CURTIN UNIVERSITY

PROJECT DELIVERY GUIDELINES

SECURITY INFRASTRUCTURE TECHNICAL REQUIREMENTS

000328

Curtin University

Details of revisions			
Level	***Details***	***Date***	***Initial***
1	*Initial version prepared for Project Delivery Guidelines from Security Infrastructure Specification V2.1*	*Jan-17*	*RPS*
2	*Update of technical details Section 3.3*	*Sept-18*	*TC*
3	*Update of Standard Drawings and Numbers* *Inclusion of Bi-Folding Door Requirements 3.3.3* *Update of Lightning Protection 6.7* *Update of Approved Camera types*	*Sept-20*	*TC*
4	*Update of Automatic Door operation in FIRE Mode* *Replace references to Security Infrastructure with Operational Technology*	*April-21*	*TC*
5	*Update of DVMS and CAP requirements* *Update of Approved Equipment*	*Mar-24*	*TC*

CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This document details the minimum requirements for the operational and technical aspects for the supply, installation, interfacing, engineering and maintenance of security services for any Curtin University (Curtin) campus.

It ensures new and refurbished systems are fit for purpose, made from durable, good quality materials, integrate well with existing infrastructure and are cost-efficient to operate and maintain.

This document builds on the information provided in *000327 PDG Security Infrastructure Design Guidelines* that describes the design approach and minimum requirements for security equipment and technologies.

Where reference is made to authorisations/approvals by Curtin or specific departments within Curtin, this also extends to a Curtin-nominated representative.

1.2 CONTRACTOR RESPONSIBILITIES

The security contractor is to:

- supply all materials and services necessary for, or incidental to, the installation and commissioning of the system as specified within this document and shown on the contract drawings, unless otherwise specified:
  - although not specifically shown or specified, supplementary miscellaneous items and devices that are incidental to, or necessary for, the complete operational installation shall be included in the works
- confirm the number and types of equipment/fittings
- ensure the equipment schedule, technical specifications (datasheets) and samples have been approved by Operational Technology, in writing, prior to the placement of orders for the appropriate equipment or any installation work being carried out
- install and interface equipment and systems complying with the relevant Australian standards, National Construction Code and the requirements detailed in this document
- comply with licensing, certifications and registration requirements detailed in the *000327 PDG Security Infrastructure Design Guidelines*
- obtain relevant permits to work via the Curtin 'Working with Us' webpage, https://properties.curtin.edu.au/working-with-us/
- liaise with other and relevant contractors/subcontractors to ensure compatibility of equipment and works with other services, e.g. mechanical, electrical and hydraulic.

CONTRACTOR REPRESENTATIVE

Where the security contractor's representatives are not suitable, the security contractor shall appoint a new representative, at no additional cost to the project.

1.3 AS-CONSTRUCTED DRAWINGS

As-constructed drawings shall be submitted for all modifications made to the security infrastructure at Curtin University. The AutoCAD blocks used to represent security hardware shall be sourced from the Standard Block Drawing (00MISC-SC-ST0001) and the attributes of these blocks shall be fully populated as required. (For drawing standards, refer to the *Curtin CAD Standard*.)

Drawings shall be reviewed by Operational Technology and approved by Curtin Drawing Services drawingservices@curtin.edu.au prior to being submitted as part of the as-constructed documentation.

1.4 INFORMATION TO BE SUPPLIED

As a part of all security works, the security contractor shall, prior to commencing any work on site, provide the following information for review and approval:

a) Construction Program

   The document shall be provided in Microsoft Project format in soft copy and/or in hard copy when requested.

b) Cable Schedule

   Cable schedules for all works shall include but not limited to:

   - IFC number
   - termination location
   - proposed cable number
   - device detail.

   The cable schedule shall be maintained up-to-date and be available for inspection by Curtin. The security contractor shall add information as changes occur, including variations.

c) Block schematic cable diagram detailing system interconnections and cable/core identification. This shall clearly identify the interconnection between each device and the associated Gallagher FT intelligent field controller (IFC).

d) Equipment samples (only for those not included in the approved equipment table).

1.5 STANDARDS AND STATUTORY REQUIREMENTS

The design, quality control, installation and testing of the complete installation shall comply with international standards and local statutory authority regulations, building and fire regulations (and where amended) and shall take precedence over the details provided in these technical requirements and drawings.

RELEVANT STANDARDS

The security contractor is to be fully conversant with all relevant standards including, but not limited to, the following:

National Construction Code (NCC) – formerly known as the Building Code of Australia (BCA)
AS/NZS1170.2 Structural design actions Wind actions
AS1049 Telecommunication Cable – Insulation, sheath and jacket Materials
AS1104 Informative symbols for use on electrical and electronic equipment
AS1345 Identification of the Contents of Pipes, Conduits and Ducts
AS1428 2010 Design for access and mobility
AS/NZS1768 Lightning Protection
AS1882 Earth and bonding clamps
AS/NZS2053.1:2001 (R2016) Conduits and fittings for electrical installations — General requirements
AS/NZS61386.1:2015 Conduit systems for cable management — General requirements
AS2124 General conditions of contract
AS/NZS2201 Intruder Alarm Systems
TR IEC61000.3.7:2012 Electromagnetic compatibility (EMC) Limits — Assessment of emission limits for the connection of fluctuating installations to MV, HV and EHV power systems
AS2546 Printed boards
HB90.3-2000 (R2016)The Construction Industry — Guide to ISO 9001:2000 — The Construction Industry — Guide to ISO 9001:2000
AS/NZS3000 S.A.A Wiring Rules
AS4806 Closed Circuit Television (CCTV)
IEC90297 Dimensions of mechanical structures of the 482.6 mm (19 in) series
AS/NZS ISO9001 Quality management systems
AS1428.1–2009 Design for access and mobility General requirements for access — New building work
AS4085-1992 Automatic sliding door assemblies

1.6 SOFTWARE AND LICENCES

Curtin purchases its security system (Gallagher FT) door licences annually to accommodate the expected growth of the security system. Other software licences for equipment and associated systems shall be provided, supplied and installed as part of the contractor works and shall become the property of Curtin University.

1.7 EQUIPMENT AND DEVICES

A list of approved security equipment and devices is shown in APPENDIX A.

Alternatives to this list are to be submitted to Operational Technology operationaltechnology@curtin.edu.au for review and approval (in writing). Approval for alternative equipment/devices must be sought prior to ordering.

The review/approval process may require demonstrable evidence or factory acceptance testing to show that the alternative equipment/device is compatible with existing systems. This is further explained in APPENDIX C.

1.8 OPERATIONAL TECHNOLOGY

For clarification of details or where a conflict in documents/requirements is identified, contact Operational Technology operationaltechnology@curtin.edu.au.

2 GENERAL REQUIREMENTS

2.1 SECURE INSTALLATION

Curtin facilities are considered to be of a commercial/public standard in regard to all security to be installed. Equipment, materials, installation methods and the quality of work shall be selected, designed and installed in a manner with awareness of the intended environment and purpose.

This shall include, but not be limited to:

- Material and equipment selection shall be suitable for a commercial/public facility.
- The fixings required shall be tamper-proof and uniform throughout the installations.
- Consideration shall be given to heavy-traffic areas and the repeated use of many devices, e.g. locks and hinges, with their selection to be based on their design for such heavy-duty wear and tear.
- The fixing methods, manner of installation, quality of work and the like for equipment and devices shall be suitable for use in a general commercial/public facility.
- Wherever possible, devices shall be flushed-mounted and all services security concealed.
- Devices however, shall remain serviceable without the need to damage infrastructure or finishes.
- Equipment installed within these facilities that are considered by Curtin to be unfit for use in a general environment shall be replaced when requested at no cost to Curtin.

2.2 SYSTEMS INTEGRATION

The works, as described in this document, shall be supplied and installed as part of the contract. Each of the systems shall interface as described in this document to provide a totally integrated security system.

The necessary labour, tools, materials and equipment to install and interface each of the systems, as described in this document, are to be provided. This includes all cabling, cable terminations, system equipment, alarm inputs, control outputs and programming to integrate all systems using high and/or low level interfaces.

2.3 SUPPLIERS/INSTALLERS

The specified security services and systems equipment shall be obtained from the manufacturer/supplier, unless otherwise stated. The equipment shall be installed by the security contractor or by the supplier or specialist sub-installer, as recommended by the manufacturer and/or supplier.

The security contractor shall not rely on a single source (i.e. the supplier, manufacturer or subcontractor) for various components of each system. The security contractor shall

procure equipment and/or resources from other sources, as directed by Operational Technology.

The works shall be carried out under the direct supervision of the security contractor, who shall remain solely responsible for the correct installation and operation of all equipment supplied and installed as part of the contract works.

3 SECURITY MANAGEMENT SYSTEM ELEMENTS

This section provides an overview of the components that make up the security management system (SMS) at Curtin.

3.1 SECURITY MANAGEMENT SYSTEM

The SMS is the Gallagher "Gallagher" FT Command Centre System and access control system with secure network access across the Curtin Security VLAN.

The SMS provides the alarm gathering, monitoring, alarm inputs, output control, operator interface/management, high level interface, low level interface and the like, that interface and integrate the following security service systems and other building and administration systems:

- lift access control systems (LACS) equipment and interfacing to meet the requirements of the lift controllers
- digital video management system (DVMS) image capture, storage, retrieval, alarm monitoring and integration
- intercom system for all call logging and response at Curtin University is commonly referred to as the campus assistance point (CAP) system
- intrusion detection system (IDS) for intruder alarm management
- building management system (BMS) and other nominated systems such as the fire system
- photo ID system.

The operation and alarm reporting functions of the SMS operate using a combination of text and graphics-based user interfaces distributed via the Curtin Security VLAN, utilising the infrastructure between all sites/facilities as well as providing secure access to other nominated sites.

Card access functions are managed using a locally supported smart-card technology.

3.1.1 SMS WORKSTATIONS

The SMS workstations manage all functions, with full control and monitoring of:

- access control devices (e.g. card readers, request-to-exit push buttons, electric locks and strikes, door magnetic reed switches, emergency door release units, magnetic locks and electronic hold open devices, lock monitors) connected to the access control system (ACS)
- control inputs and outputs, including high level and low level interfacing to the BMS and other nominated systems
- logging and reporting functions, including facilities to enter reportable incidents by way of text-based data record management using definable data-entry fields, e.g. date, time, building, offence, officer
- alarm handling and reporting with full audit logging of all system activities
- intrusion detection system arm/disarm and reporting

- campus assistance points (CAPs) and answering calls from these.

3.2 ACCESS CONTROL SYSTEM

The access control system (ACS) is a function within the SMS that assists in the control and monitoring of authorised access to select areas or buildings.

The ACS allows the access and egress through controlled doors. This occurs by a card reader, PIN, remote door control panel, the SMS operator or a locally mounted door release push button or micro-switch in the electric mortice lock.

The ACS interfaces with other security systems and devices using intelligent field controllers (IFCs) to record all systems and activities and provide the necessary operator interfaces.

3.2.1 INTELLIGENT FIELD CONTROLLER

The following aspects are requirements:

- The IFC shall be a Curtin-approved Gallagher FT intelligent field controller.
- The IFC shall send device status information and accept control commands from the SMS server.
- The IFC shall be fitted with two ethernet ports providing alternative communication capability.
- As a minimum, all inputs shall be 'end-of-line resistor' monitored and can provide four-state monitoring in the form of normal, alarm and tamper (open or short) conditions. The use of any circuits using other than dual 4k7 end-of-line resistors must be approved by (Operational Technology).
- Site items associated with a door, logic block, elevator car, interlock group or alarm zone shall be connected to the same local IFC. Cross-wiring of a device to multiple IFCs is not acceptable.
- Each output shall consist of a single pole, double-throw relay contact with a rating of one amp minimum.
- The IFC shall operate from a separately fused battery-backed 13.6 V DC supply.
- It shall be possible to disable individual or groups of alarm inputs and control any output via the SMS workstation, on a time schedule or event basis.
- During the suppressed alarm mode, the alarm point wiring shall be monitored to detect any unauthorised tampering (i.e. tamper alarms shall be monitored 24 hours a day, every day).
- The IFC shall include tamper protection for the front and back of the panel. The front panel shall be tamper-protected for the door opening, and the back of the panel to detect if the panel has been removed from the wall. These shall use optical tamper detection. Mechanical tamper devices are not acceptable.
- Each IFC shall be connected to the fire indicator panel (FIP) relevant to the building it is being installed in. Where a door becomes part of an egress path from one building to another, that door shall be connected to both FIPs via a separate relay directly connected to the secondary FIP.

- IFC power supplies shall have a minimum of four, seven amp-hour batteries.
- To ensure future growth of the system, all new IFCs, when installed, shall only be populated to a maximum of 80 per cent capacity, unless otherwise directed by Operational Technology. Each IFC shall be provided with a high density input/output (I/O) board, regardless of the number of inputs and outputs initially being connected to the IFC, unless otherwise directed.

INTELLIGENT FIELD CONTROLLER CABINETS

IFCs are to be located within an approved Gallagher dual cabinet in a nominated position within a Curtin communications room, unless otherwise agreed to by Operational Technology. If no such room exists, then an alternative secure location must be made available and agreed to by Operational Technology prior to the release of the tender request of contract documentation.

IFCs are to be provided with a 240 V double general purpose outlet (DGPO), which is to be located internally in the cabinet. The DGPO shall be on a dedicated circuit to which the cabling shall be 1 x 2c+e, 2.5 mm^2 PVC/PVC. In situations where multiple cabinets are to be installed in a common location, the DGPO for each cabinet can be connected to a single dedicated circuit. (Refer to Section 5.6.2 Equipment Panels for further information.)

All IFCs are to be arranged as per the IFC Standard Elevation & Fire System Integration Drawing 00MISC-SC-ST0002.

3.2.2 MONITOR AND CONTROL

The system shall monitor and control a wide variety of input alarms and output controls including, but not limited to:

- card readers
- electric contact magnetic reed switches
- request to exit push buttons
- door open/closed and door unlocked/locked using concealed monitor reed switches appropriate for the door installation:
  - the inactive leaf door shall also be monitored for door open/closed
  - the inactive leaf door monitor switches may be connected as part of the active leaf door monitoring
- magnetic door holders and locks (i.e. both open and closed operations)
- intrusion detection systems
- security devices (e.g. movement detectors, request for assistance push buttons, tamper alarms)
- card reader keypads for PIN assignment
- break-glass alarm devices (i.e. hard-wired emergency door release units)
- lift interfaces
- electric strikes

- intercom call points
- vehicle barriers
- fire panel interface.

The door control relay energise time shall be flexible and controllable from the operator's terminal.

The door monitoring inputs shall be shunted during a valid entry or exit, but shall provide an immediate alarm indication when a door is forced open. This shall be reported as a "Forced Door" alarm.

To prevent nuisance forced door alarms, all access controlled doors will have both an appropriate door open sensor and lock sensor. The key override monitoring shall not be connected unless otherwise directed.

Where the door is opened during a valid entry or exit and held open for longer than a predetermined time a "Door Open Too Long" alarm shall be raised via the security management system. (Refer to the section: Door Warning Sounders.)

When communications between any IFC and the server is disrupted, the IFC shall continue to work offline. Valid cards shall still be screened for authorised entry, initiating status control and alarm messages.

3.2.3 DOOR AND MONITORING OPERATION

The hardware, software and equipment shall be provided to ensure that each of the doors and other nominated devices listed operates in the manner indicated in this specification and as shown on the drawings.

Doors connected to the ACS shall meet the appropriate access, egress, disability and emergency requirements for each door as required by the National Construction Code and fire regulations.

The door hardware shall be compliant with the Curtin Door Standard and/or with the approved lock hardware specified for the building.

Written notice is to be provided that the doors directly connected and powered by the SMS/ACS are compliant with all regulations, codes and guidelines.

Any vents, grates and access points cut into any door controlled by the SMS/ACS shall not allow general access through the door.

3.2.4 LIFT SYSTEM INTERFACE

Unless otherwise specified, the lift access control system (LACS) shall operate via a low level interface (LLI) to the lift system; as further specified in this document. During the course of the project design phase, any opportunity for a full HLI should be investigated and options provided for review.

Unless otherwise specified, the lift interface shall give the security management system (SMS) the ability to secure and allow access to all available lift levels separately.

The security contractor shall coordinate, with the nominated lift subcontractor and Operational Technology, the exact location and final mounting of each device, cabling and terminations.

