DOCUMENT CONTROL

Document Name	**UWA Design and Construction Standards: Security Services - F**
Document Status	Final version
Version No.	2.0
Date of Issue	1st June 2020
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 Works, Campus Management

COPYRIGHT

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 Plan 2010* 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 faculty 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 Plan*, *UWA Masterplan*, *Landscape Vision* and *Integrated Infrastructure Strategy*, *University Policy on Alterations to University Buildings*, etc.
- 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, 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 Works, 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 Works, 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 administer the online contractor safety induction. Upon completion the contractor will be issued with a UWA Contractors Safety Induction Card which they are required to carry at all times when working for the University.

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 RELEVANT CODES AND STANDARDS

The installation and equipment shall comply with the relevant Standards, Statutory Authorities and Regulations. The document shall be read in conjunction with the document listed the *References* section to ensure all planning and preparation items are met.

2.2 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 IndigoVision training to work with the UWA CCTV system.
- Have qualified and licensed Agents, Consultants, Technicians and Installers in accordance with the Security and Related Activities (Controls) Act.
- Comply with the UWA Project Guidelines and Management Regulations.
- Comply with all regulations contained in the Occupational Health, Safety and Welfare Act (1984) and associated regulations (1996) during the currency of this contract.
- 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.
- Shall supply, cut in and install the locking hardware devices to complete the project requirement except where otherwise stated.

2.3 DESIGN REQUIREMENTS

2.3.1 General

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

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

- Access Control
- Intruder Alarm
- Alarm Monitoring and Management
- Systems Interfacing

Building entry doors shall be kept to a minimum, preferably one only. Main-entry doors should be automatic sliding doors, including electronically 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.

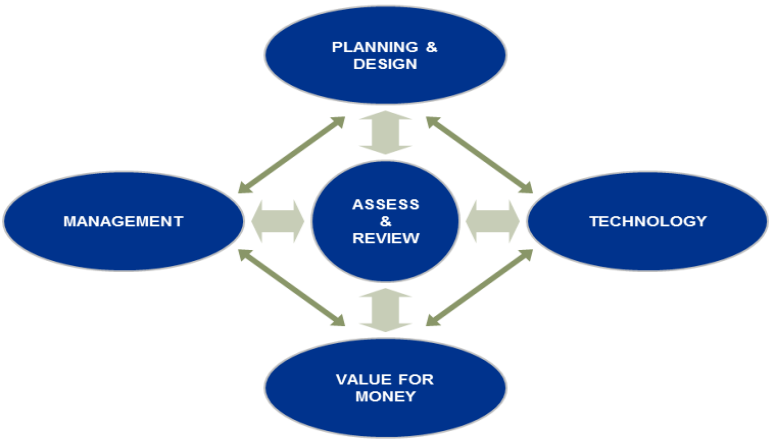
Doors in exit paths may have Hold Open devices to fix the doors in an open position and allow the free flow of traffic during normal hours.

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 Faculty, School or Section occupying the building or area.

2.3.2 Security Philosophy

The UWA security philosophy is based on the principle that “Security is not achieved by technology alone” and that a complimentary design recognises four elements of security is provided. All elements must exist in some form and in a compatible manner to yield the most effective security. These four elements achieving a balanced and comprehensive design solution are shown in the figure below.



Security Philosophy

Management

Management refers to the operational context of how the security function will be organised and managed relative to security, the individuals involved in obtaining and then maintaining a secure environment, the nomination of their primary responsibilities, duties and the like.

The management of security is considered to be the most important of the four controls and is a critical factor in determining the location and responsibilities of the various security controls and equipment rooms and the design requirements of the security systems. Management is such a pivotal role as any security system exists in a constant state of flux. This can be either due to changes in the threat environment but also due to system components wearing down.

Planning and Design

Planning and design refers to the security that is afforded by the way the facility is constructed and/or planned. It includes architectural and building considerations such as Crime Prevention through Environmental Design (CPTED) and Defence in Depth (i.e., multiple layers of security).

It recognises the various user groups within the building and how these groups are segregated, yet where applicable, how these groups interact. This also recognises the movement paths associated with all user groups to ensure that there are no conflicts or compromises.

Planning and Design also considers exterior and interior environment features such as building setbacks, landscaping, footpaths, signage, parking, common areas and the like.

Physical security, taking into consideration building fabrics and materials used in the construction of the buildings, door constructions, door hardware, glazing, lighting, cable access, services access and distribution, protection and redundancy of essential services requirements.

