area, areas may be required to be separately armed and disarmed from the rest of the overall buildings and internal movement detection may be required.

Refer the following table for the minimum security controls to be applied to Zone 4 Restricted Space.

SECURTY ZONE	EXAMPLE SPACES/BUILDINGS	MINIMUM SECURITY CONTROLS TO BE APPLIED
Restricted Space	• Laboratories (PC2, PC3, PC4) • Specialist labs and workshops (include pharmacy dispensaries) • Morgue spaces (CTEC / Anatomy) • Clinical Spaces • Animal Holding • Data Centre	**VSS** Coverage for Observation (where applicable): • External building areas for general coverage of the building (where applicable to standalone buildings) ▪ Coverage for Observation to internal areas for general coverage of the circulation spaces Coverage for Identification (where applicable):

		• Main entry to each building i.e. internal building foyer airlock area • Ground floor fire stairs door to external (internal side of door) • Inside lift cars (full internal coverage) Application of additional VSS coverage for specific areas to be applied on a project-by-project basis to fulfill specific building functions **SMS/EACS** Access control to doors: • Card readers for entry and exit • Emergency egress via breakglass, fire trip interface • Electronic locking (preference electric mortice lock and electric strike in combination) on doors. Other locks applied on project-by-project basis • Doors configured for controlled access • Monitoring of door forced via reed switch for all controlled doors • Duress push buttons on a project-by-project basis **IDS** To be applied on a project-by-project basis (pending building function): • T20 codepads for arming/disarming of building or select rooms • PIR's for motion detection • Reed switches to external doors **Intercom System**

		Applied on project-by-project basis depending on building function.

2.2.4.6 Zone 5 – Services Spaces (Plant and Equipment)

Plant and equipment rooms are restricted areas that shall be monitored as a minimum, via door magnetic reed switches. Electrical substations, switch rooms, switchboards, etc are to be keyed as follows:

DESCRIPTION	KEY REQUIREMENT
High Voltage (HV) switchrooms & externally mounted HV transformer enclosures	HV restricted key
Low Voltage (LV) distribution panels within buildings & standalone LV distribution panels	ED6 restricted key
Switchrooms, switchboards, plant rooms and enclosures	EM restricted key

All communication rooms shall be provided with electronic access control.

VSS coverage in these areas shall include

- Observation coverage of the external areas of the building

Application of additional VSS coverage for specific areas to be applied on a project-by-project basis to fulfill specific building functions and in consideration of the criticality of plant/equipment.

Refer the table below for the minimum security controls to be applied to Zone 5 Services Space.

SECURTY ZONE	EXAMPLE SPACES/BUILDINGS	MINIMUM SECURITY CONTROLS TO BE APPLIED
Services Space	• Maintenance staff offices and workshops • Plant and Services Rooms (mechanical, electrical, hydraulic, communications, lift motor rooms)	**VSS** Coverage for Observation (where applicable): ▪ External building areas for general coverage of the building (where applicable to standalone buildings) Application of additional VSS coverage for specific areas to be applied on a project-by-project basis to fulfill specific building functions **SMS/EACS/IDS** Access control to doors: • Mechanical locking on doors. Other locks (including electronic locking, applied on project-by-project basis) • Doors configured for controlled access via keys • Monitoring of door forced via reed switch for all external doors

2.3 SECURITY SYSTEM REQUIREMENTS

2.3.1 Security Management System

The existing SMS is a Gallagher Command Centre system controlling and monitoring distributed intelligent field controllers, field devices and other integrated devices.

2.3.1.1 Software Licences

All software licenses for equipment and associated systems shall be provided and supplied as part of the installation and become the property of UWA.

2.3.1.2 Server

The server provides the alarm gathering, logging, reporting, alarm handling, audit trailing, including the facility to enter reportable incidents and action taken. The SMS server is managed directly by UWA UniIT.

2.3.1.3 Workstation

SMS workstations shall communicate with the server and manage all functions with full control and monitoring of the following:

- Cardholders
- Field devices
- Door alarms
- Logs and Reports
- Intruder and Duress alarms
- Fire alarms

2.3.1.4 Gallagher Command Centre GUI Maps

The administration, monitoring and operation of the SMS shall be conducted from the Security Control Room operator terminals using Gallagher Command Centre. The user software graphical user interface (GUI) shall be updated with all new works including the updates to all maps.

All graphical maps are to be approved by UWA Security prior to completion and shall include:

- Site map
- Building maps
- Building floor plan maps
- Manual ‘one touch’ selection of each map from a site map

- Graphics map navigation controls including home or site page, page up/down/left/right, individual building and floor selection buttons, etc. Navigational controls shall be located and available on all graphical maps in a consistent form and position on each page
- Display of device descriptor when the cursor is placed over the icon.

The graphical maps shall be in full colour, including borders, shading, shadows, patterns, and the like, to the approval of the UWA Security.

2.3.2 Electronic Access Control System

The Electronic Access Control System (EACS) shall be an extension of the UWA Gallagher Command Centre SMS.

The EACS hardware devices such as electronic locks, push buttons, emergency door release units, cable transfer devices and other equipment shall comply with the nominated equipment specified within this document.

All EACS doors must be provided with suitable door hardware to ensure the door closes and latches automatically without the door slamming or the need for manual intervention.

A Gallagher Intelligent Field Controller (IFC) Cable and Point Schedule shall be submitted to UWA Security for review prior to any new Gallagher installations.

2.3.2.1 Card Readers

The UWA card readers shall be:

- Compatible with the UWA access card format and protocol (Gallagher T15 MultiTech card reader and Mifare DesFire EV3 access cards)
- Black (including the bezel) unless otherwise stated
- Cabled with a 4 core 14/0.20 security cable
- Securely fitted and installed
- Installed at 1000mm from Finished Floor Level (FFL) to the midpoint of the unit.

The reader shall have both audible and visual indicators for a successful card read. Where a back plate is required it shall be clear anodized aluminium.

2.3.2.2 Intelligent Field Controllers

The Intelligent Field Controllers (IFC) shall be a Gallagher Controller 6000.

The IFCs shall be secured and installed in a Gallagher Dual Cabinet. All Gallagher Dual Cabinets shall be Cool Grey colour. Each cabinet shall have a steel embossed label affixed via adhesive backing to the front of the cabinets noted as follows "(Building Number) - BUILDING NAME – UNIT (Unit Number)".

Each Gallagher dual cabinet shall include a Gallagher 8A Power Supply and a minimum of four 7AH 12V DC batteries providing an approximate battery back-up time period of 4 hours for each cabinet.

IFCs and associated devices (locks, card reader etc.) shall be connected to the building's essential services board. Refer to the *Design and Construction Standards – Electrical Services* for essential power requirements.