The security contractor's scope of works for the lift system shall include the following:

a) the supply and installation of:
   - card readers (install only)
   - cables associated with the termination between the security IFC and the lift controller
   - level select output relays installed close to the lift controller or lift trailing cable.
b) Undertake all cabling and termination between the security IFC and the lift controller located within the lift shaft or at nominated locations, as directed by the lift subcontractor to maintain suitable maintenance access and connectivity to the lift controller.
c) Coordinate with the lift subcontractor to attend the site to commission the interface between the security and lift systems and undertake the final witness testing.

3.2.5 THE LIFT SUBCONTRACTOR

The lift controller units and security IFCs shall be intelligent modules to allow the selection of designated level(s) only allocated to access configuration for each person(s).

Each security IFC shall have the capacity to fully monitor all lift control and monitoring inputs and outputs (I/O), in addition to a minimum of two lift card readers, or any mix of additional I/Os and card readers.

Additional I/Os to and from the IFC shall be provided within the lift car to cater for monitoring of alarms (e.g. tamper, duress, call assist, and overload). Allow four only spare alarm inputs for the lift car for these applications.

The interface between the lift controller units and the security IFCs shall be via a low level interface, unless otherwise instructed by Operational Technology, for a high-level interface.

The interface shall allow the operation of the lift car to change status from 'normal' operation mode to 'secure' operation mode and vice versa, between the lift system and SMS. Manual key activation of mode changes within the lift car will not be acceptable to perform this function. However, where the lift allows for such a key, the key shall be keyed to the Curtin University Access Control Area Master Key.

The lift system shall control and assign variable time zones of insecure to secure modes. The SMS shall implement access for users validating their access cards at the card reader and allow access to their designated floors.

The SMS shall be configured to control the nominated lift car to selected levels, via access restrictions or programmable time scheduling of access readers, as directed by Operational Technology.

Lift safety codes are to be met for the release of the lift car for all fire and safety requirements, regardless of the access control system.

The nominated lift subcontractor shall be engaged to provide:

- trailing cables for security equipment, e.g. card readers, CCTV cameras, intercoms
- the 240 V AC power supply
- I/O for interfacing for all floor selection push buttons and floor indicators
- the required cut-outs for the security devices.

The lift subcontractor is to reticulate trailing cables to the lift controller motor room locations or to the nominated location of the lift controller for termination by the nominated security contractor.

3.2.6 CLASSROOM DOOR AND INTERFACED SYSTEMS OPERATIONS

Some classrooms have two points of entry/exit. In these situations only one entry/exit shall be provided with a card reader, unless otherwise requested. The entry/exit points can be configured to operate separately or synchronously as required.

The action of the valid card read shall unlock/lock the associated door as appropriate for the action taking place.

In the case of an 'override' being applied to the classroom by either the card reader or from the SMS, the door shall unlock and any associated doors shall also unlock. Overrides of this type are to be for a set time period as agreed to with the user group and Operational Technology.

Controlled classrooms may have a number of tasks attached to the activation of a valid card read. Nominated classrooms or card readers shall provide activation/deactivation through the building management system (BMS), or another appropriate system, of the environmental room control and lighting. The security contractor shall carry out all interfacing and programming to meet the full requirements of these systems, or engage a subcontractor who is already registered with and inducted to work at Curtin and proficient with the system being interfaced.

Where applicable, the intrusion detection system in the room shall disarm for the period of the override being applied and all environmental systems shall activate. The SMS/ACS, BMS and any other required systems shall provide all reporting and status of the room at that time.

On completion of the room use, the door shall lock and any associated doors shall also lock. Where applicable, the intrusion detection system shall arm and the appropriate environmental systems shall deactivate. The SMS/ACS, BMS and any other required systems shall provide all reporting and status of the room at that time.

3.2.7 INTERCOM SYSTEM INTERFACE

Slave intercom housings shall be monitored by the SMS to provide tamper alarms.

Slave intercom calls shall be routed via the SMS workstation. Should the workstation be unavailable the call should be answerable via the failover master station.

The SMS shall provide a signal to the digital video management system (DVMS) to allow for higher recording rates (alarm) during intercom calls or tampers, where coverage of an intercom unit is provided.

3.2.8 LOCK CONTROL AND MONITORING DEVICES

3.2.8.1 *General*

Installed equipment must be as per the Curtin University Approved Equipment Schedule (APPENDIX A), unless otherwise approved in writing by Operational Technology.

The contractor shall supply the hardware devices for the electric locking, power transfer and the like for the equipment details in the schedule, except where otherwise stated.

The contractor shall cut in and install the door hardware.

The contractor shall terminate and test the installed equipment.

All works, equipment and material shall meet the requirements of this document.

3.2.8.2 *Door Hardware and Door Furniture (Ironmongery)*

The contractor shall ensure the door furniture (ironmongery) including all split spindles, cams and the like are provided for the electric locking devices installed in the door to operate as described in the specification or indicated on the drawings.

The door hardware shall be compliant with the standard AS1428.1.

The door furniture lever type shall be as per the Approved Equipment Schedule (APPENDIX A).

The contractor shall inspect all security works and inform Operational Technology in writing of any deficiencies in the nominated security works to ensure no delays occur for lockdown of the building.

3.2.8.3 *Electric Locking Devices*

The lock devices shall be as per the Approved Equipment Schedule (APPENDIX A).

The electric mortice lock shall be complete with:

- exit hub switch
- lock monitor switch
- power on to lock configuration for all internal doors (fail safe), unless otherwise stated
- power off to lock configuration for all external doors (fail secure), unless otherwise stated
- free egress operations (unless otherwise configured with a push button or an exit card reader).

The electric mortice lock type shall be suitably configured to provide access control in one or both directions as required.

Where only one card reader is shown on the associated drawings with an electronic lock, then free-egress type operations shall be provided with egress handle operations shunting the door reed switch and dead-latch monitor for a predetermined time.

If the use of an electric strike has been requested and agreed upon by Operational Technology, then:

- the lock sense input configuration shall incorporate both the latch and strike micro-switches connected in series and the open sensor shall comprise a separate reed switch located in the head of the door
- a mechanical '3570 series' mortice lock shall be used as the locking device on the door
- the mechanical door lock shall utilise the 'communicating door latch' function (both inside and outside handles are to be always locked and key override is via a cylinder with an X-type cam)
- where only one card reader is shown on the associated drawings as a push button (RX) device it shall provide free egress, and an emergency door release unit (EDRU) shall also be provided
- valid access by card reader or egress by a push button shall shunt the door reed switch and lock sensor for a predetermined time.

The electromagnetic lock shall be complete with:

- a door status indicator
- a power on to lock configuration
- bond sense monitoring.

Installed devices shall be tested and fully operational following installation and connected to the access control system (ACS).

Operational Technology shall be advised, in writing, of any door that affects the security operational requirements prior to their commissioning.

Cabling to the electric locking devices shall be a minimum 8-core 14/0.20 security cable (white in colour).

3.2.8.4 *Access Controlled Door Lock Cylinders*

Electronic doors are to be provided with an override cylinder, keyed in accordance with the Curtin University Security Master Keying System with X-type cams. Requests for cylinders are to be via the Security Technical Office (securitytechoffice.edu.au) who will provide the cylinder for installation. A door schedule and floor plan(s) are to be provided at the time of the request and no later than five weeks prior to the required date of installation. (Refer to the Process for Ordering Cylinders and Keys for Curtin Projects.)

Lockable strap bolts are to be provided with an override cylinder, keyed in accordance with the Curtin University Security Master Keying System with a suitable cam for an ADI lockable bolt, with stamping to be confirmed by the Security Technical Office.

3.2.8.5 *Cable Transfer Device*

The cable transfer device shall be as specified in the Curtin University Approved Equipment Schedule (APPENDIX A), or approved equivalent, fully recessed into the doorframe and the hinge face of the door.

The cable shall be looped from the doorframe through the steel coil, which shall recess into the door and doorframe in the closed position.

A concealed cable transfer device shall be provided where cable access to electronically operated mortice locks on all doors and electrically operated strikers on double-leaf doors are required.

3.2.8.6 *Magnetic Switches*

The magnetic reed switch shall be fully recessed into the doorframe and door at the top edge of the leading end of the door to monitor the door's open/closed status. The magnetic reed switch shall be recessed such that the door does not touch the reed switch when the door is opened or closed. The reed switch shall be secured (limited adhesive) to ensure that it cannot be picked out of the doorframe.

The block-out for the reed switch shall be inspected prior to installation to ensure it provides the space for the cabling and the device and that it may be secured correctly when removed for maintenance, and easily replaced.

Cabling shall be recessed within the doorframe, desktops and conduit.

Double leaf doors shall be monitored by a single input.

Cables shall be terminated at the device end using soldered connections and finished using heat shrink to cover all exposed wires, joints and resistors.

Magnets shall be secured (limited adhesive) in place.

Reed switches shall:

- be a fully sealed reed contact type
- operate with a door gap of 25 mm or less
- be installed such that the magnet and switch are concealed when the door is closed
- have end-of-line monitoring by the IFC.

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

The installation of the device shall ensure that it is not exposed to any possible damage from vehicle movements and all trailing cables are to be securely protected within steel conduit.

The magnet portion of all switch assemblies shall be located on the moving portion of any barrier to eliminate the need for extended trailing cables.

Fire door reed switches shall be of the appropriate type to meet the fire rating of the door, or an approved equivalent.

End-of-line resistors shall be installed to manufacturer's requirements.

Cabling shall be terminated and labelled at both ends.

Cabling for the reed switch shall be a minimum 4-core 14/0.20 security cable (white in colour).

3.2.8.7 *Request to Exit Push Button*

The push button unit shall be as specified in the Curtin University Approved Equipment Schedule (APPENDIX A).

Devices shall be mounted at 1,000 mm above the finished floor level (FFL) to align with other services installed at the door including the card reader, EDRU and light switch.

Cabling for the request-to-exit button shall be a 4-core 14/0.20 security cable (white in colour).

3.2.8.8 *Emergency Door Release Unit*

The Emergency Door Release Unit (EDRU) shall be as specified in the Curtin University Approved Equipment Schedule (APPENDIX A).

The cabling to the associated electric locking device shall be via the EDRU unit such that the operation of the EDRU shall unlock the electric locking device regardless of system status. The EDRU shall drop positive power off the lock and not the negative.

All EDRU activations shall be separately monitored by the ACS via a second contact set within the EDRU. On activation of the EDRU, the local door sounder shall be activated and an alarm generated in the ACS.

The EDRU shall be mounted at 1,000 mm above FFL to align with other services installed at the door including the card reader, push button, and light switch. Wherever possible, the EDRU shall be flush-mounted into the wall.

The EDRU shall NOT be placed in the door properties within the SMS emergency release.

Cabling for the EDRU shall be a minimum 4 core 14/0.20 security cable (white in colour).

3.2.8.9 *Card Readers*

Card readers shall be as specified in the Curtin University Approved Equipment Schedule (APPENDIX A).

Card readers shall be installed with all ancillary items and be IP65 rated for external installation.

Card readers shall be mounted at 1,000 mm above FFL to align with other services installed at the door and to meet the requirements of the Universal Design Guideline.

Both the card reader and the protective cover (where required) are to be secured using security screws, as per the manufacturer's specifications, so that they do not have any movement or 'play' and maintain their IP rating once installed.

Card readers shall provide visual and audible indication of a successful card read, (both granted and denied).

It shall not be possible to open the door controlled by the card reader by tampering with the reader or its wiring.

Card readers shall contain no wiring for activation of the following control devices:

- electric mortice locks or strikes
- magnetic door locks or holders
- lock monitors
- door reed switches
- emergency door release units (EDRU)

- request-to-exit (PB) push buttons
- other systems interface inputs/outputs.

Cabling for the card readers shall meet the manufacturer's requirements.

Where requested, vandal-resistant enclosures having an impact rating of at least IK08 shall be provided and:

- shall be fixed to the wall surface using tamper-resistant screws
- shall have bevelled edges to limit the ability for persons to use the reader as an aid to climbing the building
- other external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.

Cabling for card readers shall be via white CAT 5 or CAT 6 UTP stranded cable, cabled back to the intelligent field controller (IFC).

3.2.8.10 ***Door Warning Sounders***

Door warning sounders shall have a sound level of not less than 90 dB(A) and not greater than 130 dB(A) measured at one metre and shall sound for a period not longer than five minutes. Subsequent sounding of the audible alarm for a further period of up to five minutes shall only occur where:

- the alarm has been reset; or
- subsequent alarms are generated.

Door warning sounders are to be mounted on the secure side of the door, within a Clipsal wall box, (or similar) which shall be flush-mounted to the ceiling wherever possible. A blank face plate shall be used to conceal the sounder. If there is no usable ceiling space, the door warning sounder shall be installed on the wall above the door and be flush-mounted in a similar manner, unless otherwise agreed to by Operational Technology.

Unless otherwise specified, the door warning sounder shall annunciate in the following scenarios:

- After the access controlled door has been left open or unlocked for 20 seconds — a 'Door Open Too Long' (DOTL) alarm shall only be generated and displayed on the SMS alarm viewer as a medium priority alarm after 45 seconds. The alarm shall escalate to a high priority alarm after 240 seconds.
- After the door is forced — the alarm shall appear in the alarm viewer immediately.
- After the EDRU is activated — the alarm shall appear in the alarm viewer immediately.
- After the alarm(s) are acknowledged or become inactive — the door sounder shall turn off.

Door sounders shall not annunciate during the event of a fire alarm.

3.3 AUTOMATIC SLIDING DOOR INTERFACE

Access controlled automatic sliding doors shall be interfaced to the ACS as per the following device functional description requirements and the drawing relevant to the type and location of the door being installed.

3.3.1 DEVICE FUNCTIONAL DESCRIPTION – AUTOMATIC SLIDING DOORS

Each device, if fitted to an automated sliding door, shall be installed and shall operate in the following way:

3.3.1.1 *Door Control Key Switches*

The electronic key switches shall have four modes. The operation shall be as follows:

- OPEN key position – the door drives open and stays open. The "OPEN" key position has priority over the security system.
- EXIT key position – the door is closed and locked and only permits exit via the internal motion sensor, exit card reader, emergency door release unit or egress button. The EXIT key position has priority over the security system.
- AUTO key position (and connected to the ACS) – the door is controlled by a security system and is either secure 24/7 and only operates on a security system activation with motion sensors disabled, or is secure after hours, operates on a security system signal activation only and operates on the automated doors motion sensors during programmed day hours.
- AUTO key position (and not connected to the ACS) – the door operation is controlled by the motion sensors or, if fitted, by Request to Exit buttons.
- LOCK key position – the door is closed and locked and does not accept any signal from the motion sensors, safety sensors or ACS. Activation of the emergency door release unit must remain enabled.

All door control key switches are to be monitored by the SMS.

3.3.1.2 *Fire Alarm Input*

Upon receipt of a fire alarm signal (input) the automated or actuated door must operate in the following way:

EXTERNAL DOORS

- All external automated sliding doors are to automatically allow egress on a fire alarm signal.
- All external automated sliding doors shall operate in accordance with the National Construction Code (NCC). These doors shall open and hold in the open position:
  - The ACS mode changes to 'Lockdown', which cancels any overriding time zone and allows only select authorised users to enter the area through the door.

- The exit motion sensor is enabled.
- The entry motion sensor is disabled.
- The Request to Exit (REX) button is enabled.
- The emergency door release unit is enabled.
- The exit card reader is enabled (where fitted).

A single fire alarm interface relay with an integral red LED shall be located at every automated door as part of the LED mimic panel. Each individual fire relay shall be monitored 24/7 via the security management system. An active fire alarm must override the LOCK and AUTO position of the door control key switch.

All door open too long (DOTL) alarms, forced door alarms and any associated sounders/sirens shall be disabled until the fire alarm signal is reset to the normal state.

INTERNAL DOORS

All internal automated sliding doors:

- the entry motion sensor is enabled
- the exit motion sensor is enabled
- the entry and exit card readers are enabled
- the fail-safe electronic lock must release.

A single fire alarm interface relay with an integral red LED shall be located at every automated door as part of the LED mimic panel. Each individual fire relay shall be monitored 24/7 via the security management system. An active fire alarm shall override the LOCK and AUTO position of the door control key switch.

All door open too long (DOTL) alarms, forced door alarms and any associated sounders/sirens shall be disabled until the fire alarm signal is reset to the normal state.

Doors in general corridors and passageways shall drive open and remain in the open position until the fire signal is reset to the normal state.