Technology

The technology aspect of security refers to the equipment and/or systems that are provided to assist management in obtaining the level of security necessary to meet the identified risks. The security technology design must be a cost effective and proven solution providing flexibility, connectivity and reliability to all building users, as well as supporting the normal use and workflow of the building. It is important to note that technological solutions should not be used simply because the technology exists. Technological solutions should be applied as part of a layered security approach to complement the organisation or facilities operations, the defined management procedures and buildings design.

Value for Money

Security, including its system components, must provide value for money. Security is often seen as cost centres, sometimes seen as a necessary cost to an organisation. Security should be seen as adding value to an

organisation by ensuring the smooth running of operations of that organisation. In addition all security components of a system should provide value for money over the entire life cycle of the system. This is achieved through utilising systems which are fit for purpose, well supported and can be upgraded or expanded if the need requires. Security components and activities provide value for money by identifying and treating risks before they are realised, reducing workers compensation, preventing loss, reducing labour costs and reducing business interruptions.

2.3.3 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
- Access Control System
- Intrusion Detection System
- Digital Closed Circuit Television (CCTV) System
- Intercom System
- Automatic Barriers

2.3.3.1 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).

2.3.3.2 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.

2.3.3.3 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 prime 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
- Tampering with 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 including but not limited to:
    - Recessed door contacts (reed switches).
    - Duress buttons.
    - Movement detection devices.
    - Inputs from other systems (e.g. fire alarm panel outputs).

The Intrusion Detection System will be configured within the SMS to facilitate the monitoring of all spaces within the building and to initiate responses to cater for all situations with priority being given to all life threatening situations.

2.3.3.4 Digital CCTV System

The Digital CCTV System will be implemented to provide coverage of the following areas:

- Main vehicle entry/exit points
- External areas of the building
- Building entry/exit points
- Internal building spaces used after hours
- High risk/value areas

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

The CCTV system comprises the following components:

- Fixed CCTV cameras
- Pan Tilt Zoom (PTZ) cameras

- Network Video Recorders (NVR's)
- CCTV Workstation software
- Display Monitors

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

All cameras will be recorded on Network Video Recorders at high resolution and retained for a minimum period of thirty-one (31) days. The CCTV system is interfaced to the SMS to allow CCTV footage to be automatically displayed on an alarm monitor in the event of an SMS alarm and/or event.

2.3.3.5 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. The intercoms shall connect to the UWA PABX and when activated, dial the security emergency number.

2.3.3.6 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.

2.3.4 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.

2.3.4.1 Zone 1- Public Space (outside 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 plan nature of UWA.

To assist in the security operations of these areas, general CCTV surveillance and recording shall be provided

throughout these areas, along with strategically located help call points (intercoms). Although 100% CCTV coverage of these spaces is not feasible, CCTV 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.

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

2.3.4.2 Zone 2- Public Spaces (within 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
- Emergency egress door- provides free handle egress 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.

CCTV coverage in these areas shall include:

- Facial identification at all building entry points
- General coverage of lift lobbies
- General CCTV surveillance shall be provided to spaces that are accessible by students after hours.

The objective of CCTV 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.

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

2.3.4.3 Zone 3- Shared Private Spaces

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

- Staff only facilities
- Common teaching venues/spaces
- Laboratories
- Research areas

Entry /exit doors leading into shared private 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.

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

Depending on the use, risk and/or sensitivity of the area, internal movement detection may be required.

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.

2.3.4.4 Zone 4- Individual Private Spaces

Individual private spaces are similar to shared private spaces but are generally used by a small group (3 or less people) or an individual. Ideally these spaces should be located within a shared private space. All individual private 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, internal movement detection may be required.

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.

2.3.4.5 Zone 5- 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. Depending on the criticality of the plant/equipment, CCTV coverage of these areas may also be included.

2.3.4.6 Zone 6- Vertical Access

The security controls used to control 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.

2.4 SECURITY SYSTEM REQUIREMENTS

2.4.1 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.

2.4.1.1 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.

2.4.1.2 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 IT.

2.4.1.3 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

The workstation shall be an HP 8200 Elite with an HP LA2205wg monitor or an approved equivalent with the following minimum requirement:

- i5 or higher CPU
- 4GB RAM
- 500 GB HDD
- 22–inch monitor

2.4.2 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 IFC Cable and Point Schedule shall be submitted to UWA Security for review prior to any new Gallagher installations.

2.4.2.1 Card Readers

The UWA card readers shall be:

- Compatible with the UWA access card format and protocol
- 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 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.