2.3.2.3 Electronic Locking Devices

All electronic locking devices shall meet the following requirements:

- All electronic locking devices shall operate from a 12VDC power supply
- Internal doors with electronic mortise locks shall fail secure and remain locked from the outside in the event that power is removed from the lock. All fail secure doors must be provided with free handle egress
- External doors with electronic mortise locks shall fail secure and remain locked from the outside in the event that power is removed from the lock. All fail secure doors must be provided with free handle egress
- Doors configured with dual locking i.e. electric mortise lock and electric strike, shall be configured as follows:
    - Electric Strike – is controlled by the electronic EACS and in a 'fail secure' configuration. This lock shall be configured to operate as the main electronic access control door lock (i.e. day mode)
    - Electric Mortice Lock – is wired via the emergency break glass release and/or Fire Indicator Panel (FIP) interface (where applicable), in a 'fail safe' (i.e., power to lock) configuration.
- The electronic mortice locks shall be installed 1000mm from FFL
- Key override cylinders shall be located on the secure side(s) of the door and keyed on the restricted UWA GGMK Security key.
- Cabling to any electronic locking devices shall be a minimum 8 core 14/0.20 security cable
- The Electronic Mortice Locks (standard type) is the preferred lock for all access controlled doors. The lock shall be complete with:
    - Exit hub switch
    - Power on to lock configuration (fail safe, unless otherwise stated)
    - Free egress operations (unless otherwise configured with exit reader and breakglass unit)
    - Dead latch monitoring
    - Key override monitoring
    - A separate reed switch to reflect door status
- All other types of Electronic Locks shall only be installed following approval by UWA Security and completed with:
    - Power on to lock configuration (fail safe, unless otherwise stated)
    - "Push to Exit" button for egress operation (unless required and configured with an exit card reader)
    - Monitored Breakglass Unit (BGU) installed for emergency door release function
    - A separate magnetic reed switch to reflect door open/closed status

2.3.2.4 Magnetic Reed Switch

All doors connected to the EACS shall include a separate magnetic reed switch to reflect door open/closed status.

The standard magnetic door reed switch contacts shall be fully recessed into the door and doorframe. It shall be fitted with an “End of Line Resistor” and cables shall be terminated at the device using soldered connections and finished using a heat shrink to cover all bare wires.

Heavy duty magnetic reed switches shall be used for roller doors, shutters, or gates.

Fire door magnetic reed switches shall be of the appropriate type to meet the fire rating of the door.

Cabling to magnetic reed switches shall be a 4 core 14/0.20 security cable.

2.3.2.5 Push to Enter/Exit Button

Push to exit buttons shall be used on all automated doors interfaced to the EACS, doors fitted with electronic strikes and electromagnetic locks and electric mortice locks.

All Push to Exit buttons shall be Gallagher Touch to Exit egress devices (C861200).

It shall be engraved with the appropriate function "PRESS TO EXIT" or "PRESS TO ENTER". The lettering shall be in red and a minimum of 6mm.

The push button unit shall be mounted at 1000mm above FFL to align with other services to be installed at the door including card reader, break glass unit and the like.

Cabling for the request to exit buttons shall be a 4 core 14/0.20 security cable.

2.3.2.6 Emergency Door Release or Break Glass Unit

The unit shall be a white KAC MCP4 with double pole contact for lock power and alarm.

The unit shall have a resettable plastic insert and test key type.

It shall be provided with a hinged cover engraved with "Emergency Use Only" over the collapsible face to stop accidental use. Lettering shall be in red and a minimum of 6mm.

The cabling to the associated electronic locking device shall be via the BGU such that activation of the unit shall unlock the electronic locking device regardless of system status.

The BGU activation shall be constantly monitored by the SMS.

The unit shall be mounted at 1000mm above FFL to align with other services to be installed at the door including card reader, push button and the like.

The cabling for the unit shall be a 4 core 14/0.20 security cable.

2.3.2.7 Cable Transfer Device

The cable transfer device shall be an Abloy 8810. It shall be completely concealed and installed in accordance with the manufacturer's instructions.

A cable transfer device shall be installed to provide connection from the IFC to the electronic lock and to allow the transfer of wiring between the door and the frame.

2.3.2.8 Door Hold Open Devices

Door hold open devices are often used on fire doors that are required to automatically close in the event of a fire alarm. Where the door also provides a security barrier it shall be connected to both the EACS and the Fire System to meet all the requirements of a controlled door in a required fire egress path. The SMS shall monitor and control the device as programmed or operated. During scheduled times the device will activate and hold the door open once a door is pushed to the fully opened position and allow the bond plate to make full contact with the wall magnet.

The hold open devices shall be fitted to suit the door type and taking into account the height of the device must allow for a person to reach the device without any climbing aids to push the release button for manual override or reset.

2.3.2.9 Access Cards

The UWA access cards are Mifare DesFire EV3 Cards. The access cards are obtained by staff, students or visitors from UWA Student Administration.

Requests for card access must be made in writing via email and must be authorised by the UWA Project Manager or Responsible Officer from the School or Section.

All requests shall include the following:

- Cardholder name
- Visitor/card number
- Building name and number
- Access details such as door name/number and access times
- Access expiry date
- Project name or reason for access

Requests for card access shall be made at least three (3) days in advance of the desired activation date.

Lost cards shall be reported to UWA Security for cancellation of access permissions immediately.

2.3.2.10 Lift Interfaces

All lift interfaces shall be via a Low Level Interface between the lift controller and EACS IFC, unless otherwise

approved by UWA Security.

Where required, the lift interface shall provide the following functionality:

- Enable the EACS to “lock down” the lift to the general public, whilst enabling authorised persons to call and utilise the lift, via an authorised EACS access card. To provide this functionality a card reader shall be installed adjacent to the lift call button outside the lift to restrict an unauthorised person from calling the lift.
- Enable the EACS to restrict the selection of designated level(s) to authorised persons only, via an authorised EACS access card. To provide this functionality a card reader(s) shall be installed within the lift, adjacent to the floor selection buttons.

2.3.2.11 Automatic Door Interface

The automatic doors shall comply with the relevant Standards, Statutory Authorities and Regulations for fire connection, operation, disability access and mobility.

All automatic doors shall be provided with a key override switch, located on the external side of the door that is keyed on the restricted UWA GGMK Security key. The key override switch shall provide the following door modes:

- Auto - the EACS shall control the door when in Auto mode.
- Open - the door shall remain in the open position.
- Exit - the door shall provide egress and not entry.
- Lock - the door shall remain locked from both the inside and outside.

Note: All modes shall be overridden by a fire signal.

Each access controlled automatic sliding door shall be connected to an EACS IFC via an eight (8) core cable. Two (2) cores shall be connected to the day/night input of the automatic door controller, two (2) cores shall be connected to the pulse input of the automatic door controller control, two (2) cores shall be connected to the door open output of the automatic door controller and two (2) cores shall be connected to the lock status output of the automatic door controller.

When the door is in free access mode the doors shall open and close under control of the door PIR sensors (supplied and installed by the door manufacturer).