Doors that form part of a smoke/fire barrier shall remain closed and allow entry/egress via activation of entry/exit motion sensors until the fire signal is reset to the normal state.

Doors that give access to a 'High Secure Area' shall remain in 'Secure Mode' (Not 'Lockdown') until the fire signal is reset to the normal state.

3.3.1.3 *Emergency Door Release (EDRU)*

On activation of an emergency door release unit, the following shall occur:

- Raise an immediate alarm signal on the security management system.
- The exit motion sensor and/or 'push & go' feature must be enabled.
- Trigger the automated door to momentarily open.
- Override the LOCK and AUTO positions of the door control key switch.
- Fail-safe electronic locks must release.

- Door open too long (DOTL) and forced door alarms and associated sounders must remain enabled.
- The automated door must not remain 'held open'.

3.3.1.4 *Automated Door - Integral Motion Sensors*

All integral motion sensors shall be automatically enabled when the following conditions are met:

EXTERNAL DOOR

- Entry motion sensor
  - During business hours (unless access controlled – to follow the security management system schedule).
- Exit motion sensor
  - Active fire alarm
  - Emergency door release unit activated
  - During business hours (unless access controlled – operates via the associated request to exit button or card reader).

INTERNAL DOOR

- Entry motion sensor
  - Active fire alarm
  - During business hours (unless access controlled – to follow the security management system schedule).
- Exit motion sensor
  - Active fire alarm
  - Emergency door release unit activated
  - During business hours (unless access controlled – to follow the security management system schedule).

Internal automated doors must 'hold open', unless they form part of a smoke/fire barrier or give access to a 'High Secure Area'.

3.3.1.5 *Card Readers*

Presenting an authorised access card at either the entry or exit card reader shall momentarily unlock and open the automated door in one action. Enabling of the motion sensor only is not acceptable.

3.3.1.6 *Request to Exit (REX) Buttons*

Pressing a Request to Exit (REX) button must momentarily unlock and open the automated door in one action. Enabling of the motion sensor only is not acceptable.

Holding the REX button in shall not hold the automated door open.

3.3.1.7 *Forced Door and Door Open Too Long*

Forced door and Door Open Too Long (DOTL) alarms must be enabled 24/7 unless the following conditions occur. In this instance, the alarms will be deactivated until the condition has been reset to the normal condition:

- Fire alarm active
- Override time zone active.

If any automated door is opened without the use of an authorised access card, motion sensor or emergency door release unit, it shall generate an alarm on the security management system and annunciate on the card reader/remote arming terminal and door sounder.

If any automated door is held open past the pre-determined time, the card reader and door sounder shall emit an audible tone and an alarm shall be sent to the security management system.

DOTL alarms shall incorporate a pre-warning time to notify the local user to close the door before the alarm is activated. DOTL and pre-warning times are set globally by the security management system.

The sounder shall be incorporated into the Door Mimic Panel.

3.3.1.8 *Door Locked Alarm*

When an automated door control key switch has been turned to the LOCK key position, it must generate an alarm on the security management system. Door locked alarms must be enabled 24/7.

3.3.1.9 *Fire Test Key Switch*

The fire test key switch must meet the following requirements:

- secured on the Door Mimic Panel in a way to prevent the key switch assembly from loosening itself due to normal use
- 12-volt DC illuminated with red LED during test or fire mode and green LED in normal mode
- keyed to the Curtin master key system
- key cannot be removed when in test position
- when active, must trip the fire relay and place the automated door into fire condition mode.

3.3.1.10 *Door Mimic Panel*

The Door Mimic Panel (DMP) shall provide a uniform, standardised and clearly defined demarcation connection point between the automated door, security management system and the fire alarm panel whilst ensuring the services are electrically isolated from each other. The DMP shall assist services to efficiently diagnose faults and to maintain

and test the services that are interfaced with the automated door. The DMP shall provide a quick and easy means to identify the current condition (state) of incoming and outgoing signals.

The DMP shall provide the following minimum functionality:

- fire test key switch – to simulate a fire alarm locally at the automated door
- LED indicator lights
  - fire test red LED. This LED shall be illuminated when either the fire test key switch is activated or the door is in fire alarm condition mode.
  - fire system interface 'normal' green LED fed from the fire alarm interface relay. This LED must be illuminated when no fire alarm signal is present.
  - 'Door Locked' red LED fed from the automated door controller. This LED shall be illuminated only when the door is in the fully closed and electrically locked position.
  - 'Day Mode' amber LED fed from the security management system business hours control relay. This LED shall be illuminated when the door is in free access mode.
  - 'Open' amber LED fed from the security management system door open control. This LED shall be illuminated when a signal from the security management system is instructing the door to open.
  - EDRU activation red LED fed from the emergency door release unit relay. This LED shall be illuminated when the EDRU has been activated.
- Incorporated 'Forced Door' and 'DOTL' sounder.

3.3.2 OPERATIONAL DESCRIPTION – AUTOMATIC SLIDING DOORS

3.3.2.1 *External Automated Sliding Door*

The external automated sliding doors shall operate under the listed conditions in the following way:

- Lock output
  - operates regardless of the mode or state, when the door is fully closed and in the locked position.
- Open output
  - operates regardless of the mode or state, when the door is not fully closed.
- Key Override output
  - on when the key override is in Open, Exit or Lock position
  - off when the key override is in Auto position.
- Fire alarm input (highest priority)
  - When active, the door shall enable entry, exit motion sensor and unlock the door.

- When inactive, the door shall return to the previous state prior to the fire alarm.
- The fire alarm input must override all other modes or input signals.
- Open input shall open the door.
- When Active, shall hold open the door, unless they form part of a smoke/fire barrier or give access to a 'High Secure Area'.

- Open input (Medium priority)
  - When active, the door shall unlock and open.
  - When inactive, the door shall close.
  - The door shall remain open while this input is active.
  - The Open input shall take priority over the Lock input.
- Lock input, day/night mode (Low priority)
  - When active, the door shall close, lock and disable all motion sensors.
  - When inactive the door shall unlock and enable all motion sensors and remain in the closed position.

3.3.2.2 ***Internal Automated Sliding Door***

The internal automated sliding doors shall operate under the listed conditions in the following way:

- Lock output
  - operates regardless of the mode or state, when the door is fully closed and in the locked position.
- Open output
  - operates regardless of the mode or state, when the door is not fully closed.
- Fire alarm input (Highest priority)
  - When active, the door shall enable entry, exit motion sensor and unlock the door.
  - When inactive, the door shall return to the previous state prior to the fire alarm.
  - The fire alarm input shall override all other modes or input signals.
  - Open input shall open the door.
  - When Active, shall hold open the door, unless they form part of a smoke/fire barrier or give access to a 'High Secure Area'.
- Open input (Medium priority)
  - When active, the door shall unlock and open the door.
  - The door shall remain open while this input is active.
- Lock input (Low priority)

- When active, the door shall close, lock and disable all motion sensors.
- When inactive, the door shall unlock and enable all motion sensors and remain in the closed position.

3.4 BI-PARTING AUTOMATIC DOORS

Where an automatic door is required to be installed in an opening that the installation of an automatic sliding door does not meet requirements for Disability Access, a bi-parting sliding door shall be installed. These doors shall be installed and programmed in the same manner as the automatic sliding door.

3.4.1 ACTUATED SWING DOORS

Actuated swing doors shall only be installed where required for disability access and only where the door is an internal door. Actuated swing doors shall only be considered at a buildings perimeter where:

- An automated sliding door can not be installed, and;
- An automated bi-parting door can not be installed.

3.4.2 DEVICE FUNCTIONAL DESCRIPTION – ACTUATED SWING DOORS

Each device if fitted to an actuated door must be installed and must operate in the following way:

3.4.2.1 *Door Control Key Switches*

The electronic key switches shall have four modes. The operation shall be as follows:

- OPEN key position – the door drives open and stays open. The OPEN key position has priority over the security system.
- EXIT key position – the door is closed and locked and only permits exit via the internal motion sensor, exit card reader, emergency door release unit or egress button. The EXIT key position has priority over the security system.
- AUTO key position (and connected to the access control system) – the door is controlled by a security system and is either secure 24/7 and only operates on a security system activation with motion sensors disabled, or is secure after hours, operates on a security system signal activation only and operates on the automated doors motion sensors during programmed day hours.
- AUTO key position (and not connected to the access control system) – the door operation is controlled by the motion sensors or, if fitted, by Request to Exit buttons.
- LOCK key position – the door is closed and locked and does not accept any signal from the motion sensors, safety sensors or access control system. Activation of the emergency door release unit shall remain enabled.

3.4.2.2 *Fire Alarm Input*

Upon receipt of a fire alarm signal (input) the actuated door shall operate in the following way:

EXTERNAL DOORS

- All external swing doors
  - All external automated sliding doors are to automatically allow egress on a fire alarm signal
  - The access control system mode changes to 'Lockdown', which cancels any overriding time zone and only select authorised users are able to enter the area through the door.
  - The exit motion sensor and 'push & go' function is enabled.
  - The entry motion sensor is disabled.
  - The Request to Exit (REX) button is enabled.
  - The exit card reader is enabled (where fitted).
  - The emergency door release unit is enabled.
  - The electronic lock on these doors shall unlock in a fire alarm condition.

A single fire alarm interface relay with an integral red LED shall be located at every automated door as part of the LED mimic panel. Each individual fire relay shall be monitored 24/7 via the security management system. An active fire alarm shall override the LOCK and AUTO position of the door control key switch.

All door open too long (DOTL) alarms, forced door alarms and any associated sounders/sirens shall be disabled until the fire alarm signal is reset to the normal state.

Automated doors are not to 'hold open' for the duration of the fire alarm signal state

INTERNAL DOORS

- All internal swing doors:
  - The entry motion sensor is enabled.
  - The exit motion sensor is enabled.
  - The entry and exit card readers are enabled.
  - The fail-safe electronic lock must release.

A single fire alarm interface relay with an integral red LED shall be located at every automated door as part of the LED mimic panel. Each individual fire relay shall be monitored 24/7 via the security management system. An active fire alarm shall override the LOCK and AUTO position of the door control key switch.

All door open too long (DOTL) alarms, forced door alarms and any associated sounders/sirens shall be disabled until the fire alarm signal is reset to the normal state.

Doors that form part of a smoke/fire barrier shall remain closed and allow entry/egress via activation of entry/exit motion sensors.

Doors that give access to a 'High Secure Area' shall remain in 'Secure Mode' (Not 'Lockdown').

Automated doors shall 'hold open', unless they form part of a smoke/fire barrier or give access to a 'High Secure Area'.

3.4.2.3 *Emergency Door Release Unit (EDRU)*

On activation of an emergency door release unit the following shall occur:

- Raise an immediate alarm signal on the security management system.
- The exit motion sensor and/or 'push & go' feature shall be enabled.
- Trigger the automated door to momentarily open.
- Override the LOCK and AUTO positions of the door control key switch.
- Fail-safe electronic locks shall release.
- Door open too long (DOTL) and forced door alarms and associated sounders shall remain enabled.
- Unless it is an internal swing door, the automated door shall not remain 'held open'.

3.4.2.4 *Automated Door - Integral Motion Sensors*

All integral motion sensors shall be automatically enabled when the following conditions are met:

EXTERNAL DOOR

- Entry motion sensor
  - During business hours (unless access controlled – to follow the security management system schedule).
- Exit motion sensor
  - Active fire alarm.
  - Emergency door release unit activated.
  - During business hours (unless access controlled – operates via the associated request to exit button or card reader).

INTERNAL DOOR

- Entry motion sensor
  - Active fire alarm
  - During business hours (unless access controlled – to follow the security management system schedule).
- Exit motion sensor
  - Active fire alarm

- Emergency door release unit activated
- During business hours (unless access controlled – to follow the security management system schedule).

3.4.2.5 *Card Readers*

Presenting an authorised access card at either the entry or exit card reader shall momentarily unlock and open the automated door in one action. Enabling of the motion sensor only is not acceptable.

3.4.2.6 *Request to Exit (REX) Buttons*

Pressing a Request to Exit button shall momentarily unlock and open the automated door in one action. Enabling of the motion sensor only is not acceptable.

Holding the REX button in shall not hold the automated door open.

3.4.2.7 *Forced Door and Door Open Too Long*

Forced door and Door Open Too Long (DOTL) alarms shall be enabled 24/7 unless the following conditions occur. In this instance, the alarms will be deactivated until the condition has been reset to the normal condition:

- Fire alarm active
- Override time-zone active.

If any automated door is opened without the use of an authorised access card, motion sensor or emergency door release unit, it shall generate an alarm on the security management system and annunciate on the card reader/remote arming terminal and door sounder.

If any automated door is held open past the pre-determined time, the card reader and door sounder shall emit an audible tone and an alarm shall be sent to the security management system.

DOTL alarms shall incorporate a pre-warning time to notify the local user to close the door before the alarm is activated. DOTL and pre-warning times are set globally by the security management system.

The sounder shall be incorporated into the Door Mimic Panel.

3.4.2.8 *Door Locked Alarm*

When an automated door control key switch has been turned to the LOCK key position, it shall generate an alarm on the security management system. Door locked alarms shall be enabled 24/7.

3.4.2.9 *Fire Test Key Switch*

The fire test key switch shall meet the following requirements:

- be secured on the Door Mimic Panel in a way to prevent the key switch assembly from loosening itself due to normal use

- 12-volt DC illuminated with red LED during test or fire mode and green LED in normal mode
- keyed to the Curtin master key system
- key cannot be removed when in test position
- when active, shall trip the fire relay and place the automated door into fire condition mode.

3.4.2.10 *Door Mimic Panel*

The Door Mimic Panel (DMP) shall provide a uniform, standardised and clearly defined demarcation connection point between the automated door, security management system and the fire alarm panel whilst ensuring the services are electrically isolated from each other. The DMP will assist services to efficiently diagnose faults and to maintain and test the services that are interfaced with the automated door. The DMP shall provide a quick and easy means to identify the current condition (state) of incoming and outgoing signals.

The DMP shall provide the following minimum functionality:

- fire test key switch – to simulate a fire alarm locally at the automated door
- LED indicator lights
  - fire test red LED. This LED shall be illuminated when either the fire test key switch is activated or the door is in fire alarm condition mode.
  - fire system interface 'normal' green LED fed from the fire alarm interface relay. This LED shall be illuminated when no fire alarm signal is present.
  - 'Door Locked' red LED fed from the automated door controller. This LED shall be illuminated only when the door is in the fully closed and electrically locked position.
  - 'Day Mode' amber LED fed from the security management system business hours control relay. This LED shall be illuminated when the door is in free access mode.
  - 'Open' amber LED fed from the security management system door open control. This LED shall be illuminated when a signal from the security management system is instructing the door to open.
  - EDRU activation red LED fed from the emergency door release unit relay. This LED shall be illuminated when the EDRU has been activated.
- incorporated 'Forced Door' and 'DOTL' sounder.

3.4.3 OPERATIONAL DESCRIPTION - ACTUATED SWING DOORS

3.4.3.1 *External Actuated Swing Doors*

The external actuated swing doors shall operate under the listed conditions in the following way:

- Lock output

- operates regardless of the mode or state, when the door is fully closed and in the locked position.

- Open output
  - operates regardless of the mode or state.
- Key Override output
  - on when the key override is in Open, Exit or Lock position
  - off when the key override is in Auto position.
- Fire alarm input (Highest priority)
  - When active, the door shall enable entry, exit motion sensor and unlock the door.
  - When inactive, the door shall return to the previous state prior to the fire alarm.
  - The fire alarm input shall override all other modes or input signals.
  - Open input shall open the door.
  - When Active, shall hold the door open, unless they form part of a smoke/fire barrier or give access to a 'High Secure Area'.
- Open input (Medium priority)
  - When active, the door shall open.
  - The door shall remain open while this input is active.
  - When inactive the door shall close.
- Lock input (Low priority)
  - When active the door must close and disable all motion sensors.
  - When inactive the door must unlock and enable all motion sensors and remain in the closed position.

3.4.3.2 ***Internal Actuated Swing Doors***

The internal actuated swing actuated doors shall operate under the listed conditions in the following way:

- Lock output
  - operates regardless of the mode or state, when the door is fully closed and in the locked position.
- Open output
  - operates regardless of the mode or state.
- Fire alarm input (highest priority)
  - When active, the door shall enable the motion sensors and momentarily open the door once.
  - When inactive, the door shall return to the previous state prior to the fire alarm.

- The fire alarm input shall override all other modes or input signals.
- Open input shall open the door.
- Open output functions as normal.