2.4.2.2 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.

Each Gallagher dual cabinet shall include a Gallagher 8A Power Supply and a minimum of four 7AH 12V DC batteries.

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

2.4.2.3 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 safe to unlock in the event that power is removed from

the lock

- 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
- The electronic mortice locks shall be installed 1000mm from Finished Floor Level
- 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

2.4.2.4 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.

2.4.2.5 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.

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.

2.4.2.6 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.

2.4.2.7 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.

2.4.2.8 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.

2.4.2.9 Access Cards

The UWA access cards are Mifare 4K Contactless Smart 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 department or school.

All requests shall include the following:

- Cardholder name
- Visitor/card number
- Building name and number
- Access details like 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.

2.4.2.10 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.

2.4.2.11 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 day mode the doors shall open and close under control of the door PIR sensors.

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

- In night 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 night 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 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 finished floor level.

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

2.4.2.12 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 shall become an integrated part of the Gallagher SMS to provide controlled access at nominated doors.

The WAC shall be based primarily on 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 will be fitted with a Salto Controller and a Gallagher IFC.

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

Cards currently held and used by students will be reprogrammed/reconfigured to allow them to be used at the new 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 Smartcards
- 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 finished floor level.

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.

2.4.3 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.

2.4.3.1 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.

2.4.3.2 Motion Detectors

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

2.4.3.3 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

2.4.3.4 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 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 RAS on site.

A Gallagher Prox Plus Reader 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 PIN.

A Gallagher Remote Arming Terminal (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 LCD text displayed shall provide a clear description of the event.

2.4.3.5 Wireless Transmitters and Receivers

Wireless transmitters and receivers shall be compatible with the existing Gallagher Security Management System 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.

2.4.4 Closed Circuit Television (CCTV) System

Closed Circuit Television (CCTV) 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 CCTV System is based on an Indigo Vision Digital Video Management System (DVMS) which is utilised to control, monitor, manage and record all CCTV cameras. All CCTV cameras shall be connected and recorded to the Indigo Vision DVMS.

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

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

2.4.4.1 Network Video Recorders

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

Recordings shall be at a minimum:

- Resolution of 1920x1080

- 13 frames per second
- Continuous mode recording
- 31 days recording retention on hard disk drive

The NVR shall be configured as RAID5 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 being recording. Where 10 cameras or less are being recorded a minimum of 12TB shall be provided. Where 11 cameras or more are being recorded a minimum of 24TB shall be provided.

No more than 20 CCTV cameras shall be recorded on a single NVR.

Liaise with BITS and/or the Communications Consultant to confirm network bandwidth availability and requirements.

2.4.4.2 Cameras

Placement and mounting of cameras shall be at a height of approximately 3 metres minimum and 5 metres maximum for ease of maintenance. 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.

The adjustment of settings shall include flange ring setting, iris, focus and zoom. Adjustments are to include the use of standard colour TV test patterns to improve fine tuning for maximum image quality.

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 IP based. All cameras installed must include the appropriate licenses to connect and record onto the Indigo Vision DVMS, this shall include the Indigo Vision ONVIF Licence required for non-Indigo Vision cameras.

The lens focal length shall be selected by the PSC to provide the required field of view. The required field of view shall be aligned to one of the following *AS4806.2* categories:

- Face Identification

- Face Recognition
- Detection of an Intruder
- Crowd Control/Monitoring
- Vehicle number plate visual recognition

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

- Camera No
- Description
- AS4806.2 Category e.g. Face Identification
- Network Video Recorder ID
- Lens Focal Length
- Camera Model
- Serial Number
- Network Switch Location
- MAC Address
- IP Address

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 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 an IP65 rating.

Refer to Approved Equipment List for approved external fixed dome cameras.

Pan Tilt Zoom (PTZ) Dome Cameras

Refer to Approved Equipment List for approved PTZ dome cameras.

2.4.5 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 CCTV where are available.

2.4.5.1 Help Point Intercom

Help Point Intercoms shall be a commercial grade direct dialling unit. It shall connect to a PSTN/PABX line. It shall 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 building telephone system.

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

2.4.5.2 Standalone Intercom

The standalone intercom system shall provide clear voice communication and/or video transmission to the local master desk unit. 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 master station and then cascade through other master stations as programmed until the call is answered.