When the door is in secure mode the door shall operate as follows:

- In secure mode the door controller closes and locks the door and the door does not respond to the door PIR sensors.
- Access will occur only by use of a valid access card presented to the associated door card reader.
- An authorised card presented to the card reader shall provide an unlock command to the sliding door controller. The controller unlocks, and opens the door for a predetermined time typically 15 seconds, after which the door closes and locks.

- Egress in secure mode is allowed when the Press to Exit button is activated. The EACS shall provide an unlock command, via the pulse input, to the sliding door controller. The door unlocks and opens for the predetermined time, after which the door closes and locks.

Located with all “Press to Exit” buttons and/or internal card readers are monitored BGUs. When the BGU is activated, the door control unit shall go into fire mode. The BGU shall be wired to the emergency open terminals on the door controller under advice from the auto door contractor to ensure correct operation.

The automatic door shall be directly connected to the FIP and provide full functionality as dictated by the *NCC*.

All activation devices like card readers, emergency door release units and push buttons shall be installed at a height of 1000mm from FFL.

Automatic doors shall be connected to building’s essential services board. Refer to the *Design and Construction Standards – Electrical Services* for essential power requirements.

2.3.2.12 Wire Free Access Control (Data on Card or Wireless)

Wire Free Access Control (WFAC) is an access control system used in areas such as Student Housing, where there are multiple individual spaces that require a higher level of credential control than lock and key and where wired electronic access control would be cost prohibitive.

The WFAC is an integrated part of the Gallagher SMS providing controlled access at nominated doors.

The Wireless Access Control (WAC) shall be a Salto Systems Access Control System incorporating a combination of wireless electro/mechanical readers for each student room doors, online Salto readers/hotspots at nominated locations and Gallagher access control on building perimeter/accommodation main entrance doors.

Each building that contains a Salto online reader shall be fitted with a Salto Controller and a Gallagher IFC.

The Salto System card readers and controllers shall be integrated into the existing Gallagher SMS.

Cards held and used by students are programmed/reconfigured to allow them to be used at the WAC reader points. These cards will be updated automatically for both common door and student room door access whenever a student presents their card to an online Salto System reader.

The WAC shall be integrated into the SMS and shall be capable of monitoring for attempted unauthorised entry, forced door, door ajar, and report these events to the SMS for logging and alarm notification. Attempted unauthorised entry, forced door, door ajar and other alarm monitoring does not apply to doors fitted with Salto Wireless Offline Card Readers.

The WAC shall also monitor the status of all doors and tamper alarms connected to the system. In the event of an alarm or tamper, the WFAC system shall report this status, via the SMS.

The existing WFAC system comprises of:

- Mifare DesFire EV3cards
- Salto wall readers
- Salto Electronic Locks/Escutcheons with key override
- Salto Control units
- Salto Gateway unit
- Portable Programming Device
- Encoders
- Energy Saving Devices

All locks, readers or any door activation devices shall be installed 1000mm from FFL.

All devices installed shall be compatible with the current version of Gallagher and Salto software. Unless otherwise specified there shall be no need to upgrade software to cater for any new installations.

2.3.3 Intruder Detection System

The Intruder Detection System (IDS) shall be fully compatible with the Gallagher SMS and shall be fully integrated with the EACS. The alarms shall be monitored and controlled by the SMS. It shall provide an internal audible alarm locally and no external alarms unless otherwise stated in the project requirements.
Each area covered with intruder detection devices must have its own Remote Arming Station (RAS).

All IDS devices shall be installed in accordance with the manufacturer's instructions.

2.3.3.1 Magnetic Reed Switches and Contacts

Each magnetic reed switch shall be fitted with an “End of Line Resistor” and cables shall be terminated at the device using soldered connections and finished using a heat shrink to cover all bare wires.

The door magnetic reed switch shall suit the type of door frame and meet fire or security requirements.

Heavy duty magnetic reed switches shall be installed on roller doors, shutters, or gates.

Fire door magnetic reed switches shall be of the appropriate type to meet the fire rating of the door.

Cabling for the magnetic reed switches shall be a 4 core 14/0.20 security cable.

2.3.3.2 Motion Detectors

Passive Infrared (PIR) Detectors

PIRs are to be provided in locations where an individual rooms or areas shall be separately armed and secured within a building. These includes areas within Semi-Controlled, Controlled and Restricted spaces and where this has been identified on a project-by-project basis.

Detectors shall be installed in accordance with the manufacturer's instructions. Detectors shall send a tamper

alarm when there is an attempt to remove the cover or the detector.

The final location of the detector shall be determined with consideration given to both architectural and structural features and any obstruction that may limit the detector's detection coverage. All detectors shall be cabled with a 4 core 14/0.20 security cable.

The General Purpose PIR Detector shall include the following features:

- 16m coverage with 9 curtains
- 86 degrees field of view
- Mirror Optics
- Active Anti-masking
- 4D Signal processing

The 360 PIR Detector shall include the following features:

- 4D signal processing
- 360 degrees Field of view
- 9 curtains 20 m volumetric coverage
- 2 Independent Mirror optics and Dual element pyroelectric infrared sensors
- 20m coverage with 18 curtains

The Long Range PIR Detector shall include the following features:

- 4D signal processing
- 12m and 24m volumetric coverage
- 60m long range with single curtain
- 86 degrees Field of view
- Mirror optics and Dual element pyroelectric infrared sensor

The Dual Technology Detector shall include the following features:

- 4D signal processing
- Mirror optic PIR and Microwave
- Dual element pyroelectric infrared sensor
- 7m, 10m, or 16m coverage with 9 curtains
- 86 degrees Field of view

VSS Video Motion Detection (VMD)

Video Motion Detection (VMD) via the VSS shall be used is areas that are more widely accessible and contain internal VSS coverage. This applies to areas and buildings that are accessible after hours, fire stairs etc. This includes areas within Public Space (internal) areas.

2.3.3.3 Duress Buttons

There are two types of duress buttons, Desk Mount and Wall Mount. All duress alarms shall be locally silent and shall report back to UWA Security via the SMS. Duress alarms shall be audible in the Security Office and the sounder shall only be deactivated when the alarm is acknowledged.

The Desk Mount Duress Alarm Button shall include a centre pull activated slide switch. It shall have a pulling action slide switch operation and a key to reset the alarm. This device shall be mounted under the desk and shall be installed in a concealed non-visible location.

The Wall Mount Duress Alarm Button shall:

- be a robust, resettable mushroom type push button.
- have a “re-assurance” indicator activated by the SMS when the alarm is received
- be non-keyed with turn to reset and with arrows to indicate turn direction
- have a mounting or back plate labelled “Duress Button”
- be mounted flush on wall and in clear view.

2.3.3.4 Remote Arming Station /Terminal

The remote arming station/terminal shall be installed within the protected area. It allows users to arm (set) and disarm (unset) areas of the intruder alarm system.