- Open input (medium priority)
  - When active, the door shall unlock and open the door.
  - The door shall remain open while this input is active.
  - When inactive, the door shall close.
- Lock input (low priority)
  - When active, the door shall close, lock and disable all motion sensors.
  - When inactive, the door shall unlock and enable all motion sensors and remain in the closed position.

3.4.4 AUTOMATED REVOLVING DOORS

Detail to be provided in next revision

3.5 INTRUSION DETECTION SYSTEM

The intrusion detection system (IDS) shall be connected to an approved IFC, forming part of the security management system (SMS).

In the event of an alarm or tamper, the IDS shall report the status to the SMS. All alarms shall be passed to the alarm processor for handling by the SMS workstation and/or dial out to a remote monitoring site if and where required.

3.5.1 SYSTEM FEATURES

The IDS control outputs shall include, but not be limited to:

- alarm reporting to the SMS down to the alarm zone level
- allow connection for building siren and strobe.

The system shall provide spare capacity for the provision of future IDS services within the building.

Detection equipment shall be controlled by nominated ACS devices and remote arming terminals (RATs), remotely from the SMS workstation or within programmable time schedules.

When an area/zone/sector is ‘armed’, movement within the area or unauthorised movement through a door covered by the IDS shall initiate an alarm.

It shall not be possible to clear an alarm until the area/zone/sector or door has returned to a secure state.

Unauthorised tampering with detectors, cabling or equipment enclosures shall cause a tamper alarm to be transmitted to the SMS and the operator terminal.

The tamper circuits and nominated zones shall operate 24 hours a day; regardless of whether the system is in the ‘armed’ or ‘disarmed’ state.

A separate sector shall be provided to control each intrusion detection device.

The devices and sectors shall be capable of being grouped into user defined zones.

Where approved by Operational Technology, the IDS shall be able to be armed or disarmed from a nominated ACS device using a valid access card and/or keypad code. The nominated ACS device used to arm or disarm the IDS shall not be a perimeter or external device.

The appropriate graphical map shall have an icon for each IDS zone to allow the zone to be armed/disarmed from the SMS workstation.

Entry/exit delays shall be programmed for a predetermined period of time, normally thirty seconds, for both arming and disarming of the IDS. This can be extended to a period no longer than one minute, if required, with the approval of Operational Technology.

All operator actions associated with the IDS shall be logged as events and recorded by the SMS.

3.5.2 VOLUMETRIC INTRUSION DETECTION DEVICES

Volumetric intrusion detection (VID) devices shall be suitably secured in place on either appropriately designed brackets to support the unit weight or fixed to ceilings/walls as appropriate for the sensor being installed.

VIDs shall be suitable for each environment and include such features as:

- self-checking
- automatic temperature compensation
- noise immunity to RFI and EMI
- anti-masking detection circuitry
- trouble output.

3.5.3 PASSIVE INFRARED GENERAL PURPOSE DETECTOR

Passive infrared (PIR) detectors shall be suitably secured in place on either appropriately designed brackets to support the unit weight or fixed to ceilings/walls as appropriate for the sensor being installed.

PIRs shall be suitable for each environment and include such features as:

- minimum beam width pattern of 86°
- protection range of seven curtains of 15 metres
- precision mirror optics with gliding focus
- anti-masking protection
- self-testing and reporting of the PIR and anti-masking features
- tamper alarm as a separate and unique alarm output
- signal processing to analyse the shape and size of the incoming signal to filter out false alarms without reducing security

- LED alarm indication that can be enabled or disabled, where required.

3.5.4 360 DEGREE PIR DETECTORS

All 360° PIR detectors shall be suitably secured in place on either appropriately designed brackets to support the unit weight or fixed to ceilings/walls as appropriate for the sensor being installed.

The 360° PIRs shall be suitable for each environment and include such features as:

- volumetric detection that shall provide nine curtains of eight metre detection extending horizontally out from the detector and down to the floor so that movement directly under the detector is within the detection zone
- a protection area of 360°
- a protection range of an eight metre radius
- precision mirror optics with gliding focus
- anti-masking protection
- tamper alarm as a separate unique alarm output
- signal processing to analyse the shape and size of the incoming signal to filter out false alarms without reducing security
- LED alarm indication that can be enabled/disabled as previously specified
- rotation of the sensing head on the base that shall allow 15 degrees of rotation in either direction for exact placement of curtains
- inclusion of 'window' screens to blank off any unused beams, to suit required coverage
- operating temperature range of 0–60 °C.

3.5.5 DETECTOR INSTALLATION

Detectors shall be fitted with a tamper micro-switch to produce an alarm indicating interference with the detector cover or removal of the detector. Detector installation shall be:

- in accordance with the manufacturer's recommendations
- security mounted to prevent any vibration affecting their performance
- sealed with a suitable sealant to prevent ingress of draughts, dust and insects
- with the detector operating at no more than 90 per cent of the manufacturer's specified range.

Magnetic reed-switch tamper devices shall not be acceptable.

Detectors shall be installed unobtrusively on brackets, if required, that match the adjacent architectural features and finishes.

All mounts/brackets shall be approved prior to installation.

The final location for installation shall be determined on site with consideration given to both architectural and structural features and any furnishings that may limit or interfere with the detector's effectiveness.

The installation, detectors and cabling for each device shall include all necessary inputs and outputs to utilise all features including alarm, tamper and self-diagnostic outputs.

Detectors and tamper alarms shall be connected to the ACS as follows:

- Each intrusion alarm shall connect and report to the SMS. Alarm zones shall form part of the programming schedule issued by Operational Technology.
- Tamper and anti-masking alarms shall connect and report to the IDS to identify and report the individual detector/alarm zone and shall report on a 24-hour basis.

3.5.6 AUDIBLE ALARM WARNING DEVICES

Audible alarms shall comply with AS2201.1 and have:

- a sound pressure level of not less than 90 dB(A) and not greater than 130 dB(A) measured at one metre
- an alarm condition on a single zone that shall cause the audible alarm(s) to sound for a period no longer than a total of five minutes. Subsequent sounding of the warning device for a further period of up to five minutes shall only occur where:
  - the intruder alarm has been manually reset on site, or
  - a subsequent alarm is generated in a different zone of a multi-zone system.

3.5.7 VISUAL ALARM WARNING DEVICES

Where requested, a flashing blue light shall be included and installed as per AS2201.1.

Where used, such devices shall be:

- installed on the exterior of the building, in a location that is clearly visible to campus security patrols
- located at a height to minimise the possibility of inadvertent damage and to discourage vandalism.

3.6 INTERCOM SYSTEM

The intercom system is voice over internet protocol (VoIP) based and has a high level interface with the SMS. Utilising VoIP allows intercom functionality and related intercom alarms and events to be supported through the SMS workstation.

Intercom units shall be associated with access controlled door enabling authorised operators to open the door in response to a call made from the intercom unit. The operator shall be able to perform the following functions:

- Respond to calls and monitor the status of the intercom system.

- Forward the call to another SMS workstation or intercom unit from the same intercom system.
- Place a call on hold, enabling the operator to service other calls and return to the call when ready.
- End a call.
- Initiate calls.

All intercom events shall be recorded in the SMS, including the operator who answered or initiated the call, the intercom unit, the call duration and the time the call was made and answered.

All intercom events are to be recorded.

Each entrance station must be able to call a master station and then cascade through other master stations (if applicable) as programmed until the call is answered.

The intercom system shall operate using VoIP or SIP Protocols and provide clear undistorted speech communications, free from background noise and/or external interference regardless of plant or other background noise.

Intercom stations (i.e. master/control, slave/remote and voice/video) shall, where nominated, include additional contacts to allow remote monitoring of all call requests by the SMS with select calls triggering the DVMS cameras to provide images on the alarm/events monitors. Similarly, all external intercom stations shall include tamper alarms, be vandal resistant and be monitored by the SMS and DVMS, where cameras are available.

3.6.1 REMOTE/SLAVE DOOR STATIONS

Communications between remote intercom stations and the designated master station shall be selectable from either the slave or master station. Calls initiated from the slave station shall not establish conversation until manually accepted by the receiving master station (similar to privacy operation).

3.6.2 LOCAL VIDEO INTERCOM STATIONS

LOCAL VIDEO MASTER STATIONS

Local video master stations shall be as per the Approved Equipment Schedule (APPENDIX A).

Requests by a faculty/school/department or area to have a local video intercom installed to act as a reception call point must be submitted to the Director, Operations and Maintenance, Properties Facilities & Development for approval.

Where instructed by Operational Technology, video master stations shall be connected to the associated access controlled door via the SMS to enable the local operator to open the door in response to a call made from the local video entrance unit.

Local video master stations shall be mounted in a location that ensures an unauthorised person cannot reach and/or activate the device. This can either be on a wall positioned for easy accessibility by the user or securely fastened to a work space to ensure the unit cannot be inadvertently damaged.

LOCAL VIDEO ENTRANCE STATIONS

Local video entrance stations shall be as per the Approved Equipment Schedule (APPENDIX A).

Where instructed by Operational Technology, video intercom entrance stations shall be utilised and be connected to the SMS workstation and act as described in 3.2.7.

In circumstances where a semi stand-alone intercom station has been approved by Operational Technology to act as a local reception call point (by a school or department), the video entrance station shall, for the timeframe prescribed, connect to a local video master station that shall be answered by the school or department directly. At a prescribed time, all after-hours calls shall be routed back through to the SMS workstation and act as described in 3.2.7.

Where a local video entrance station is mounted, it must have adequate signage installed directly above the door identifying its intended purpose, e.g. "B109 Health Services Reception". Such signs shall in no way resemble a campus assistance point (CAP) sign.

To avoid confusion, local video entrance stations are not to be installed within one metre of a campus assistance point, and preferably be at least two metres away.

3.6.3 MOUNTING OF REMOTE/SLAVE/ENTRANCE STATIONS

Remote/slave/entrance stations shall be flushed-mounted and fitted with a stainless steel faceplate, clearly engraved with operating instructions. Where flush mounting is not possible, a surface-mount housing shall be provided. (See APPENDIX A for the approved surface mount.)

Remote/slave/entrance stations located externally shall be suitably weatherproofed and located on external walls in suitably recessed mounting boxes. Exposed stations shall include a rain 'drip' cover. The speaker shall have internal protection against water damage.

Cabling shall be installed with adequate 'slack' to allow for the complete removal of the station for service access without undue stress on the cabling.

Stations shall be securely fixed in place using secure fixings or permanent rivets.

Where external stations cannot be installed on building structures they shall be installed on building entry totems. To ensure compliance with AS1428-2009, a secondary button shall be installed and terminated into the station as an input. The secondary button shall not be connected in series. (Refer to Curtin University Architectural - Security Building Intercom (CAP) Totem Drawing 00MISC-SC-ST0010.)

Intercoms not mounted on building entry totems are to include the mounting of a campus assistance point sign that shall be installed by the contractor. The position of the sign shall be as shown on the Curtin University Security Standard Access Controlled Door Detail Drawing 00MISC-SC-ST0003.

3.6.4 POWER SUPPLIES

Where possible, the intercom call points shall derive power from the network switch via power over ethernet (POE), otherwise a separate power supply or POE adapter will be required.

3.7 DIGITAL VIDEO MANAGEMENT SYSTEM

Curtin's CCTV system is an enterprise-wide digital video management system (DVMS) which all CCTV cameras must be connected to. The system includes:

- network video recorders (NVRs)
- a site configuration database
- DVMS workstation software located on specific Curtin workstations
- cameras and associated equipment such as lenses, housing and brackets
- monitoring stations (Display Screens) including mini PC's for local viewing of building cameras
- bi-directional high-level interface (HLI) to the SMS
- open protocol (ONVIF) licensing.
- Analytics

The DVMS forms a fully integrated system controlled from the Curtin security operations room.

The equipment allows camera control, camera selection, display control and monitoring from the nominated control locations.

New and existing cameras shall be connected to, and recorded on, the DVMS.

Cameras required for a specific function other than security or surveillance (e.g. iLectures, teaching or other such faculty requirements), are not covered by these requirements and are not to be connected to the DVMS.

3.7.1 NETWORK VIDEO RECORDER (NVR)

Network video recorders (NVRs) are supplied and installed by Curtin University. The security contractor shall program the NVRs as required.

The contractor shall configure the primary and backup NVR servers for each camera.

The system shall be configured to continuously record each camera unless otherwise specified.

Recorded information shall be date and time stamped and stored within every file for easy retrieval.

The system shall be configured, programmed and set up to record and store all system cameras each at a minimum rate of thirty frames per second at 4MP resolution using H.264 compression standards.

The system shall be configured, in coordination with Operational Technology, to provide the minimum recording rates detailed above and store all images for a minimum of thirty-one days recording on the NVRs.

The recording schedules and alarms must then be synchronised between the primary and backup NVR server. In the event of a primary NVR server failure, the NVR workstations will be switched to playback and use alarms from the backup NVR server. In the event of the backup NVR server failing, the primary NVR server will continue to record and manage alarms. The administrator should not be required to take action in this instance.

3.7.2 DVMS DATABASE

The DVMS database stores information about the components connected to the system (e.g. NVRs, encoders, decoders, monitors, workstations) as well as acting as the central repository for alarms. The DVMS database shall be updated by the installing technician each time a new component is connected to the DVMS.

3.7.3 SOFTWARE AND PROGRAMMING

The security contractor shall perform all programming of the DVMS and associated SMS interfaces as required.

Programming of system configurable items shall be protected against accidental or deliberate modification by unauthorised persons.

As a minimum, programming shall include:

- allocating cameras to sequences, groups and guard tours
- configuring alarm inputs (sources) and alarm outputs
- creating or updating graphical maps from .bmp, .dwg and .jpg files and assigning to sites
- adding camera vistas in the map to indicate the camera view
- assigning cameras/encoders to NVRs and creating recording job schedules.

3.7.4 DIGITAL VIDEO ENCODERS

Video encoders shall be as per the Approved Equipment Schedule (APPENDIX A).

Where installed, encoders shall be configured to ensure that:

- each stream is configured as independent H.264 streams
- each stream shall support 1MP, 2MP and 4MP resolution and record at 1 to 30 frames per second (fps) and simultaneously on both streams should also be available. Configuring any resolution at any frame rate shall be possible, per video stream
- an alarm is created where video motion detection (VMD) or video loss is caused by a defective camera or cable, or by camera masking
- each camera is initially configured to record thirty (30) frames per second at 4MP resolution, with the smallest possible compression rate.

VIDEO COMPRESSION

The encoder architecture must support H.264 (ISO 14496-10) video compression. DSP Codec implementations will not be considered due to their inherent performance limitations, which can result in reduced frame rate, reduced video quality, video artefacts and increased bandwidth utilisation.

3.7.5 CAMERAS

Curtin utilises a number of different cameras depending on the application, including:

- Internal/external IP fixed dome camera
- Internal/external IP fixed full-bodied camera
- pan tilt zoom (PTZ) camera
- multi-head camera
- internal/external infrared (IR) fixed dome camera
- internal/external infrared (IR) bullet camera.
- thermal camera
- Automatic Number Plate Recognition (ANPR) camera

3.7.5.1 *IP Cameras*

IP cameras shall be connected to the Curtin VLAN, via an RJ45 data outlet. The RJ45 data outlet shall be surfaced-mounted and concealed within the roof space of the building as shown on Drawing 00MISC-SC-ST0013 or as approved by Operational Technology.

External PTZ cameras shall be powered by the network switch's power over ethernet (PoE) supply, unless agreed to by Operational Technology. Where PoE is not available at the switch, a power injector shall be provided that is powered from the power distribution unit (PDU) within the rack and shall be installed on a rack mount shelf unless otherwise directed by Curtin DTS Networks.

3.7.5.2 *Camera Optimisation*

After installation, cameras shall be optimised for the application and scene. Optimisation shall include but not be limited to:

- focusing
- zooming
- framing (pan/tilt)
- setting of the home position (PTZ) and setting of the dwell time before returning to the home position (10 minutes)
- exposure settings:
  - backlight compensation
  - shutter speed
  - iris settings
  - day/night settings
  - dynamic contract control (DCC).

EXPOSURE SETTINGS

Camera lenses supplied shall be vari-focal, manual zoom or electronic zoom capable.

The lenses shall include video drive auto iris.

The lens focal length shall be selected by the contractor to provide the required field of view as specified at each location. Final adjustments will be arranged under the supervision of Operational Technology.

Manual zoom lenses shall include appropriate locking mechanisms to prevent any vibrations or unauthorised tampering that may affect the zoom or focus settings.