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

2.4.6 Electronic Key Cabinet

The UWA Electronic Key Cabinet System shall be a CQRiT electronic key cabinet which shall be utilised to secure, monitor and manage keys or other small assets. CQRiT electronic key cabinets are available in 4 sizes with 12, 25, 50 or 100 key positions. The size of the cabinet shall be determined by the number of keys and/or small assets being stored within the cabinet, including a minimum of 10% spare capacity.

The electronic key cabinet shall be programmed and integrated to the Gallagher SMS via the existing CQR exchange High Level Interface (HLI) to provide controlled access using the UWA access card. The HLI shall be programmed to

- Automatically import cardholders and access groups from Gallagher into the key cabinet
- Send all transaction data, including alarms, from the key cabinet to Gallagher

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

2.4.6.1 Authentication and Access

Authentication and access shall be via UWA access card reader. The card reader shall be a Gallagher T15 card reader installed and interfaced to the key cabinet. Local PIN code shall only be used for maintenance and admin access.

2.4.6.2 Key rings and tool kit

C.Q.R.iT high security key rings and tool kit shall be provided with the key cabinet to suit the keys to be stored.

2.5 GENERAL CONSTRUCTION AND INSTALLATION REQUIREMENTS

2.5.1 Coordination

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

2.5.2 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.

2.5.3 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.

2.5.4 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 armoring 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 cables including patch leads shall be clearly labelled.

2.5.5 Fire Connection

The FIP shall send a signal to the Security Management System and report as a critical alarm. A Neatrol 8 Pole Fire Relay 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.

2.5.6 Enclosures and Cabinets

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

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 Security Management System.

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.

2.5.7 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 maximize the enclosure capacity. All installed batteries shall be dated and secured in the panel.

2.5.8 Uninterruptible Power Supply

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 by project, provide a single phase UPS that is rated to provide two hours of UPS back-up (at full load) to the CCTV 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.

2.5.9 Systems Integration

All Security Services 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 services systems may have Low Level Interfaces (LLI) and High Level Interfaces (HLI). 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

2.5.10 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

2.5.11 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 Faculty / 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, ACS, CCTV surveillance and DVR system interfacing, icons requirements, Etc.
- CCTV surveillance 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, ACS, CCTV surveillance and DVR system interfacing for all intercom stations.

2.5.12 Documentation and Drawing

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

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 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 UWA from using, copying or referring to them
- Be prepared by a qualified draftsperson

2.5.13 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 Fire Panel or Fire Indicator Board to the IFC fire relay.

2.5.14 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.

2.5.15 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.

2.5.16 Warranty

A warranty for all equipment, materials, works and the like shall be provided for a Defects and 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 Checklist for Project Team

3.1 ELECTRONIC ACCESS CONTROL

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
Assess if EAC is a project requirement	Services consultants	CM (Security) / Client Faculty	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 Works) / Client Faculty	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 • Test Plans and Results • Technical Documents • Configuration details • Manuals and User Guides • Security Drawings	Contractor	CM (Security) / CM (Capital Works)	Gate 6 Handover

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
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

3.2 CCTV

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
Assess if CCTV 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 CCTV design	Services consultants	CM (Security) / CM (Capital Works) / Client Faculty	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 CCTV cameras	Services consultants	CM (Security)	Gate 3 Planning
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	Contractor	CM (Security)	Gate 5 Construction

ACTIVITY	RESPONSIBILITY	STAKEHOLDER(S)	TIMEFRAME
and night			
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, 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
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
CCTV- Internal Fixed Dome Camera	Indigo Vision BX420 HD Vandal Resistant HD Minidome
CCTV- External Fixed Dome Camera	Indigo Vision BX420 HD Vandal Resistant Minidome
CCTV- Internal PTZ Camera	Indigo Vision BX520 In-Ceiling 4MPPTZ Dome
CCTV- External PTZ Camera	Indigo Vision BX520 External Pendant 4MPPTZ Dome
CCTV- Network Video Recorder	Indigo Vision Enterprise NVR-AS 4000 RA12TB (Linux version) or Indigo Vision Enterprise NVR-AS 4000 RA24TB (Linux version)
Intercom (Help Point)	Jacques VDL-411
Intercom (Standalone- Master)	Aiphone JF-2MED