The Remote Arming Stations shall be a Gallagher T15 card reader with an alarm Light Emitting Diode (LED) status back plate. The reader shall provide the ability to Arm (set) and Disarm (unset) the intruder alarm. The Alarm LED Status Plate shall be a Red and Green LED on an aluminium plate engraved to show “ARMED” when RED and to show “DISARMED” when Green. The back plate shall match other existing UWA Remote Arming Station (RAS) on site.

A Gallagher T20 Remote Arming Terminal (RAT) shall be used in sensitive areas where a higher level of security is required. Access can only be achieved by presenting a valid card and a Personal Identification Number (PIN). Gallagher T30 Keypad Readers shall be used on approval of UWA Security.

A Gallagher RAT shall only be used when there is a requirement for users to perform functions such as arm, disarm, or isolate alarm zones (individually or all at once), and view and acknowledge alarms.

All Liquid Crystal Display (LCD) text displayed shall provide a clear description of the event.

2.3.3.5 Wireless Transmitters and Receivers

Wireless transmitters and receivers shall be compatible with the existing Gallagher SMS where all IDS alarms are integrated and managed. The wireless transmitters and receivers shall be Innovonics Echostream and shall be compatible with existing wireless devices if there are any. It shall be installed in accordance with the manufacturer's instructions.

2.3.4 Video Surveillance System (VSS)

The Video Surveillance System (VSS) is inclusive of VSS cameras, VSS Servers, and Network Video Recorders (NVRs).

VSS may be used in nominated areas as directed by Campus Management. Refer to the *UWA CCTV policy* (available from UWA Security) prior to design and installation.

The UWA VSS is based on an Avigilon Video Management System (VMS) which is utilised to control, monitor, manage and record all VSS cameras. All VSS cameras shall be connected and recorded to the Avigilon NVRs.

All devices shall be installed in accordance with the manufacturer's instructions.

All VSS components shall be connected to building's essential services board. Refer to the *Design and Construction Standards – Electrical Services* for essential power requirements.

2.3.4.1 VSS Architecture

The Avigilon VSS architecture includes:

- Central VSS server within the Reid Building acting as the database host
- NVRs distributed within individual buildings, with the NVRs rack mounted within communications rooms within their respective buildings
- Main operator's workstation located within the Security Control Room.

All new NVR's are to be installed within the Physics Data Centre. All current NVRs shall be centralised into the Physics Data Centre as part of new project works.

2.3.4.2 Network Video Recorders

All VSS cameras shall be recorded onto a Network Video Recorder (NVR). All licenses required to stream live VSS images and capture them is the responsibility of the PSC. The recording equipment shall be connected to the UWA network and the existing UWA VSS system. All recordings, playback and live streaming shall be remotely accessible from Avigilon Control Centre software.

Recordings shall be at a minimum:

- Resolution of 1920x1080
- 13 frames per second background recording (i.e. no activity recording)
- 25 frames per second recording on motion/activity detection
- Continuous mode recording
- 35 days recording retention on hard disk drive

The NVR shall be configured as RAID6 storage, including hot swappable disks for ease of service. It shall also be capable of recording both MPEG-4 and H.264 and shall be 19" rack mounted (horizontally). All hard drives

shall be approved by the NVR manufacturer.

Liaise with CM (Security) to determine if a new NVR(s) is required or if an existing NVR has spare capacity to cater for additional camera(s). If an existing NVR is not available or does not have capacity, then additional NVR(s) shall be provided to record and store the additional camera footage.

The storage capacity of the NVR shall be determined by the number of cameras recording. All additional NVRs shall be 96TB models. The quantity of VSS cameras applied to each new and existing NVR shall be coordinated with UWA Security during the design process to determine if spare capacity can be utilised or additional NVRs are required. This shall be completed on a project-by-project basis.
Liaise with UniIT and/or the Communications Consultant to confirm network bandwidth availability and requirements.

2.3.4.3 Cameras

Placement and mounting of cameras shall be at a height of approximately 3 metres or below for ease of maintenance. Cameras required to be mounted higher than 3 metres shall require confirmation from UWA Security. The field of view must be clear of any obstruction to provide clear views of areas and images of people as intended. The cameras must be placed in an area with good lighting conditions but below light fittings. The cameras shall be aimed to avoid effects of streaking and glare from direct sunlight.

Lens and camera adjustments must be verified at night to provide optimum coverage and performance during both day and night conditions. All settings must be “locked” and recorded for future reference and included within the Operations & Maintenance Manuals submitted by the PSC as part of the project works..

The cabling to the cameras must be protected from vandalism and tampering. Cabling shall be installed hidden from view through the ceiling and/or walls.

Unless otherwise specified all new cameras shall be Internet Protocol (IP) based. All cameras installed must include the appropriate licenses to connect and record onto the Avigilon VSS, this shall include the relevant Avigilon Licence required for non-Avigilon cameras.

The lens focal length shall be selected by the PSC to provide the required field of view in accordance with the VSS coverage functions and objectives (refer *Section 2.3.3.4* of this document) and AS/NZS 62676.4.

A camera schedule shall be submitted to UWA Security for review prior to any VSS camera installations. As a minimum the schedule shall include:

- Camera No
- Description
- Camera function in accordance with AS/NZS 62676.4.
- Network Video Recorder ID
- Lens Focal Length

- Camera Model
- Serial Number
- Network Switch Location
- MAC Address

All VSS cameras shall be configured to the Avigilon VSS reflective of the current camera configuration and recording requirements.

Internal Fixed Dome Camera

The internal fixed dome cameras shall be powered directly from the network via the built in PoE (Power-over-Ethernet) port.

Refer to *Approved Equipment List (Section 4.1)* for approved internal fixed dome cameras.

External Fixed Dome Camera

The external fixed dome camera shall be powered directly from the network via the built in PoE (Power-over-Ethernet) port. The camera enclosure shall have a minimum IP65 rating.

Refer to *Approved Equipment List (Section 4.1)* for approved external fixed dome cameras.

Pan Tilt Zoom (PTZ) Dome Cameras

Refer to *Approved Equipment List (Section 4.1)* for approved PTZ dome cameras.

2.3.5 Intercom System

The Intercom System shall operate using digital technology, provide clear undistorted speech communications and be free from background noise.

All external Intercom Stations shall be vandal resistant with the correct IP rating for the environment. Each intercom shall be monitored by the SMS and VSS where available.

2.3.5.1 Help Point Intercom

Help Point Intercoms shall be Avigilon H4 Video Intercoms. Intercoms shall be configured and programmed to the UWA LAN and utilise Microsoft Teams to dial the security emergency number or a pre-configured phone number when the front panel button is pressed. It shall provide a hands free, vandal and water resistant interface to a UWA IP telephone system.

The Intercom System shall interface with the SMS/ACS and the VSS to initiate appropriate camera views at a call location when available.

Existing analogue Jacques Help Point Intercoms shall be retrofitted with an Analogue-to IP-convertor to allow

intercoms to communicate via the UWA LAN.