The locking mechanism shall be tamper-proof.

Nominally, the lens focal length must be in accordance with the defined views as detailed in this document. However, should lens changes be necessary, the contractor shall provide alternative (i.e. of different focal length) lenses in exchange, at no cost to the project.

FIELD OF VIEW

The contractor must locate all cameras as shown on the drawings to view the area(s) as indicated. The following minimum guidelines are provided to assist in the final adjustment and location of cameras and lenses.

- A minimum of 85 per cent of the marked 'security zone' must be viewed and recorded at all times.
- The angle of view should ensure that the image of persons within the security zone does not exceed five degrees from the horizontal viewing plane.
- Items of fixed equipment must be in full view with 100 per cent of the object width overlap on all sides, top and bottom.

The contractor must notify Operational Technology in the event of any difficulties in meeting compliance with the above.

FINAL ADJUSTMENT OF LENS SETTINGS

Lens and camera adjustments must be verified at night to provide optimum coverage during both day and night conditions. Settings must be 'locked' and recorded for future reference.

Adjustment of settings and recordings shall include flange ring setting, iris, focus and zoom. Adjustments are to include the use of standard TV test patterns to improve fine tuning for maximum image quality. Final adjustments shall be performed while viewing the camera via the control centre and not via a local handheld monitor connected directly to the camera.

In addition, cable numbers and descriptions, and equipment makes and models must be recorded and presented in a detailed commissioning document (and included in the project's Operations and Maintenance Manual).

CAMERA HOUSINGS

Housings shall be sealed to prevent ingress of dust, insects and moisture, to a minimum IP65 rating.

Housings shall provide the facility for termination of conduit fittings. Cable entries shall be concealed internally to the housing or via the housing bracket.

Camera housings and brackets shall be fitted with tamper-proof security screws. Security screws shall be the 'post button head' type. Fixings on all external camera brackets and housings shall be manufactured from marine-grade 316 stainless steel.

The contractor shall submit samples and details of all proposed housings to Operational Technology for comment and approval prior to supply or manufacture.

The following features shall be required as part of the housing design:

- The housing is to be building- or slab-mountable, on custom designed and manufactured brackets.
- The housing is to have a polycarbonate or Lexan vandal-proof viewing window or dome (smoked colouring).
- The conduit and cable entries shall be within the camera housing or bracket and shall be made airtight using an approved epoxy sealant.
- The camera housing shall be adequately sized to permit easy adjustment of the camera controls and to facilitate ease of servicing.
- The camera housing shall be suitably sized to accommodate one camera fitted with a lens and all associated cabling.
- The camera housing shall incorporate a matching sunshade to provide protection from solar radiation and to minimise rain and direct sunlight falling upon the viewing panel for external units.
- The camera housing shall be fitted with a precision-cut rubber gasket to the removable cover to ensure IP65 rating is maintained.
- Reasonable measures shall be taken in mounting cameras to minimise the risk of camera theft or damage.

INTERNAL CAMERA HOUSINGS

The internal dome housing shall meet the requirements of the area they are installed in and, unless otherwise specified, be flushed-mounted into the ceiling void and secured correctly to the manufacturer's specifications.

Unless otherwise directed, internal dome cameras shall be fitted with smoked dome lens covers.

EXTERNAL CAMERA HOUSINGS

External camera housings shall be weatherproof, sealed to prevent ingress of dust, insects and moisture and have an IP rating of IP66. The housings are to incorporate a sun shield that shall also divert any rain away from the viewing window. Housings shall be of rugged construction and highly vandal-resistant.

Contractors shall provide a product datasheet and, when requested by Curtin, a sample housing to Operational Technology for approval prior to placing any orders.

Where a housing is deemed unacceptable by Curtin, the contractor shall replace it with an acceptable replacement, at no cost to the project.

TAMPER ALARMS

Camera housings and equipment enclosures shall be fitted with tamper switches connected to the alarm inputs of the encoder or NVR for interfacing with the SMS for reporting on the SMS workstations.

Tamper switches shall be monitored 24 hours a day.

CAMERA BRACKETS

Camera brackets must be welded steel (i.e. plastic brackets will not be considered). Brackets must match the camera housing construction and provide adequate adjustment to ensure optimum viewing positions are achieved.

Adjustments must be securely fixed such that accidental or deliberate misalignment of cameras is not possible.

Brackets must be electroplated and painted to match camera housings. Brackets must be rigid and vandal proof.

CAMERA POWER SUPPLIES

Where required, camera power supplies shall conform the manufacturers specifications or where not provided, to the minimum requirements as shown in the following table:

Features	Specification
Input Current	1.2 A @ full load
Output Voltage	24 V AC
Channels/Units	9 or 15 as required
Fault Output	1 SPDT relay and LED
AC Output Indication	Output channel status LEDs (Green = OK, Red= fault)
Dimensions (mm)	427W x 360D x 128H mm
Input Voltage	240 V AC/50–60 Hz
Safety Standards	AS/NZS61558.1:2000 incl. Amdts 1–3 AS/NZS61558.2.6:2001 AS/NZS 60950.1:2011
EMC Standards	AS/NZS CISPR 11:2011 Group 1 Class A (Conducted and radiated)
Mounting	Rack Mountable

3.8 PROGRAMMING

The necessary programming associated with the works shall be implemented to ensure all systems operate, function and interface as detailed in this specification.

Programming shall include the initial setup, implementation of system interfaces and data entry in accordance with the requirements of each door, zone, local/remote operation or network interface to other systems. Programming should be as per the Curtin University-supplied Security Programming Instruction.

For a full understanding of the programming requirements and standards, the *Security Programming Standard* document must be read and understood in conjunction with the Important Notes section of the *Security Programming Instruction*.

4 ELECTRONIC EQUIPMENT REQUIREMENTS

The equipment supplied and installed as part of the contract shall comply with appropriate standards and the following requirements:

- The equipment shall be 19 inch (or 482.5 mm) rack mountable, modular in design and allow expansion of equipment without redundancy of installed equipment, unless otherwise stated.
- Cooling shall be by natural ventilation in cubicles and by forced ventilation in equipment racks.
- Switching contacts shall be rated by the component manufacturer for 100,000 operations at the installed current rating and operating current (i.e. AC or DC).
- Relay coils shall be suitable for operation from their respective supply voltage +20%, -25% in the battery powered equipment and +15% in mains-only powered equipment.
- A frequency of 1,000 Hz shall be used for test and reference purposes in audio circuits.
- Cabling shall be protected against damage by current overloads.
- Cables liable to bending during service or maintenance shall be of a flexible multi-core type.
- Plugs and sockets shall be labelled with the name of the circuit they are connected to.
- Cabling within equipment shall be neatly laced and tied and supported on metal brackets as necessary.
- Interconnections between internal modules shall be via plug socket connections, wherever possible.
- Indication lamps shall be LEDs.

4.1 REDUNDANT/SALVAGED EQUIPMENT

Redundant and salvaged equipment removed from Curtin University's systems or buildings remains the property of Curtin. The salvaged items are to be handled as shown in the following table:

Item Type	**Salvaging Requirement**
Electronic devices	Returned to Operational Technology
Door ironmongery	Returned to Operational Technology
Door cylinders	Returned to Security Technical Office
Reed switches, redundant cabling, door frames, doors	Treat as waste material
Waste material, e.g. packaging	To be disposed of by the contractor in accordance with the contract

4.2 FIRE SYSTEM CONNECTION

The fire system connection from the fire indicator panel (FIP) to the intelligent field controller (IFC) shall be via a 24 V hard-wired, fire-rated cable, connected to a fire interface relay within the IFC enclosure. This shall be supplied and installed by either the security contractor or the nominated fire service provider approved to work on Curtin University fire systems. Connection to the FIP must only be completed by the nominated Fire Service Provider.

Upon receiving a fire signal from the FIP the IFC shall:

- unlock all internal electronically controlled emergency exit doors
- unlock all perimeter doors that do not normally permit egress when locked
- silence all local audible devices connected to the SMS
- generate a critical priority alarm on the SMS.

Note: Automatic doors must be independently connected to the FIP so that the door responds to a fire alarm signal, as required by the National Construction Code, and not be reliant on the SMS to provide egress permissions in the event of an active fire signal.

5 EQUIPMENT FITTINGS AND ACCESSORIES

5.1 GENERAL

Device heights and types of devices are provided within this specification. Any conflict found between sections of this document should be notified to Operational Technology via email at operationaltechnology@curtin.edu.au.

The contractor shall inspect and become familiar with the drawings, floor plans, door and wall construction and facing to ensure adequate fixing, access and installation space for all equipment.

The fittings shall be new and of the type/make specified.

The fittings shall be installed flush, unless otherwise specified.

In external areas, face plates and fixtures shall have mastic or a silicon-type sealant installed between the face plate and the wall and be fixed using tamper-proof screws.

Wherever possible, wall and ceiling structures should be reinforced during construction to allow the use of standard fixing arrangements to mount security equipment.

The contractor shall submit for approval a detailed schedule of all secure fixings to be used.

5.2 POSITION AND RELATIONSHIP OF ACCESSORIES

The contractor shall ensure the position and relationship of all accessories are rationalised as further specified.

The equipment in adjacent areas shall be aligned horizontally and/or vertically.

Where devices and equipment are shown on drawings as being adjacent but at different heights, and where they are located within one metre of each other, they shall be aligned vertically, one above the other, unless it is specifically necessary for pendant type connections.

Due care and consideration shall be given to outlets from other trades, e.g. electrical services connections, so that they are installed and coordinated at the same heights and are aligned horizontally; one beside the other.

Special care shall be given to ensure that common sizing, colour and brands are utilised for accessories.

Where outlets are installed in brickwork, care shall be taken the ensure wall boxes are aligned centrally on/or between mortar joints and that where possible, flush plates and/or fittings are of standard brick dimensions. Generally, the positioning of outlets is available off drawing elevations but, where they are not shown, the exact position shall be approved Operational Technology.

Where confusion arises as to the exact position of any equipment, clarification shall be sought from Operational Technology.

5.3 FABRICATED EQUIPMENT

Fabricated equipment shall be of robust, symmetrical and unwarped construction.

Metal work shall be neatly and accurately cut, free of swarf and undulations or any other distortions.

Bends and folds in sheet metalwork shall be produced with a suitable bending machine.

Welding shall be neatly executed with the finished weld ground or filed smooth, seamless and level with the surrounding surface.

Fabricated metalwork shall be painted in accordance with the requirements detailed in Section 6.8 Painting. The colour of the paint finish shall be as directed by Curtin.

5.4 LOCATION AND FIXING OF EQUIPMENT

Equipment shall be rigidly fixed, neatly and symmetrically to rigid supports.

The exposed fixings shall utilise a tamper-proof head or a permanent fixing.

Fixings are to be in accordance with engineering practices and suitable for the purpose intended.

Heights shown on drawings (or specified) are the heights from finished floor level to the centre of the equipment, unless otherwise stated.

The locations shown on the drawings for all fittings and accessories are approximate only and the final locations shall be determined on site to comply with the site requirements and shall be approved by Operational Technology.

The precise location of all equipment shall be confirmed prior to commencing the installation works.

5.5 MASTER KEYING AND LOCKS

Security keys shall be of the same type coordinated to the Curtin University Master Keying System and common to all security equipment panels and enclosures. The keys and key suite for equipment and cubicle racks shall be keyed to the existing university master keying system.

Key suites to locks shall be submitted to the Curtin Security Technical Office for comment and review prior to procurement of locks and keys to ensure coordination with all site keying systems.

During the construction period, builder key issue, control and return shall be strictly controlled. A register shall be maintained of all keys provided indicating their current status. The register shall indicate the printed name and signature of the person(s) to whom keys have been issued.

5.5.1 LOCK CYLINDERS

All doors connected to the access control system (ACS) shall be keyed appropriately to the relevant Curtin Security Access Control Area Master Key. That is to say, all doors (swing/actuated/sliding/bi-folding/revolving), roller doors, gates or other such barrier connected to the access control system, must be provided with a key and cylinder to

allow for manual operation in the event of total systems failure. For mortice type doors, the cylinders are to be fitted with cams that do not allow for the door to remain in the unlocked state, e.g. X-type cams. For all automatic type doors, the cylinder shall be an electronic key switch suitable to the operation of the door.

Lockable strap bolts are to be provided with a security cylinder and a suitable cam for the ADI lockable strap bolt. These cylinders are to be keyed as directed by the Security Technical Office. A request is to be emailed to the securitytechoffice@curtin.edu.au detailing the relevant door hardware schedule and drawings.

5.6 EQUIPMENT ENCLOSURES

5.6.1 GENERAL

In general, all enclosures shall meet with Ingress Protection (IP) Category IP55 standard and be located as indicated on the drawings or to the satisfaction of Operational Technology.

Panels, racks and cubicles shall be complete with dust seals on doors.

Externally located enclosures shall be IP65-rated and be constructed from 2.5 mm thick (minimum), marine-grade aluminium with a powder-coated finish.

Where necessary, panels, racks and cubicles shall be supplied with rear mounting plates and top entry cable gland plates to facilitate top entry of cables from overhead cable trays, cable ducts or conduit.

Where possible, 19 inch (or 482.6 mm) rack mounting shall be utilised to accommodate equipment, with special attention given to providing adequate access for service accessibility to on-board diagnostic indicators and rear-mounted connections.

Holes provided for cable access shall be provided with a grommet and be suitably sealed to prevent moisture ingress and provide protection to cables.

Panels and/or escutcheons shall be fitted with knurled chrome-plated thumb screws.

Screws shall be complete with captive fibre washers.

Equipment panels, racks and cubicles shall be complete with a tamper switch, connected to the security management system (SMS).

Equipment enclosures shall be labelled appropriately to clearly indicate their function.

Each section of the enclosure, panel, rack and cubicle shall be labelled to indicate equipment/device identification number and local power supply circuit number.

The contractor shall submit drawings with construction and finish details of all equipment enclosures, panels, racks and cubicles to Security Infrastructure prior to purchase or manufacture.

Drawings shall include such details as metal work type and thickness, IP rating, cables access facilities, paint finish method and colour, proposed equipment layout.

5.6.2 EQUIPMENT PANELS

Equipment panels within buildings shall be located in a communications room, unless otherwise approved by Operational Technology, and shall:

- have clear labelling showing the IFC equipment name as per the programming schedule supplied by Operational Technology, e.g. 400-IFC-01-0001
- have clear labelling identifying the TO connection plate numbers within the cabinet
- have clear labelling identifying the DGPO plate numbers within the cabinet
- be fitted with tamper alarm switches interfaced to the SMS
- be fitted with approved key locks to access doors
- be fitted with terminals designed for the size and type of cables installed
- have labelling that is clearly readable and of a permanent type
- have included a laminated circuit schedule detailing all terminated and spare cable cores and cabling; the circuit schedule shall be mounted on the inner face of the enclosure
- have concealed-type hinges where it is not possible to remove the hinge pins while the door is in the closed position
- have the cables neatly arranged and loomed; cable strain relief shall be provided for each cable or loom
- have appropriately labelled access equipment indicating their function
- have screws complete with captive washers.

The proposed layouts of equipment panels, racks and enclosures shall be submitted to Curtin for review and comment prior to commencing installation works. The layouts shall identify proposed equipment installation and allowances for spare capacity. The drawings shall indicate the locations of security equipment enclosures and cabinets.

The contractor shall confirm the quantity of enclosures and cabinets indicated on the drawings are sufficient for the amount of equipment to be supplied and installed, prior to commencing installation works.

5.6.3 EQUIPMENT LABELLING

Self-adhesive equipment identification labels shall be supplied and installed to each prime equipment item installed as part of the works. Labels shall be laminated or have a clear contact covering to provide protection in plant rooms and equipment cubicle environments.

The equipment labels shall, as a minimum, detail:

- the date of equipment being commissioned (start of defects liability)
- the serial number of the equipment
- the MAC address of the equipment (where applicable)
- the name of the installing company.

A sample of the proposed label shall be supplied to Curtin for approval, prior to installation on the equipment.

5.6.4 SPARE CAPACITY

Equipment enclosures providing battery backup and power supply units (PSU) shall have a minimum spare capacity to accommodate the full population of the installed hardware.

5.6.5 UNIFORMITY OF EQUIPMENT

Equipment installed shall maintain uniformity as part of the works, and with Curtin systems or equipment as noted in this document.

The supply of uniform equipment shall be coordinated with the various suppliers.