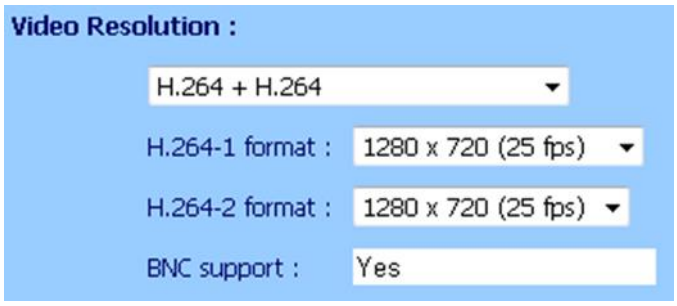
Intercom (Standalone- Slave)	Aiphone JF-DV
Electronic Key Cabinet	CQRiT

4.2 CCTV CAMERA CONFIGURATION REQUIREMENTS

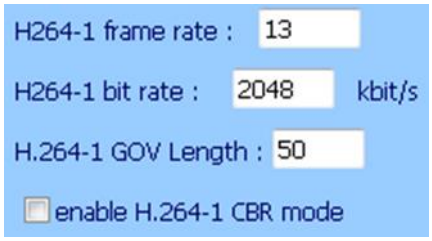
4.2.1 Internal Cameras

IndigoVision

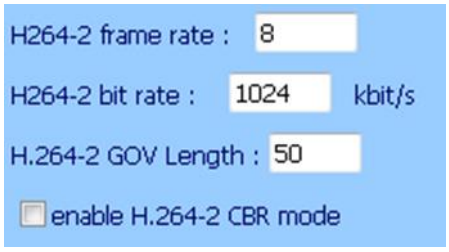
Multi-Encoder



H.264-1 Configuration (Recording)



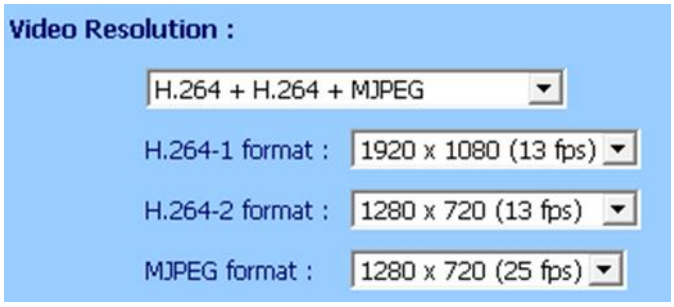
H.264-2 Configuration (Viewing)



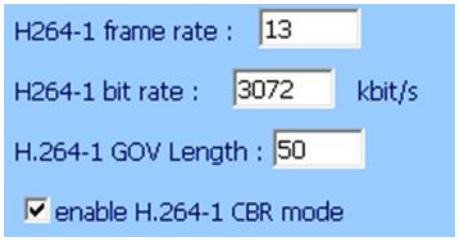
4.2.2 External Cameras

IndigoVision

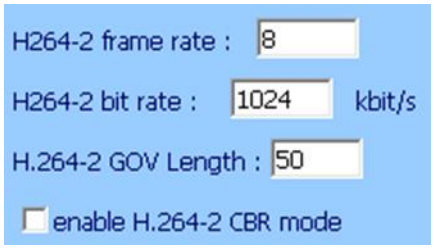
Multi-Encoder



H.264-1 Configuration (Recording)



H.264-2 Configuration (Viewing)



4.3 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			
		Output 7			

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

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

4.4 CCTV CAMERA SCHEDULE

Camera No.	Camera Description	Category e.g. Face ID	NVR ID	Lens Focal Length	Camera Model	Serial Number	Network Switch Location	MAC address	IP address

Abbreviations

ACS	Access Control System
CCTV	Closed Circuit Television
CCR	Central Control Room
CM	Campus Management
CPU	Central Processing Unit
EACS	Electronic Access Control System
FIB	Fire Indicator Board
FFL	Finished Floor Level
HDD	Hard Disk Drive
HLI	High Level Interface
IDS	Intrusion Detection System
IFC	Intelligent Field Controller
IP	Internet Protocol
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LLI	Low Level Interface
NCC	National Construction Code
NVR	Network Video Recorder
PABX	Private Automatic Branch Exchange
PIN	Personal Identification Number
PIR	Passive Infra-Red
PSC	Preferred Security Contractor
PSTN	Public Switched Telephone Network
PTZ	Pan/Tilt/Zoom
RAS	Remote Arming Station
SMS	Security Management System
UPS	Uninterruptible Power Supply
UWA	The University of Western Australia

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/NZS 2201	Intruder Alarm System
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 4806.2	Closed Circuit Television (CCTV) – Application
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 61000.3.2	Electromagnetic Compatibility (EMC)
BS EN 61000.6.3	Generic Emission Standards
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
National Construction Code	

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