2.3.5.2 Standalone Intercom

The standalone intercom system shall be Avigilon H4 Video Intercoms configured and programmed to the UWA LAN and utilise Avigilon Client to provide clear voice communication and/or video transmission to the local workstation. The type and model shall suit the environment and the intended use as required by the project. External units shall be a vandal resistant unit with microphone, speaker and call button activation. The remote station must have the facility to call a designated Avigilon Client application (loaded to a workstation) within the area associated with the intercom unit.

The activation of a “door release” button on any master station shall be recorded on the SMS transaction summary.

Alternatively these intercoms can call to the Security Control Room phones / Avigilon Client for response and the control room able to unlock doors or gates remotely via Gallagher.

The Intercom System shall interface with the SMS/ACS and the VSS to initiate appropriate camera views at a call location when available.

2.3.6 Electronic Key Cabinet

The UWA Electronic Key Cabinet System is a self-manufactured system that uses Gallagher IO Boards wired back to the controller. If a Key Cabinet is required, a request is to be made to the Security System Officer with the following details

- Size of Cabinet (10, 25, 50)
- Number of Cabinets

The Cabinet uses Key Capture mechanisms from Keyhold.

UWA’s Preferred Locksmith supplies 570 Oval Cylinders keyed to the UWA System.

The key with the highest level of access shall be locked into the cabinet.

Please refer to *UWA Security - Keyhold Cabinet Installation & Setup Manual f*or additional information.

2.3.6.1 Authentication and Access

Authentication and access shall be via a Gallagher T20 Card Reader, keyed to the UWA Mifare Classic Key.

2.3.6.2 Battery Back-up

Electronic Key Cabinets shall be provided with minimum four (4) hours built in battery back-up supplied by the

manufacturer.

2.4 GENERAL CONSTRUCTION AND INSTALLATION REQUIREMENTS

2.4.1 Coordination

The PSC shall directly coordinate work between other trades and UWA personnel in order to complete the project requirement.

2.4.2 Protection of Finishes and Fixtures

All finishes, fixture and fittings are to be adequately protected against damage to the satisfaction of UWA. Any damage caused by the PSC must be repaired immediately and all costs borne by the PSC. Any further damage to finishes and fixtures highlighted during the installation will be the responsibility of the PSC to make good.

2.4.3 General Installation Standards

The UWA facilities are considered to be of a high quality commercial/public standard in regard to all security to be installed. All equipment, materials, installation methods and workmanship shall be selected, designed and installed in a manner which is mindful of the environment and purpose intended.

This shall include, but not be limited to:

- Material and equipment selection shall be suitable for a commercial/public facility
- All fixings required shall be tamper proof type and uniform throughout the installation
- Consideration shall be given to heavy traffic areas and the repeated use of devices when selecting locks, door closers, hinges and the like which will need to be designed for such heavy duty wear and tear
- All fixing methods, manner of installation, workmanship and the like for equipment and devices shall be suitable for use in a high quality commercial/public facility
- Wherever possible, devices shall be flush mounted and all services securely concealed
- All devices however shall remain serviceable without the need to damage infrastructure, finishes and the like. Wherever possible service access shall be provided by others or as part of this contract
- Any equipment installed within these facilities which are considered by UWA not to be fit for use in a high quality facility shall be replaced at no cost when requested by UWA.

2.4.4 Cabling

The cables shall meet the requirements of the appropriate Australian Standard for installation, cable size, use

and environment.

All cabling shall be neatly tied/loomed to prevent damage to terminations and stress on cables. It shall also prevent interference or obstruction to other services. It shall be installed under the 'loop into fittings' system with adequate slackness behind each device to facilitate removal for inspection, adjustment or replacement.

If any kinks or abrasions to insulation, braiding, sheathing or armouring occur during the installation of cables, the affected cable shall be withdrawn and replaced with a new cable.

All cabling shall be concealed and installed on a metal cable tray, cable duct and/or conduit. All cabling and cable containment systems shall be coordinated with the Electrical and Communications services. All security cabling shall be installed on common services cable tray, supplied and installed by the electrical/communications services contractor. The PSC shall provide all required conduits and catenary as required for a complete installation of the security systems.

All cables including patch leads shall be clearly labelled.

2.4.5 Fire Connection

The FIP shall send a signal to the SMS and report as a critical alarm. A Jackfuse PP9PTC Power Distribution & Fire Monitoring Board, a Gallagher Fuse & Fire Relay Board or an approved equivalent shall be installed at each Gallagher IFC to remove the power to the electronic locks to allow free access to exit routes. In addition, all automatic doors shall be directly connected to the FIP and must not be reliant on the fire connection at the Gallagher IFC.

The PSC shall liaise with the Fire Engineer to connect the IFC to the fire system.

2.4.6 Enclosures and Cabinets

The equipment enclosures shall be a Gallagher Dual Cabinet for the access control IFCs and expansion boards.

All Gallagher Dual Cabinets shall be Cool Grey and include stainless steel labels to identify relevant controllers installed within the cabinets.

All other equipment panels, racks and cubicles for internal use shall be high quality ‘Rittal’ type or equivalent approved by UWA, suitably sized to accommodate all equipment with spare capacity remaining for future expansion.

The enclosures shall be installed in accordance with the manufacturer’s instructions and in a secured location. It shall be fitted with tamper switches that are monitored through the SMS.

The height and position of enclosures shall be readily accessible for service and maintenance without difficulty, hazard and being able to be used as a climbing aid. The top of the Gallagher Dual Cabinet shall be no higher

than 1,800mm.

All keys for enclosure locks shall be of approved high security rating and supplied in duplicate to UWA.

All equipment enclosures within the building shall be located in a secured room or cupboard and clearly labelled.

Refer to the *UWA Design and Construction Standards – Communications Services* for equipment rack requirements.

2.4.7 Battery Back Up

The batteries shall be a sealed lead acid type. Four back-up batteries (12V 7.2AH) shall be installed within each access control cabinet to maximise the enclosure capacity, providing an approximate battery back-up time period of 4 hours for each cabinet. All installed batteries shall be dated and secured in the panel.

2.4.8 Uninterruptible Power Supply (UPS)

Back-up power supply systems shall be coordinated with the Electrical distribution system. Refer to the *Design and Construction Standards – Electrical Services* for essential power requirements.

If required, provide a single phase UPS that is rated to provide two hours of UPS back-up (at full load) to the VSS and other nominated sub-systems equipment powered directly from mains power. The UPS shall have a low battery alarm, which shall be displayed on the SMS.

2.4.9 Systems Integration

All Security Systems shall be configured to maximise the interconnectivity across the UWA network infrastructure and interface with other UWA systems to achieve the optimum functionality, performance and reliability.

The security system may have LLIs and HLIs. The LLI shall be a set of dry/voltage free contacts controlled via a signal from the Gallagher IFC. The HLI shall be provided using a standard protocol or language and an established software product that is fully compatible with the SMS.

The Security Systems may interface with the following systems, but not be limited to:

- Fire System
- Lift System
- Automatic Doors
- Building Management System
- UWA Data and Control Systems

2.4.10 Standard Naming Convention

The PSC shall follow the UWA standard naming convention when programming all the site items.