6 INSTALLATION REQUIREMENTS

6.1 FIRE RATING OF PENETRATIONS

The *000321 PDG Fire Safety Project Guideline* should be considered when providing penetrations of this type.

6.1.1 PROCEDURE FOR PENETRATIONS

The following procedure shall be adhered to prior to the contractor conducting any penetration:

- Curtin will attempt to locate any existing electrical and communications drawings and make these available.
- A structural engineer shall be engaged by the contractor to provide a recommendation as to the suitability of the proposed location for the penetration.
- A scan of the area is to be undertaken by a Curtin-nominated company (engaged by the contractor).
- Curtin is to be provided with the scan report and, based on the documentation, will decide whether to grant approval for the penetration.
- If there is no definitive clear path, then a second scanning company is to be engaged to scan the area (engaged by the contractor). The report is to be provided to Curtin for review.
- If there is still no identifiable clear path, Curtin will make a ruling as to whether the building's power is to be shut down prior to the penetration being made. Any interruptions to services in this instance will be rectified by the contractor, for which a claim can be made against the project.
- Once approval of the proposed location is given, the contractor is to engage a Curtin-nominated company to perform the penetration works.

Note: Unused or partially used penetrations shall be 'made good' to the satisfaction of Curtin. This shall include all flushing and the trimming of openings.

6.2 CEILING CUT-OUTS

Ceiling cut-outs required for conduit penetration to surface-mounted equipment and for the flush-mounting of equipment shall be provided by the security contractor as part of the contracted works.

Equipment shall not be secured to the ceiling grid or ceiling hangers. Heavy items of equipment such as monitors and PTZ cameras shall be fixed to the slab so that no weight or stress is placed on the ceiling structure.

6.3 POWER SUPPLY

The AC power supply to the security installation shall be provided at a nominal 240 V AC 50 Hz from the supply in each building.

The equipment supplied and installed as part of the contract shall be capable of operating over the following voltage and frequency ranges:

- voltage 240 V AC +/-6%
- frequency 50 Hz +/-5%.

6.4 BATTERY BACKUP

A minimum of 12 hours stand-by power shall be provided to all control and field equipment installed as part of the contracted works.

Batteries and battery chargers shall be located in all equipment panels.

Battery chargers shall be capable of restoring the battery from a fully discharged state to a fully charged state within a period of 12 hours after restoration of supply and at the same time maintain the installation in a fully operational state.

Monitoring of the mains supply shall be from the output of the charger but isolated from the battery and shall be fail safe.

Batteries shall be suitable for continuous standby duty and shall be supplied with the date of manufacture.

Batteries shall be the sealed lead-acid type.

Installed batteries shall show the date of installation in a clear and legible manner, i.e. indicating the date the equipment is energised and is reliant on the battery to operate in the event of a mains power failure.

Where the batteries are installed in a separate battery cabinet and not attached to the main panel, the cabinet shall be fitted with a tamper switch connected to the security management system.

Battery replacement shall be able to be carried out by customer maintenance staff with minimal instruction.

The battery capacity shall be calculated by obtaining the total quiescent current drain of the system (excluding battery trickle charging). This figure shall be divided by two, then multiplied by three and then multiplied by the period of standby (e.g. 12 for 12 hours). This is the minimum ampere-hours of the standby battery.

6.5 ENVIRONMENTAL REQUIREMENTS

The equipment supplied to meet the requirements of this specification shall be suitable for continuous operation at ambient temperatures of between 0 and 50 degrees Celsius and 95 per cent non-condensing humidity for in-building installations.

Equipment that is to be installed in field environments, including in field equipment cubicles, shall be suitable for continuous operation at ambient temperatures of between +10 and +75 degrees Celsius with 95 per cent humidity.

Externally mounted fittings, fixtures and materials supplied and installed as part of the works shall be suitable for continuous operation when exposed to ultraviolet radiation and climatic extremes, including solar loading. This shall include physical and operational integrity without degradation of the physical construction or functional operation.

6.6 EMC/EMI REQUIREMENTS

The total integrated system shall not cause any interference, nor be affected by electromagnetic transmissions.

Where the inherent characteristics of equipment could possibly cause interference, the equipment shall be provided with effective interference suppression devices and techniques to eliminate the interference.

The equipment supplied and installed as part of the works shall be checked so it does not interfere with the reliable operation of other systems connected to the common power supply or located within the project environment or adjacent buildings.

Upon request from Curtin, a demonstration shall be provided of possible causes of noise generated within the project environment that may affect the reliability of any equipment supplied, be it through simulation or any other method necessary to identify the interference. Possible measures to eliminate any identified interference shall be discussed and confirmed with Curtin prior to procurement and installation.

6.7 LIGHTNING PROTECTION

Adequate lightning and transient protection shall be provided on all external systems, equipment and hardware that is not installed within a building structure, e.g. car parks, remote campus assistance points, camera poles, to meet the requirements of this specification and any relevant standard, legislation, Act or code of practice.

Protection of equipment shall be in accordance with AS/NZ1768-1991 and include both primary and secondary protection and suppression of both differential and common mode transients.

Particular attention shall be given to all external cabling devices that are interconnected and/or interfaced to the various systems. As a minimum, lightning protection for external equipment shall be installed in the supporting equipment cubicle prior to the point of connection to the backbone communications infrastructure. External cabling shall be provided with inline lightning protection.

The lightning and transient protection devices shall be installed for all video, data and power supply cabling.

Equipment necessary to prevent or minimise lightning damage to systems and system components shall be provided as part of the works.

Typically it will be necessary to consider the following points for surge protection devices:

a) At the point of entry of external services e.g. electricity supply and communications.

b) At the connection of the external services to the equipment.

c) At the connection of long internal cabling to the equipment e.g. communications and LAN.

The following two mechanisms can damage equipment:

a) An excessive voltage/current enters the building via a service due to either a lack of protection or incorrectly installed protection.

NOTE: When protection is correctly installed both the mains and communications point of entry surge protection devices are bonded to the main earth bar by conductors of 1.5 m or less.

b) An excessive voltage/current is induced into the internal wiring loop.

6.7.1 PROTECTION PROCEDURE

The procedure for protecting equipment is as follows:

a) Install secondary protection at the equipment when the risk of damage due to induction into the external service conductors (electricity supply and communications) and the building conductors exceeds an acceptable level.

b) Install point of entry protection when the risk of damage due to a direct strike to the structure or the service conductors exceeds an acceptable level.

6.8 PAINTING

Metal work shall be free from grease, rust, scale and shall be finished with an approved factory-applied paint system of a selected, approved colour.

Finished surfaces of all paint work not otherwise specified shall be free from bubbles, runs or any other imperfections and have a high gloss finish.

The touching up of finished surfaces shall be accurately matched to the factory-applied finish.

6.9 SOLDERING

The solder shall be resin-cored solder with a 65 per cent tin content. No separate flux is permitted.

The solder shall provide a good electrical bond between the conductor and the tag and meet with the following:

- Prior to soldering, the joint shall be mechanically sound.
- The soldered joint shall not be subject to mechanical stress.
- No excess solder shall remain on the tag.
- No solder droppings shall be left on or about the work.

Work showing evidence of a corrosive flux being used shall be rejected.

Soldered joints and connections between cables, devices and end-of-line resistors shall be fully encased within heat shrink. PVC electrical tape shall not be used as a means to cover solder joints.

6.10 VERMIN, INSECTS AND MOISTURE

Enclosures, cabinets, ducting, housing and conduit shall be sealed or otherwise protected to prevent the entry of vermin, insects or moisture that could damage the equipment, cabling or degrade the performance of the installed system.

6.11 'AS NEW' CONDITION ON COMPLETION

Proper care shall be taken to protect all apparatus, materials and equipment stored or installed on site.

Any fitting, accessory, cabling, material or item of equipment that forms part of the work shall not be used for any purpose other than for approved testing.

The works, including all materials and equipment, shall be handed over at the date of practical completion in an 'as new' condition.

Should Operational Technology (Operational Technology), consider any components, including wiring, to be unsuitable, they shall be removed and replaced at no cost to Curtin.

6.12 MAKING GOOD

Where alterations are required as part of the works, the holes left where hardware has been removed shall be filled flush with the surface and repainted to match the existing colour to the nearest break or wall return.

Where hardware has been removed from door frames, the frame shall be repaired with similar material to the existing frame and any necessary repainting or revarnishing of the frame undertaken.

If, during the execution of the works, damage is caused, the repair of the damage shall be done using materials compatible with the surrounding material and finished off flush with the surface on which they occur. These repairs shall include painting of damaged surfaces to match existing to the nearest break or wall return.

'Making good' shall include but not be limited to the re-establishment or repair of all ceiling panels, wall finishes, bitumen, roadways, paths, lawns, irrigation pipe work, sprinklers and other areas that were damaged in the course of carrying out the works.

7 CABLING

7.1 GENERAL

The following requirements shall apply:

- For electrical, data or communications cabling, refer to the relevant Curtin guidelines as a guide to the relevant requirements.
- The contractor shall supply, install, label, terminate and connect all cabling necessary to complete the installation, including all audio, data, control, fibre-optic (where applicable), communications cabling and device cabling.
- The contractor shall liaise with the electrical subcontractor to coordinate cabling and conduit requirements associated with any electrical works.
- Terminated cabling shall be neatly labelled and tied/loomed to prevent damage to terminations and interference to or the obstruction of other services.
- Where large volumes of cables are installed within a penetration or cavity or where cables drop long distances within a building, the security contractor shall take measures to support the cables at regular intervals to reduce the risk of damage to the cables.
- Unterminated (spare) cabling shall be neatly labelled and tied/loomed to prevent damage, interference to or the obstruction of other services.
- Strain relief shall be provided for cables connected to rack-mounted equipment.
- Cables shall have stranded copper conductors and be PVC insulated with an overall PVC sheath, unless otherwise specified.
- Cabling shall be concealed and installed on a metal cable tray, or within a cable duct and conduit. Cabling shall be installed with due regard to future removal and replacement of cables. Like cables are to be grouped in ducts or on trays and secured with the appropriate coloured cable tie.
- TPI cables shall be 0.6/1.0 kV grade. Insulation shall be V75 grade.
- Cables shall be new and delivered on site in unbroken reels; with the manufacturer’s label attached.
- Due consideration shall be given to voltage drop when calculating cable sizes.
- Cabling shall comply with the current AS/NZ3000 and any additional requirements specified hereunder.
- Installation methods and cable routes shall be to the satisfaction and approval of Curtin.
- Cables shall be installed in a manner eliminating any possibility of strain on the cable or on cable terminations.
- Adequate loose cable shall be left behind all equipment to facilitate inspection, adjustment or replacement.
- No joints or connections will be permitted.

- Cabling installed in environments such as external conduit and pits where it is likely to be submerged in water for a time greater than 48 hours shall be rated for underground, external use.
- Where devices are installed that have cable secured within the ceiling space, two metres of coiled cable shall be provided at each end of the cable. For fibre-optic cable, a minimum of five metres shall be coiled at each end.
- For devices or hardware with BNC (or similar) type connectors, cables are to be terminated using an approved high-quality connector that is matched to both the cable and the device that the cable is being connected to. These connectors shall be applied to the cable using a custom crimping tool that is specifically designed for the connector type. Under no circumstances will adaptors, reducers or gender changes be permitted.
- For devices or hardware with circuit board-mounted RJ45 (or similar) type sockets, interface cables are to be terminated using an IDC style connector that is matched to both the cable and the device that the cable is being connected to. These connections shall be applied to the cable using a custom crimping tool that is specifically designed for the connector type. Under no circumstances will adaptors, reducers or gender changes be permitted.
- For devices or hardware with RJ45 (or similar) panel-mount sockets, e.g. with data patch panels and data outlets, cables are to be terminated using an IDC style connector.
- To the extent possible, patch leads (for video, data, voice, audio, optical) shall not be manufactured on site but be purchased in a pre-made and pretested form from a recognised supplier/wholesaler.
- Patch leads must be from the same manufacture as the permanent link
- DIN rail-mounted terminal blocks shall be used as the means to make individual cable connections to the same source, such as the 'common of an alarm input' or an 'extra low voltage power supply'. DIN rail-mounted terminal blocks providing a common source to multiple cables shall be fitted with a custom bridging link. The security contractor shall provide spare (unused) capacity of 20 per cent or five terminals (whichever is the lesser) for future use.
- DIN rail-mounted terminal blocks shall be colour coded or permanently labelled to clearly differentiate between DC power supplies, AC power supplies, LAN earth, alarm inputs and relay outputs. Terminal partitions shall be used as a means to provide physical segregation.

7.1.1 CABLE DAMAGE

During the installation of cable where any kinks or abrasions to the insulation, braiding, sheathing or armouring occurs, the affected cable shall be withdrawn and replaced with new cable.

In the event of finding evidence for reasonable doubt as to the non-compliance with this clause, Curtin reserves the right to direct that the suspect cable be withdrawn for inspection. The cost of withdrawing and replacing the cable shall be at the security contractor's expense.

7.1.2 CABLES IN CEILING SPACE

Cables in major cable routes shall be installed on cable trays.

Cables shall be supported at intervals not exceeding 1,000 mm utilising catenary wires, approved trimmers, and roof or ceiling support members.

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

A minimum clearance of 400 mm shall be maintained from false ceilings, luminaries, hot water pipes or other heat or electrical noise generating equipment.

7.1.3 CABLES IN CONDUIT

In addition to the general requirements, cables shall be installed in conduit in such a way as to prevent twisting or kinking of the cables or damage to the cable sheaths.

Communications, data or security cables installed in underground conduit shall be complete with an external nylon jacket.

7.1.4 CABLE IN DUCTING

Where cables are installed in ducting, cables shall be grouped and taped for easy identification.

Holes in ducting through which cables pass shall be provided with a suitable grommet.

Changes in direction of ducting shall be set so that the maximum bending radius of cables enclosed in the duct will not be exceeded.

7.1.5 CABLE IN PITS

Cables in pits shall:

- be neatly loomed and supported to prevent cable damage and to assist in cable identification
- be labelled at no less than 200 mm and no greater than 300 mm upon entry to the pit with an approved cable label. (Refer to section 7.1.7 Cable Numbering.)

7.1.6 CABLES ON TRAYS

Cables shall be neatly loomed, securely fixed to the tray and installed parallel with the edge of the tray.

Cables shall be arranged on the tray to ensure:

- unnecessary crossover of cables is avoided
- adequate ventilation is allowed to prevent heating of cables
- segregation of independent services.

7.1.7 CABLE NUMBERING

Cables and cores shall be allocated, identified and fitted with unique cable numbers.

Labels shall be affixed within 250 mm of each termination and on the end crimp for cores and in all instances physically located so that the label is in plain view.

Labelling shall use the Dymo Industrial–Rhino heat-shrink system for all cable labels, unless otherwise approved by Operational Technology. Approval shall be sought for each package of work, regardless of previous arrangements.

Cable identification numbers shall be allocated using an established prefix allocated by Operational Technology and submitted for approval. Cable identification numbers shall be recorded and submitted as part of the project cabling schedule.

Cables shall be fitted with tags at the following points:

- on the cable sheath next to the gland at each end
- in cable pits
- at any additional point on the cable sheath (or around the core bunch) where the preceding requirements are not readily traceable from the core terminations.

Cable identification tags shall be orientated uniformly to read left to right from the logical viewing point horizontally, and from top to bottom when viewed vertically.

Duplication of cabling and equipment identities shall be avoided.

The following table should be referred to when developing the cable schedule and labelling of cables:

Cable Label	**Core Label (at termination connection)**	
D 4.01-1	BEN 314.IFC.04.01	Input 1
D 4.01-2	BEN 314.IFC.04. 01	Input 2
IFC#01 FIRE	BEN 314.IFC.04. 01	Input 3
IFC#01 MAINS FAIL	BEN 314.IFC.04. 01	Input 4
IFC#01 BATT LOW	BEN 314.IFC.04. 01	Input 5

7.1.8 COORDINATION AND SEPARATION OF SERVICES

Each respective section shall have installed systems and services physically separated from other systems to a disciplined and coordinated layout plan. Adjacent services shall run approximately parallel. Crossing services shall cross at approximate right angles.

Individual services between common points of the work shall follow similar parallel routes.

Cables shall be parallel to the building's major axes.

7.1.9 COORDINATION AND FEASIBILITY

The drawings, schematics and specification indicate the main routes and positions for the various service installations and equipment in relation to the building and other services.

Details shown on the drawings shall be checked and the detailed layout coordinated with the building structure and other services. Details of proposed major cable routes shall be submitted for approval before proceeding.