The convention shall be:

[Building Number] [Building Name] [Room Number] [Description] [Site Item]

Example for Access Zone:139 Reid G24 Meeting Room AZ

2.4.11 Programming

The PSC shall carry out full programming of all systems, including initial setup and data entry in accordance with the requirements of each area/zone, local/remote operation or network interface to other systems. The PSC shall directly coordinate with UWA Security, the School / Section and the Campus Management project manager.

The programming shall include, but not be limited to:

- Parameter setup for all security services systems, equipment, interfaces and integration components.
- Access groups, cardholder access schedules and cardholder membership
- Access zone schedules and alarm zone schedules
- The IDS arming/disarming requirements, SMS, EACS, VSS interfacing, icons requirements, etc.
- VSS and NVR system response to select SMS alarms and intercom calls
- Graphical mapping, icon placement and identification
- Programming of interfaces and integration to all security services and building systems, UWA systems and UWA required messages
- The intercom call preferred master station, unanswered call diversion and all SMS, EACS, VSS interfacing for all intercom stations.

2.4.12 Documentation and Drawings

Confidentiality

The security services documents, drawings and the technical specification shall be handled as confidential documents at all times.

Documentation

The following documentation shall be supplied to UWA in electronic format except where electronic versions cannot be provided:

- Commissioning Sheets
- Gallagher Wiring Reports
- Test Plans and Results

- Technical Documents
- Configuration Details
- Manuals and User Guides
- UWA Campus Management – Asset Data Capture Form

Drawings

All schedules shall be submitted to UWA Security for the proposed equipment location, view, equipment type and the like, for review prior to the commencement of the works or the purchase of equipment.

Legible and accurate "As Constructed" drawings, in accordance with *UWA Specifications for As Constructed Documentation*, shall be provided as a pre-requisite to the granting of practical completion.

As a minimum the following As Constructed Drawings shall be included:

- Floor layout plans shown installed location of all security devices
- Schematic diagrams
- Network connection diagrams
- Cabinet layouts and fit-off details

As constructed security drawings or plans shall:

- Show all works / variations completed
- Be suitable for high quality reproduction
- Be free of copyright conditions and the like that may prevent UWA from using, copying or referring to them
- Be prepared by a qualified draftsperson

2.4.13 Testing and Commissioning

Testing shall be documented and all test sheets for all commissioned items shall be provided to UWA Security. All equipment installed and operated shall be included in the Testing and Commissioning process.

During commissioning, the PSC shall:

- Confirm that all equipment is fully operational
- Provide a comprehensive final commissioning report outlining all test results, as constructed details, performance test data on all cables and any other information deemed necessary for future records
- Supply all labour, materials and equipment required to fully commission and test the entire installation to the satisfaction of UWA Security
- Allow for minor programming changes as a result of testing and commissioning
- Repair or replace any equipment which fails to operate correctly, or is considered by UWA, to be installed incorrectly
- Supply all system passwords.

UWA and/or their representative will only undertake acceptance testing upon written confirmation that every point has been fully tested in accordance with this document and is 100% operational.

The PSC shall provide verification that all points have been commissioned and signed off prior to the final acceptance testing by UWA and/or their representative.

Final performance and acceptance testing to be conducted with UWA and/or their representative shall, as a minimum include:

- Physical inspection of each point, device and final system installation
- Test function of each zone, point and device
- Test alarm response and annunciation of each zone, point and device
- Check logging and recording of activity for each zone, alarm point and device
- Test required interface with other systems for each zone, alarm point and devices
- Confirmation that each system performance complies with the project specification.

On completion of the work satisfy UWA that the system operates in accordance with the requirements of this specification.

Fire Interface Test

A Fire Test shall be carried out to the satisfaction of UWA. The PSC is responsible to ensure that the appropriate UWA personnel and all areas affected are advised of a fire test.

New IFC's with a new fire cable installed shall be tested end to end from the FIP or Fire Indicator Board to the IFC fire relay.

2.4.14 User Training

User training sessions shall comprise Operator training and Administrator/ Technical training. Operator training shall comprise an overview of the complete security system and all functions to effectively carry out daily housekeeping, alarms and responses. The Administrator / Technical training shall include all operator training as well as higher-level housekeeping, alarm management and system operations.

Provide on-site training to the nominated UWA staff and operators. Training shall be comprehensive, "hands on", covering all aspects of system operation or equipment and sub-systems. Provide a Training Schedule if required.

2.4.15 Practical Completion

Practical Completion shall only be granted after:

- A physical inspection of the works and functional testing is completed and accepted by UWA
- Testing and commissioning of all installed equipment is completed

- UWA are satisfied that the system is operating in the correct and specified manner
- All nominated staff are trained to a demonstrable level of competency, where the staff may carry out their required functions
- UWA has accepted all systems and confirmed that all training has been provided to staff
- All information is provided to UWA.

If all of the above criteria are met, Practical Completion shall be granted.

Failure of the system during the 28 day test period will incur a further two (2) weeks of testing after the faulty component is repaired and commissioned, until the complete system operates faultlessly for 28 continuous days.

2.4.16 Warranty

A warranty for all equipment, materials, works and the like shall be provided for a Defects Liability Period (DLP) of 52 weeks. The DLP shall only commence from the date Practical Completion is granted in writing by UWA or their representative.

During DLP the PSC shall attend on-site within two (4) hours of notification of a failure of the equipment and associated systems installation. This call out requirement shall apply on a 24 hour, 7 day a week basis.

All works implemented which prove to be faulty from workmanship or materials shall be, without additional charge, fully maintained and serviced during the defects liability period.

UWA reserves the right, on failure to perform such corrective works, to engage others to finish such work without further notice. The costs of such works shall be deemed a debt to the PSC.

3 Electronic Access Control

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
Assess if EAC is a project requirement	Services consultants	CM (Security) / School or Section	Gate 2 Feasibility
For refurbishments, check if existing security measures are sufficient and in accordance with the design requirements of this document	Services consultants	CM (Security)	Gate 2 Feasibility
Approval / Sign-off on security design	Services consultants	CM (Security) / CM (Capital Projects) / School or Section	Gate 2 Feasibility
Determine if there are existing Gallagher FT IFCs in the building	Services consultants	CM (Security)	Gate 3 Planning
Determine if existing Gallagher IFC(s) meet installation requirements	Services consultants	CM (Security)	Gate 3 Planning
Determine if Gallagher IFC is in a suitable location, e.g., cable access from access control doors	Services consultants	CM (Security)	Gate 3 Planning
Determine if existing Gallagher IFC has spare card reader capacity	Services consultants	CM (Security)	Gate 3 Planning
Determine if existing controller has sufficient Input/Output (I/O) capacity	Services consultants	CM (Security)	Gate 3 Planning
Determine if there is sufficient network capacity to cater for all new Gallagher IFCs	Services consultants	CM (Security)	Gate 3 Planning
Full inspection and commissioning of the system	Services Consultant / Contractor	CM (Security)	Gate 6 Handover
Consultant inspections and witness testing	Services Consultant / Contractor	CM (Security)	Gate 6 Handover
Provide all Security As Constructed documentation, including: • Commissioning Sheets • Gallagher Wiring Reports	Contractor	CM (Security) / CM (Capital Projects)	Gate 6 Handover