7.1.10 SPECIAL CABLING

Where the equipment being supplied and installed requires special cabling (e.g. screened cables, unshielded twisted pair, coaxial, optical fibre, blown optical fibre and other special types of cable), the special cabling is to be provided.

When designing the cabling system network, the type of cable required for the interconnection of the various components that make up the total system to be installed shall be determined. This shall comply with the performance requirements of the appropriate Act, regulation, standard of performance requirements of this specification, whichever requires the highest performance.

Correct shielding is to be provided to all data, audio and video cabling to remove all EMI (electromagnetic interference).

7.1.11 COAXIAL CABLING

Coaxial cabling used for the purpose of closed circuit television (CCTV) within buildings or other approved short-haul distances shall, as a minimum, be RG-59B/U with a solid pure copper core and minimum 95 per cent copper braid shield. The copper shall have less than two per cent impurities.

7.1.12 ELECTRICAL AND COMMUNICATIONS CABLING

The UTP, fibre communications cabling and electrical cabling works shall be undertaken by a Curtin-registered and inducted communications or electrical contractor.

Refer to *000313 PDG Data Communications Cabling Requirements* and *000312 PDG Electrical Services Guidelines* for specific requirements.

7.2 CABLING – ABOVE GROUND

7.2.1 GENERAL CABLE ENCLOSURES

Cabling shall be installed in cable enclosures, unless protected from mechanical damage by building structures. Cable enclosures shall be installed:

- within internal ceiling or roof spaces via catenary systems
- cast into concrete walls, floor slabs, in wall cavities and the like; rigid or flexible PVC conduit may be installed.

In plant and service rooms and other similar areas, rigid or flexible steel conduit, steel cable ducts or steel cable trays shall be installed. Steel conduit and cable ducts shall be painted to match the adjacent structures.

Cabling in risers shall be installed on a cable tray for the full height of the riser with equipment panels, cubicles and fibre optic termination panels mounted over the top of the cable tray (wherever possible) to reduce the space usage.

Cable enclosures and conduit shall be concealed. No surface-mounted cable enclosures or conduit shall be installed without prior approval from Operational Technology. Approval shall be sought for each instance regardless of previous arrangements.

Cable enclosures and conduit necessary for the installation of cabling for the various systems shall be supplied and installed as specified in this document.

7.2.2 CONDUIT

Conduit shall not be surface-mounted without prior approval from Operational Technology. Approval shall be sought for each instance regardless of previous arrangements.

Conduit installed shall comply with the minimum requirements of this specification and any relevant standards, whichever requirement is greater.

Unless other specified, conduit used throughout the installation shall be light-duty rigid PVC.

Conduit work shall:

- comply with relevant local or international standards for conduit and fittings
- not have oval conduit installed
- have a minimum size conduit of 20 mm
- be considerate of reasonable spare internal capacity, drawing in of future cables and heat expansion.

Conduit and ducts shall be of an adequate size and have the reserve capacity for at least one additional circuit, unless the conduit size is specified.

Conduit saddles (double saddles) shall be spaced at a maximum of 1,200 mm apart.

Half saddles shall not be used and will not be accepted.

Where saddles cannot be fixed to the building structure, a suitable bracket shall be supplied and installed.

Conduit shall be a minimum of 1,500 mm clear of gas and hot water pipes.

Conduit shall be installed parallel with any existing conduit or pipework.

Conduit installed in cavity walls shall be fixed to the external surface of the inner face and shall not touch the outer face.

PVC conduit joints shall be made solid and waterproof using an approved PVC welding solution.

Metallic conduit that is exposed to weathering shall have a galvanised finish and be painted to match the wall finish.

Flexible conduit shall be steel PVC-sheathed conduit.

Conduit shall be installed far enough above ceilings and below floors to avoid accidental piercing, e.g. by nails, or restricting removal of ceiling tiles or floor panels.

Where possible, conduit shall be installed 150 mm clear of the underside of roof decking.

Surface conduit shall be finished and painted to match surroundings.

7.2.3 CONDUIT – FLEXIBLE

Flexible conduit shall only be installed between rigid conduit and equipment subject to movement or vibration and across seismic joints and is only be installed internally.

7.2.4 IDENTIFICATION OF CONDUIT

The conduit to be installed shall be correctly colour coded to comply with relevant standards. In particular, conduit shall be:

- orange – for electrical power above extra low voltage (ELV)
- white – for fibre optic cabling and communications circuits including ELV circuits (i.e. security).

7.2.5 LIGHT-DUTY RIGID PVC CONDUIT

The conduit is to be a minimum size of 20 mm.

The conduit is to be stamped with conduit class, size and appropriate standard approval.

Conduit work shall meet the following:

- Set conduit where exposed to view or where permanent deformation of the cross-section will occur.
- For sets and bends, use applied heat in a manner that does not cause deformation of the conduit diameter or discoloration.
- Install PVC expansion couplings in straight conduit runs every two lengths when under roofs and every three lengths in other locations, irrespective of intervening conduit fittings or where conduit passes across structural expansion joints.
- Install saddles so conduit is held firmly in place yet allow for movement due to linear expansion and contraction of the conduit.
- Where conduit passes through a firewall, sleeve with a next sized steel conduit extending 300 mm either side of the firewall. Seal remaining gaps at each end of the steel conduit with intumescent material and pack the penetration with suitable fire-retardant material. The contractor shall provide certification of the the penetration at a 2 hour fire rating.

7.2.6 STEEL CONDUIT

Exposed external conduit shall be galvanised steel.

Steel screwed conduit fittings shall be used with Class B conduit, and galvanised where applicable.

Conduit work shall meet the following:

- Before installation, clean the threads of all conduit and fittings to bright metal by the use of taps and dyes. Internally ream ends of the conduit so they are free of sharp edges and projections. Paint exposed threads on metal conduit installations with a zinc-rich paint.
- Where the conduit terminates in wall boxes, specifically fabricated metal boxes, switchboards and termination boxes, it shall be fixed in grip entries, welded to the box or by lock nuts on each side of the box material.
- Where using lock nuts, fit a female PVC bush after the inner lock nut.
- Bends shall be made with tools specifically designed for bending steel pipe, with easy sweeps and shall comply with the manufacturer's recommended bending radius, and shall be not less than three times the external diameter of the conduit.
- Conduit bends, sweeps and the installation method shall not cause mechanical stress sufficient to result in deformation. Any conduit that is deemed by Operational Technology to have been stressed or steel work deformed shall be replaced.
- Joints in galvanised conduit and water pipe installations shall be made watertight by applying thread seal tape or other approved jointing material to threads.

7.2.7 STEEL CABLE DUCT

The ducts shall be fabricated from not less than 1.2 mm zinc anneal with machine-folded return edges for rigidity. Steel cable ducts shall only be installed in plant rooms, equipment rooms, roof spaces or risers, unless otherwise approved by Operational Technology. Approval must be sought for each instance regardless of previous arrangements.

The steel cable duct shall:

- have minimum dimensions of 50 x 50 mm and installed cable shall not exceed 60 per cent of usable capacity
- be equipped with clip-on, removable covers, not greater than 1,200 mm and be fixed with secure screws at each end
- be complete with matching couplings, elbows, reducers and the like as required
- be equipped with steel couplings between duct sections that will maintain mechanical strength and electrical conductivity
- be fitted with integral partitions throughout its length where it is necessary to accommodate different services within the common ducting envelope
- be fitted with matching bends sets etc. and other accessories

- where possible, be mounted with the lid uppermost and allowing adequate space above for access to the duct
- match the components and ensure the fixing system is complete with angle pieces, brackets and the like as required; ensuring the heads of fixing bolts are located inside the duct
- where the fixings, e.g. bolts/screws are located within the duct, use adequate silicon grommets or similar to ensure the cable sheath is protected from damage
- where ducting is installed with the lid facing downwards, provide approved fibre cable retainers at maximum intervals of 600 mm
- allow for the termination of ducts in the respective items of equipment.

There shall be coordination with other trades prior to and during the installation of cable trays and ducts to ensure that the system is installed in an efficient manner.

FLAT ON WALLS

Single ducts may be fixed directly to wall surfaces. For groups of ducts, use supports of P3300 galvanised mill strut (at maximum 1,500 mm vertical centres) fixed horizontally on the wall and spanning the total width of ducts.

FLAT ON UNDERSIDE OF CONCRETE SLABS

Single ducts may be fixed directly to the slab. Multiple ducts are to be fastened to galvanised Unistrut P330 spanning the total width of the ducts.

DOWN FROM SLAB OVERHEAD

Use supports for galvanised Unistrut P1000 with 10 mm galvanised threaded rod hangers at 1,500 mm centres.

SUSPENDED OFF WALLS AND ABOVE CEILINGS

Use supports of Unistrut P1000 or galvanised rigid MS cantilever brackets at 1,500 mm centres. Supports shall be securely supported from walls or the ceiling support system.

At each support bracket, fit to the structure and to each duct end with at least two fixings.

7.2.8 CABLE TRAYS

Cable trays shall be manufactured from a minimum 1.2 mm mild steel sheet.

The cable trays shall:

- be fabricated and shaped to provide rigidity, such that when loaded with cables plus 50 kg point load at mid span they do not deflect more than 10 mm at any point
- be perforated with slotted holes over the entire tray area suitable for the attachment of fittings/fixings using metal thread studs and nuts or nylon tray nuts complete with matching splice plates, tree, transitions and the like, as required and be of a suitable radius at changes of direction

- have a minimum bending radius of 300 mm
- in ceiling spaces, have horizontal runs of cable installed to avoid other fittings and services and where possible within the space be 150 mm above the ceiling surface unless otherwise shown on the drawing(s); and have sufficient space allowed for further removal of ceiling tiles
- in equipment rooms and roof spaces, have the positioning of tray runs shown as approximate only; installation shall be as directed on site to avoid other fittings and services
- at each support bracket, be fixed to the structure and to each tray with at least two fixing studs
- allow for their termination at the respective items of equipment.

There shall be coordination with other trades prior to and during the installation of cable trays to ensure that the system is installed in an efficient manner.

7.2.9 HEAVY-DUTY PVC CONDUIT

Underground conduit shall be heavy-duty rigid PVC.

Heavy-duty conduit is to be the size nominated on drawings.

Conduit work shall meet the following:

- The joints between conduit and/or accessories shall be solid and waterproof. Junction boxes and the like in heavy-duty conduit systems shall be complete with a neoprene gasket.
- Conduit exposed to sunlight shall be protected with an approved painted steel cover.
- There shall be no installation of conduit fittings such as elbows and bends in underground conduit runs. Changes in direction shall be made using large radius sets in the conduit or alternatively, within a cable pit.

7.2.10 CONDUIT FITTINGS

The conduit fittings shall:

- use junction boxes of adequate size to allow installation of cables without damage to the cabling installation
- not comprise elbows and tees, unless specified and shown on drawings
- be of a material and finish compatible with the type of conduit system being installed, with the exception of wall boxes.

7.2.11 PROVISION FOR DRAWING IN OF CABLE

Conduit installations shall be arranged so that:

- wiring can be readily drawn in or out without damage
- removal, damage or alteration to any part of the building structure is avoided
- no disruption to the conduit installation continuity occurs

- draw wires are provided in all conduit.

The removal of access panels, floor traps, ceiling traps/tiles (at drawn-in positions) or electrical fittings shall not be deemed to be damaging to parts of the building structure.

7.2.12 CONDUIT TO BE CONCEALED

Conduit shall be installed within walls, wall cavities, secure ceiling spaces, or contained in floor slabs, chased into walls and or otherwise hidden by the finished building structure.

When concealing conduit within walls (chased), adequate measures are to be put in place to ensure the production of dust is kept to a minimum and once completed, all surfaces are to be thoroughly cleaned and the area returned to its original condition.

7.2.13 CONDUIT AND CONDUIT FITTING INSTALLATION

Unless otherwise specified, drawn-in boxes shall be installed in a straight conduit installation at a maximum distance of 12 m apart and in other positions to facilitate the ready drawing in of cables. Where conduit runs are grouped together in accessible locations, drawn-in boxes shall be grouped together at definite and approved positions.

In inaccessible positions, conduit boxes shall not be used to change direction in or branch off from the conduit installation.

No more than one bend shall be used between any drawn-in positions. Where more than one bend is required, the change of direction shall be achieved by setting the conduit in a large radius bend.

Conduit and boxes shall be plugged in an approved manner against ingress of dirt, moisture or foreign matter. This procedure shall be carried out immediately after installation of the conduit and shall remain in place until the permanent wiring is installed.

Before the permanent wiring is drawn in, conduit shall be dry internally and free of foreign matter. Refer at all times to drawings and study the requirements of other services, e.g. mechanical ventilation ducting, piping and the location of other reticulation equipment, and install conduit and ducting clear of these.

Conduit fittings shall be rigidly secured to the conduit.

Conduit tees will not be permitted. Three-way conduit boxes shall be used instead.

High-impact PVC or nylon conduit bushes shall be fitted at all conduit ends.

Conduit installation in all positions shall:

- be installed in an orderly manner and grouped, where practicable, in one plane
- be installed parallel with the major axes of the structure
- be securely fastened to rigid supports with approved clips type or saddles – single-sided clips and saddles are not an approved fixing.

7.2.14 SUPPORT STRUCTURES

Where required, support structures shall be installed truly – either vertically, horizontally or parallel with the major axis of the building.

7.3 CABLING – BELOW GROUND

7.3.1 GENERAL

Where the common services trench is not adjacent, then the following applies:

- Install conduit a minimum of 400 mm below finished ground level.
- Install conduit to the manufacturer's preferred recommended practice.
- Excavate trenches straight and true and to an adequate depth to provide the required cover for the conduit.
- Ensure the bottom of trenches are flat and clear of protrusions such as rocks and tree roots, prior to the installation of conduit and backfill.
- Provide all shoring sheet piling or support necessary to maintain safe excavation of trenching.
- Lay a bed of clean absorbent sand 100 mm deep in the bottom of the trench.
- Arrange conduit so that the manufacturer's identification and the conduit category are uppermost and in clear view.
- Install conduit from buildings with a slight fall to the first junction box or cable pit external to the building. The box or pit shall have adequate drainage, be clean and clear of debris.
- Ensure underground conduit is provided with a 7/.067 (2.5 mm^2) PVC insulated draw wire, regardless of whether it contains cables.
- Make joints between conduit and accessories solid and waterproof.
- Cover conduit with 150 mm of rubble-free sand and place an identification tape, 150 mm above the conduit along the entire length of the conduit.
- For communications or security cable, use white plastic tape approximately 150 mm wide and indelibly marked "WARNING – COMMUNICATIONS CABLE BELOW", at not more than one metre intervals along the entire length of the conduit.
- For electrical cable, use orange plastic tape, approximately 150 mm wide and indelibly marked "DANGER – ELECTRICAL CABLE BELOW", at not more than one metre intervals, along the entire length of the conduit.
- Complete backfilling of trenches with clean fill and compact to match surrounding material.
- Perform backfilling and tamping of trenches where it passes under buildings, paths, car parks and other load bearing areas, in layers at 20 m maximum thickness.

7.3.2 CABLE PITS

Cable pits shall conform to the following:

- Install cable pits at locations required to facilitate the installation of cable without causing damage to the cable.

- Provide cables pits with Security Construction and Equipment Committee (SCEC)-endorsed lockable lids. Locking type to be coordinated with site-specific requirements.
- Ensure lids are moulded with the words "ELECTRIC CABLES", "EARTH PIT" or "COMMUNICATIONS CABLES" as appropriate.
- Ensure appropriate lid selection for the pit environment, e.g. concrete lids in landscaped areas or steel lids in heavy foot or vehicular traffic pathways.
- Drilling of neat, fitting holes shall be done in fibrous cement pits for conduit/pipe entries. Holes, no less than 4 x 25 mm, shall be drilled along the bottom of the pit for drainage purposes.
- Install pits level and with their lids flush with the finished ground level.
- Ensure the pits are the minimum size to facilitate cable installation including the minimum bonding radius.
- Neatly loom cabling within pits and support them to prevent cable damage and to assist in cable identification.

8 PRIOR TO COMPLETION OF WORK

Prior to practical completion, the following is to be completed:

- testing and commissioning of each system:
  - the system has been accepted as operating correctly
  - Operational Technology is satisfied that the system is operating as per the contract specification document
  - systems equipment has been proven to operate faultlessly for a total period of two weeks following the successful commissioning of the complete security system
- training for designated Curtin representatives to a satisfactory level of competency
- full administration rights to the systems application is handed over to the appropriate Curtin representative
- documentation has been supplied for final approval; including all documentation as specified as part of the contract.