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
• Test Plans and Results • Technical Documents • Configuration details • Manuals and User Guides • Security Drawings			
All electronic access control doors operate correctly	Services Consultant / Contractor	CM (Security)	Gate 5 Construction
All alarms are logged on Gallagher	Services Consultant / Contractor	CM (Security)	Gate 5 Construction
Update Gallagher graphical maps with the latest background drawings	Contractor	CM (Security)	Gate 5 Construction
Undertake fire interface test	Services Consultant / Contractor	CM (Security)	Gate 6 Handover

3.1 VSS

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
Assess if VSS is a project requirement, in accordance with this document	Services consultants	CM (Security)	Gate 2 Feasibility
Check that the minimum security requirements has been included in the design	Services consultants	CM (Security)	Gate 2 Feasibility
Approval / Sign-off on the VSS design	Services consultants	CM (Security) / CM (Capital Projects) / School or Section	Gate 3 Planning
Determine number of cameras to be installed	Services consultants	CM (Security)	Gate 3 Planning
Determine location of closest network switch	Services consultants	CM (Security)	Gate 3 Planning
Determine if network switch is in a suitable location for the works	Services consultants	CM (Security)	Gate 3 Planning
Determine if existing network switch has sufficient capacity to cater for the new cameras and other IP devices. *If not, an additional network switch is required.*	Services consultants	CM (Security)	Gate 3 Planning
Determine if the existing network switch has the capability of providing Power over Ethernet (PoE)	Services consultants	CM (Security)	Gate 3 Planning
Determine if there is an existing NVR in the building or if there is an NVR elsewhere that can be used	Services consultants	CM (Security)	Gate 3 Planning
Determine if there is sufficient spare capacity in an existing NVR to cater for the recording of additional VSS cameras	Services consultants	CM (Security)	Gate 3 Planning

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
Determine if existing NVR should be replaced to cater for the new cameras Note: NVR's older than 5 years should be replaced.	Services consultants	CM (Security)	Gate 3 Planning
Check that the field of view of each camera meets the camera's objective	Contractor	CM (Security)	Gate 5 Construction
Check camera focus during both day and night	Contractor	CM (Security)	Gate 5 Construction
Check that camera is recording	Contractor	CM (Security)	Gate 5 Construction
Check that camera is configured correctly	Contractor	CM (Security)	Gate 5 Construction

4 Specifications

4.1 APPROVED EQUIPMENT LIST

EQUIPMENT TYPE	MAKE & MODEL
Access Card	Mifare 4K Contactless Smart Cards
Electronic Access Control - Enclosure	Dual Gallagher Cabinet (Cool Grey), including 8A Power Supply
Electronic Access Control - Intelligent Field Controllers	Gallagher Controller 6000 including either: 8H Module or 4H Module
Electronic Access Control - Expander Modules	Gallagher HBUS 8 IN/4 Out Gallagher HBUS 16 IN/16 Out
Electronic Access Control - Card Reader	Gallagher T15 Multi-Tech Reader (C300480)
Electronic Access Control - Card Reader with PIN	Gallagher T20 Reader
Magnetic Reed Switch	Sentrol 1078C
Heavy Duty Magnetic Reed Switch	Sentrol 2200AH
Cable Transfer Device	Abloy 8810
Electronic Mortise Lock	Lockwood 3572 AM 1 Series 60mm Back Set
Electronic Strike	Padde ES2000
Electromagnetic Lock	Padde Z4 monitored Padde Z8 monitored
Emergency Door Release Unit	KAC MCP4
Push Button (Internal)	Gallagher Touch to Exit (C861200)
Hold Open Devices	Dorma EM Series Dorma EMR/EMF door closer
Wireless Access Control Electronic Locks / Escutcheons with key override	Salto XS4 Escutcheon Wireless lock with Mifare/BLE Online Lock with Key Override & DND
Wireless Access Control units	Salto BLUEnet Wireless RFNODE3
Wireless Access Control Gateway unit	Salto BLUEnet Wireless Gateway X3C
Wireless Access Control Portable	Salto PPD800 Portable Programming Device

EQUIPMENT TYPE	MAKE & MODEL
Programming Device	
Wireless Access Control Encoders	Salto EC904B0AUS Card Encoder
Passive Infrared Detector- 90°	Aritech EV435AM
Passive Infrared Detector- 360°	Aritech DD669AM
Long Range Passive Infrared Detector	Aritech EV 635
Dual Technology Detector	Aritech DD475
Desk Mount- Duress Button	Ademco 270R
Wall Mount – Duress Button	SMART7030R
Wireless Transmitters and Receivers	Innovonics Echostream
Fire Relay Board	Jackfuse PP8PTC Power Distribution & Fire Monitoring Board
VSS- Fixed Dome Camera	Avigilon H5A Dome Camera (4.0C-H5A-D01-IR)
VSS- Fixed Dual Head Dome Camera	Avigilon H5A Dual Head Camera (10.0C-H5DH-DO1-IR)
VSS- Multisensor Dome Camera	Avigilon H5A Multisensor Camera 4 x 5MP (20C-H4A-4MH-360) 3 x 5MP (15C-H4A-3MH-270)
VSS – Bullet Camera	Avigilon H5A Bullet Camera series
VSS- PTZ Camera	Avigilon H5A-PTZ Camera Internal – 4.0C-H5A-PTZ-DC36 External – 4.0C-H5A-PTZ-DP36
VSS – LPR Camera	Avigilon H4 Licence Plate Capture (LPC) Camera (3.0C-HD-LP-B1)
VSS- Network Video Recorder	Avigilon AINVR-PRM-96TB AI NVR Premium 96 TB (120 TB Raw) with Avigilon Control Center
Intercom (Help Point)	Avigilon H4 Video Intercom
Intercom (Standalone- Master)	Avigilon Client application on workstation
Intercom (Standalone- Slave)	Avigilon H4 Video Intercom
Electronic Key Cabinet	Keyhold

4.2 GALLAGHER IFC CABLE AND POINT SCHEDULE

IFC No	
Gallagher Name	
MAC Address	
IP Address	
Termination Location	

Cable ID	Name in Gallagher	Point ID	Device Type	Cable Type	Comments
		Input 1			
		Input 2			
		Input 3			
		Input 4			
		Input 5			
		Input 6			
		Input 7			
		Input 8			
		Input 9			
		Input 10			
		Input 11			
		Input 12			
		Input 13			
		Input 14			
		Input 15			
		Input 16			
		Input 17			
		Input 18			
		Input 19			
		Input 20			
		Input 21			
		Input 22			
		Input 23			
		Input 24			
		Output 1			
		Output 2			
		Output 3			
		Output 4			
		Output 5			
		Output 6			

Cable ID	Name in Gallagher	Point ID	Device Type	Cable Type	Comments
		Output 7			
		Output 8			
		Reader 1			
		Reader 2			
		Reader 3			
		Reader 4			
		Reader 5			
		Reader 6			
		Reader 7			
		Reader 8			
Expander Module					
		Input 1			
		Input 2			
		Input 3			
		Input 4			
		Input 5			
		Input 6			
		Input 7			
		Input 8			
		Input 9			
		Input 10			
		Input 11			
		Input 12			
		Input 13			
		Input 14			
		Input 15			
		Input 16			
		Output 1			
		Output 2			
		Output 3			
		Output 4			
		Output 5			
		Output 6			
		Output 7			
		Output 8			
		Output 9			
		Output 10			
		Output 11			
		Output 12			
		Output 13			
		Output 14			

Cable ID	Name in Gallagher	Point ID	Device Type	Cable Type	Comments
		Output 15			
		Output 16			

4.3 VSS CAMERA SCHEDULE

Camera No.	Camera Description	Category e.g. Observation, Recognition, Identification	NVR ID	Lens Focal Length	Camera Model	Serial Number	Network Switch Location	MAC address

Abbreviations

BAU	Business As Usual
BCA	Building Code Assessment
BMS	Building Management System
BGU	Breakglass unit
CM	Campus Management
COTS	Commercial Off-the-Shelf
DGP	Data Gathering Point
DLP	Defects Liability Period
EACS	Electronic Access Control System
EKMS	Electronic Key Management System
ESD	Environmentally System Design
ESS	Electronic Security System
FIP	Fire Indicator Panel
FFL	Finished Floor Level
GUI	Graphical User Interface
HLI	High Level Interface
HV	High Voltage
IDS	Intrusion Detection System
IFC	Intelligent Field Controller
IP	Internet Protocol
IPxx	Ingress Protection (XX denotes rating i.e. IP56)
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LLI	Low Level Interface
LV	Low Voltage
NCC	National Construction Code
NVR	Network Video Recorder
PIN	Personal Identification Number
PIR	Passive Infra-Red
PoE	Power over Ethernet
PSC	Preferred Security Contractor
PTZ	Pan/Tilt/Zoom
RAS	Remote Arming Station
RAT	Remote Arming Terminal
SGT	Security Group Tag
SMS	Security Management System

UPS	Uninterruptible Power Supply
UWA	The University of Western Australia
VMD	Video Motion Detection
VMS	Video Management System
VSE	Virtualised Server Environment
VSS	Video Surveillance System
WAC	Wireless Access Control
WFAC	Wire Free Access Control

References

AS CA S009	Installation Requirements for customer cabling (AS/CA - AS/Communications Alliance)
AS HB 90.3	The Construction Industry Guide to ISO 9000
AS/NZS 1049.1	Telecommunication Cable - Insulation, Sheath and Jacket – Part 1: Materials
AS/NZS 1049.2	Telecommunication Cable - Insulation, Sheath and Jacket – Part 2: Test Methods
AS/NZS 1099	Tests for Electronic Equipment
AS/NZS 1100	Technical Drawings
AS/NZS 1101	Graphical Symbols for General Engineering
AS/NZS 1102	Graphical Symbols for Electrotechnology
AS/NZS 1170.2	Structural Design Actions- Wind Loads
AS/NZS 1345	Identification of the Contents of Pipes, Conduits and Ducts
AS/NZS 1428.1	Design for Access and Mobility
AS/NZS 1725	Chain-link fabric security fences and gates
AS/NZS 1768	Lightning Protection
AS/NZS 1882	Earth and Bonding Clamps
AS/NSZ 1939	Degrees of protection provided by enclosures for electrical equipment (IP Code)
AS/NZS 2201	Intruder Alarm System (all parts)
AS/NZS 2279	Disturbances in Mains Supply Networks
AS/NZS 2546	Printed Circuit Boards
AS/NZS 27001	Information Technology – Security Techniques- Information Security Management Systems – Requirements.
AS/NZS 3000	Electrical Installations (Known as the Australian/New Zealand Wiring Rules)
AS/NZS 3555	Building Elements- Testing and rating for intruder resistance.
AS/NZS 3901	Quality Assurance Standards
AS/NZS 3905.2	Quality Systems Guidelines
AS/NZS 4145	Locksets and hardware for doors and windows
AS/NZS 4251.1	Electromagnetic Compatibility – Generic Emission Standards
AS/NZS HB167	Australian/ New Zealand Standard – Security Risk Management
AS/NZS HB3	Drawing Standards

AS/NZS ISO 31000 Risk Management- Principles and Guidelines

AS/NZS IEC 60839.11 Alarm and Electronic Security Systems

AS/NZS 61000.3.2 Electromagnetic Compatibility (EMC)

BS EN 61000.6.3 Generic Emission Standards

AS/NZS 62676.1.1 CCTV - General

AS/NZS 62676.1.2 CCTV – Performance requirements for video transmission

AS/NZS 62676.2.1 CCTV – Video transmission protocols

AS/NZS 62676.2.2 CCTV – IP interoperability implementation based on HTTP and REST

AS/NZS 62676.3 CCTV – Analog and digital video interfaces

AS/NZS 62676.4 CCTV – Application guidelines

AS/NZS 62676.5 CCTV - Data specification and Image Quality AS/NZS 61386

Conduit Systems for Cable Management

HB 29 Communications Cabling Manual

HB 167:2006 Security Risk Management

IEC 297 Dimensions of Mechanical Structures of the 482.6 mm (19) series.

ISO 11064 Ergonomic Design of Control Centres

ISO 9000 Quality Assurance Standards

IEC 62676 Video surveillance systems for use in security applications

ISO/IEC 14443A Identification cards -- Contactless integrated circuit cards -- Proximity cards

National Construction Code (NCC)

Change Log

It is envisaged that revisions to this document will be undertaken at intervals of not more than two (2) years. This version differs from the previous version in the following areas:

Section	Title	Description
1.6	Professional services	Inclusion of safety induction.
2.3.4.5	Zone 5 Plant and Equipment	Addition of plant and equipment rooms to be keyed
2.4.2.2	Intelligent Field Controllers	Information regarding IFC's and associated devices (locks, card reader etc.) to be connected to building's essential services board.
2.4.2.11	Automatic Door Interface	Paragraph on override switch on auto doors
2.4.4	Closed Circuit Television (CCTV) Systems	Addition of all CCTV components to be connected to building's essential services board.
2.4.4.1	Network Video Recorders	Amended for clarity
2.4.4.2	Cameras	Amended for clarity
2.4.6	Electronic Key Cabinet	New section on electronic key cabinets
3.0	Checklist for Project team	Refresh of section 3
All	Major update	Significant update to the standard