8.1 TESTING AND COMMISSIONING

8.1.1 GENERAL

Practical completion will only be issued once the whole of the security installation satisfies the operational performance requirements and Operational Technology is satisfied that all security systems are operating effectively.

Individual building and security infrastructure shall be thoroughly tested in the presence, and to the satisfaction of Operational Technology, or nominated representative. Performance and acceptance testing shall include a thorough inspection (point by point) of the entire installation and verification that the installation complies with the requirements of this specification and the *Security Infrastructure Programming Guideline*. As a minimum, the security consultant is expected to undertake testing in accordance with the *Security Infrastructure Commissioning Guideline*.

Performance and acceptance testing to determine the security services achieve the required level of performance will only be undertaken after all routine testing, adjusting, commissioning, approvals and building work associated with the works are complete and have been fully tested and commissioned by the contractor.

All costs associated in demonstrating that the security services perform as specified, shall be borne by the contractor.

The following testing shall be conducted:

- commissioning testing of the installation
- performance and acceptance testing of the installation.

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

Testing and commissioning shall follow the Security Programming Instruction with the tests, outcomes and reports documented in the worksheets.

Testing and commissioning shall allow for any programmed staging of works. Where staging of works is applicable, elements of the works may require testing on several occasions as a result of the integration/relocation and commissioning of services and equipment as building works progress.

Testing and inspections shall be conducted as required by Operational Technology to ensure that the system and all other works comply with the project requirements.

Equipment that fails to operate correctly or is found to be installed incorrectly shall be repaired or replaced by the contractor. Where any test is unsuccessful, the defective equipment shall be repaired as appropriate and subjected to retesting.

The contractor shall provide written a "notice of intent to test" to Curtin not less than 21 working days prior to conducting the testing.

Installation and/or equipment will only be accepted by Operational Technology after satisfactory completion of testing.

8.1.2 PERFORMANCE AND ACCEPTANCE TESTING

Final performance and acceptance testing shall include the following:

- physical inspection of each point and device
- testing the function of each point and device
- testing local system functions while controllers are offline
- testing alarm response and annunciation of each point and device
- checking the logging and recording of activity for each alarm point and device
- testing the required interface with other systems for each alarm point and device
- confirming that each system performance complies with the project specification.

On completion of the works, the security contractor shall satisfy Operational Technology that the security services installation operates in accordance with the requirements of this document and the project-specific scope of works.

PERFORMANCE AND ACCEPTANCE TESTING ATTENDANCE

Allowances should be given for the following personnel (or their nominated representatives) to attend performance and acceptance testing:

- Curtin University – Operational Technology
- the security consultant
- security contractor staff.

EQUIPMENT FAILURES

Equipment failures arising during the contract shall be documented and recorded by the security contractor in a failure summary report.

The failure summary report, shall as a minimum, detail:

- the date of failure
- the parent equipment name
- details of the failure
- action taken to rectify the failure
- the number of occurrences of the failure.

8.1.3 COMMISSIONING

The contractor shall fully test and commission all security services to ensure that correct operation of all systems prior to final performance and acceptance testing with Operational Technology.

During the conduct of commissioning, the security contractor shall comply with the following:

- Confirm that all equipment is fully operational and provides the required functionality.
- Provide a comprehensive final commissioning report that outlines all test results, as-constructed details, performance test data on all cables and any other information deemed necessary for future records.
- Provide Gallagher FT activity reports for new intelligent field controllers (IFC) and new devices (e.g. doors, intrusion detection devices and any camera that has an HLI to the security management system).
- Supply all labour, materials and equipment required to fully commission and test the installation to the satisfaction of Operational Technology.
- Allow for minor programming changes and camera adjustments as a result of testing and commissioning and/or final performance and acceptance testing.
- Repair or replace any equipment that fails to operate correctly, or is considered by Operational Technology to be installed incorrectly.

8.2 TRAINING

On completion of the commissioning of the security services, the security contractor shall provide training and demonstration to Curtin representatives of the installation and shall comprehensively train client-nominated trainers and subject-matter experts, who will deliver training to operational staff, to the approval of the Curtin.

Training aids and course notes necessary to conduct effective operational and maintenance training shall be supplied by the security contractor. Training shall be comprehensive, covering all aspects of the system installed as part of these works.

8.3 DOCUMENTATION

Prior to the completion of any security works, the security contractor is to provide the following documentation for review and approval. Documentation shall be provided as per the contract requirements, in a digital format and include all product documentation, testing and commissioning sheets and drawings.

As a minimum, it is to include:

- general systems overview – a one-page, non-technical description of the actual works; with specific technical terms and jargon explained
- general description of system operation including each subsystem – a non-technical description of the installed system, how the equipment operates and user functionality
- detailed system implementation documentation and block diagram
- as-constructed drawings
- schematic diagrams for each system showing the final as-constructed system
- Gallagher FT wiring reports for all intelligent field controllers (IFCs) affected by the works and for all new devices connected to the security management system (SMS)
- completed Security Programming Instruction (that includes the testing/commissioning sheets and reports)
- cable schedules
- screenshots of the Gallagher FT graphical maps
- screenshots of the camera view taken from IndigoVision Control Centre
- equipment samples and product sheets (only those not included in the approved equipment table).

The manufacturer- or supplier-provided standard equipment manuals shall not replace the installed system specific manuals, which shall fully describe the actual systems 'as installed'.

ABBREVIATIONS

Abb.	Description
AC	Alternating Current
ACS	Access Control System
BMS	Building Management System
CAP	Campus Assistance Point
CCTV	Closed Circuit Television
CIF	Common Intermediate Format
CPTED	Crime Prevention Through Environmental Design
CU	Curtin University
DC	Direct Current
DGPO	Double General Purpose Outlet
DLP	Defect Liability Period
DVMS	Digital Video Management System
EMI	Electromagnetic Interference
FIP	Fire Indicator Panel
FFL	Finished Floor Level
FPS	Frames Per Second
GPO	General Purpose Outlet
HLI	High Level Interface
IDS	Intrusion Detection System
IFC	Intelligent Field Controller
IP	Internet Protocol
IR	Infrared
LACS	Lift Access Control System
LAN	Local Area Network
LLI	Low Level Interface
MTBF	Mean Time Between Failure
NCC	National Construction Code (formally BCA)
NVR	Network Video Recorder
PIR	Passive Infrared (Sensor)
PoE	Power Over Ethernet
OT	Properties Operational Technology
PSU	Power Supply Unit
PTZ	Pan Tilt Zoom

Abb.	Description
RAT	Remote Arming Terminal
SMS	Security Management System
UTP	Unshielded Twisted Pair
VDU	Visual Display Unit
VLAN	Virtual Local Area Network
VMD	Video Motion Detection
VoIP	Voice over Internet Protocol

REFERENCES

Reference title
000312 PDG Electrical Services Guidelines
000313 PDG Data Communications Cabling Requirements
Curtin CAD Standard
Security Programming Instruction
000327 PDG Security Infrastructure Design Guidelines
Universal Design Guidelines
000321 PDG Fire Safety Project Guideline
Security Programming Guidelines
Security Commissioning Guidelines

APPENDIX A APPROVED EQUIPMENT

Security equipment must be shown on the following approved equipment list, unless otherwise approved in writing by Operational Technology, operationaltechnology@curtin.edu.au.

A.1 Access Control System

APPROVED EQUIPMENT TYPE	MANUFACTURER	MODEL
Gallagher FT – Intelligent Field Controller (IFC) Boards and Modules	Gallagher	FT Controller 6000 – (C300100) FT Controller 6000 HighSpec – (C300101) 6000 8H Module – (C300182)
Gallagher FT – IFC Power Supply	Gallagher	FT 8A Power Supply – (C200440)
Gallagher FT – IFC Dual Cabinet	Gallagher	Dual FT Cabinet – (C200401) Dual FT Cabinet for HBUS – (C200104)
Batteries	SIOMAR	18 AH 12 V DC 7 AH 12 V DC
Card Reader	Gallagher	T15 Multi Tech Reader – (C300480) T20 Terminal – (C300460) **NB – All redundant card readers are to be replaced as part of any refurbishment or upgrade project.**
Electric Mortice Lock	Lockwood	3572 EL MO Series 60 mm Back set
Cable Transfer	Abloy	8810
Electric Strike	Padde	ES2000 ES9000 (for doors pre-load back pressure) **NB – Only to be used on doors with automated door actuators**
Electromagnetic Lock	Padde	Z2 – Monitored Z4 – Monitored
Solenoid Lock	Abloy	EL 402 **NB - To be used in place of drop bolts or vestibule locks**

APPROVED EQUIPMENT TYPE	MANUFACTURER	MODEL
Lockable Strap Bolt	Australian Defence Industries (ADI)	5004 ADI Bolt
Panic Exit Device	Lockwood	9500/9600 Series Panic Exit Device with Mortice Lock
Access Controlled Panic Exit Device	Lockwood	9000 Series
Strap Bolt	Stanco	Size to suit Door
Emergency Door Release Unit (EDRU)	Gianni Industries	CP – 33G
Press to Exit Button	Smart by Seadan Security	4350G Green
Remote Release Button	Clipsal	
Reed Switch – Concealed	Sentrol	1078C
Reed Switch – Heavy Duty	Sentrol	2200AH 2202
Reed Switch – Fire Door	Sentrol	As required to meet the fire rating of the door
Door Sounder	Altronics	S6112 – Peizo Buzzer **NB – Must be pulsating type**
Duress Button	CQR by Seadan Security	EPA-NG / PLUS
Door Closer and Accessories	Dorma	TS93-B (Pull-Side) TS-93G (Push-Side) w/Angle Bracket TS93-BEMF (Pull-Side) TS93-GEMF (Push-Side) w/Angle Bracket TS93 Limiting Stop TS93 G SR (Used on Double Doors) TS93G SR-EMF (Double Doors w/Electronic Hold Open)
Automatic Door Actuator	Dorma	ED100/250 (as required for door weight) **NB – Must be configured as 'Push & Go' and must be installed with safety sensors enabled**

APPROVED EQUIPMENT TYPE	MANUFACTURER	MODEL
Emergency Lockdown Button	Safety Technology International by Locksmith Supply Company	STI Stopper Station Push & Turn to Reset with Shield SS-2321 N/O Contact Part No. 10196 **NB – MUST BE RED BUTTON** **Custom text wording "EMERGENCY LOCKDOWN"**
E100 Escutcheon NB – TO BE USED ONLY AS DIRECTED BY SECURITY INFRASTRUCTURE	Aperio	Escutcheon – E102MU1SS1 Cover Plate – E100-PL2SSS Mortice Lock – 3572SCHOHD
KS100 Server Cabinet Lock	Aperio	KS102MB or KS102PB
AH30 Aperio 1:8 RS485 Hub	Aperio	AH30-3-0

A.2 Intrusion Detection System

APPROVED EQUIPMENT TYPE	MANUFACTURER	MODEL
Passive Infrared (PIR) Sensor	Texecom	Premier Elite AMQD
PIR 360 Degree Sensor	Texecom	Premier Elite AM 360DT
Remote Arming Terminal	Gallagher	FT Remote Arming Terminal (C200602) **NB – Once the T20 Alarm Module is available the T20 shall be used**
Internal Screamer	Secor	Peizo Siren White (Top Hat)
External Screamer/Strobe	Texecom	Premier Elite Odyssey 3 Metal

A.3 Digital Video Management System

APPROVED EQUIPMENT TYPE	MANUFACTURER	MODEL
Contractor to provide list of cameras to Operational Technology for approval for each project.	AXIS BOSCH GENETEC HANWAH iPRO	Camera selection must be capable of providing a minimum of H.264 4MP recording stream and H.264 2MP live view stream. Camera selection must conform with the intention and purpose of the camera position description (see table below)
Network Video Recorder		As Specified by Operational Technology
Camera Power Supply		As required to suit Camera **NB – Must be approved by Operational Technology and DTS**
Camera Mounts and Accessories		As required to suit camera and intent

CAMERA POSITION DESCRIPTION						
Camera selection shall be based on the following position descriptions. These are predefined based on the university's needs and the use of surveillance cameras as described within the Curtin University Security Infrastructure Digital Video Management System (DVMS) Guideline.						
Intent	**Location**	**Camera Type**	**Purpose**	**Analytics / Requirements**	**Other**	**Manufacturer**
Surveillance and Public Safety Incident & Emergency Management	Internal	Fixed Dome	Identify POI at Entrances	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				Face Recognition		Hanwha
				People Counting		
				Movement Detection		
				Direction of Travel		
		Fixed Dome	General Area Surveillance	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
		Fixed Dome		Object Detection		AXIS

			Laboratory Safety	Object Classification		Bosch
				Colour Recognition		iPro
				Face Recognition		Hanwha
				People Counting		
				Movement Detection		
				Direction of Travel		
		Fixed Dome	Secure Storage Area	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				Face Recognition		Hanwha
				People Counting		
				Movement Detection		
				Direction of Travel		
		Fixed Dome	Lift Cars	Object Detection	Must be finished to match the internal of the lift car. e.g. stainless steel, white or painted.	AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha

				Movement Detection		
		Fixed Dome or Bullet	Lecture Theatres	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
		Fixed Dome or Bullet	Classrooms	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
		Fixed Dome or Bullet	Stadium / Internal Courts	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha

				Movement Detection		
				Direction of Travel		
		Multi-Head / Sensor	General Area Surveillance	Object Detection	Capable of remote configuring the field of view and focal length of each camera	AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
		Pan Tilt Zoom	Surveillance of Lecture Theatre	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
				Object Tracking		
	External	Fixed Dome	Building Entrances	Object Detection		AXIS
				Object Classification		Bosch

				Colour Recognition		iPro
				Face Recognition		Hanwha
				People Counting		
				Movement Detection		
				Direction of Travel		
		Fixed Dome or Bullet	General Area Surveillance	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
		Multi-Head / Sensor	General Area Surveillance	Object Detection	Capable of remote configuring the field of view and focal length of each camera	AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		

		Pan Tilt Zoom	Carparks, Ovals, Large Open Spaces	Object Detection	Able to be controlled via other input sources such as Radar	AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
				Object Tracking		
				Scheduled Auto Tracking		
				Self Cleaning (Wiper)		
		Pan Tilt Zoom	General Area Surveillance	Object Detection		AXIS
				Object Classification		Bosch
				Colour Recognition		iPro
				People Counting		Hanwha
				Movement Detection		
				Direction of Travel		
				Object Tracking		
				Scheduled Auto Tracking		

				Self Cleaning (Wiper)		
Vehicle Monitoring	Roads	Automatic Number Plate Recognition	Main Entrances	License Plate Recognition		Genetec AutoVu
				Vehicle Recognition		
				Vehicle Classification		
				Vehicle Count		
				Object Detection		
				Object Classification		
				Colour Recognition		
			Secondary Intersections	License Plate Recognition		
				Vehicle Recognition		
				Vehicle Classification		
				Vehicle Count		
				Colour Recognition		
	Carparks	Multi-Head / Sensor Fixed Full Body Fixed Dome Bullet	Wayfinding and Bay Availability	Vehicle Recognition		AXIS
				Vehicle Classification		Bosch
				Vehicle Count		iPro
				Colour Recognition		Hanwha

Technical Support Cameras	Internal	Pan Tilt Zoom	Audio Visual Tech Support	Object Detection		AXIS
				Object Classification		
				Colour Recognition		
				People Counting		
				Movement Detection		

A.4 Intercom System

APPROVED EQUIPMENT TYPE	MANUFACTURER	MODEL
Slave Call Point	AXIS	2N 10” 2N 7”
IP Video Master Station	Jacques	2N Reception
Door Release Module	Advantech	ADAM 6060

APPENDIX B STANDARD DRAWINGS

The table below lists the standard installation drawings for all security equipment, which are available upon request from Drawing Services, drawingservices@curtin.edu.au.

DRAWING TITLE	DRAWING NUMBER
Curtin University Security Blocks	00MISC-SC-ST0001
Curtin University Security Standard IFC Layout	00MISC-SC-ST0002
Curtin University Standard Access Controlled Door Details	00MISC-SC-ST0003
Curtin University – Security Perimeter Auto Door Standard Requirements	00MISC-SC-ST0004
Curtin University – Security Internal Auto Door Standard Requirements	00MISC-SC-ST0005
Curtin University – Security Sliding Door Mimic Panel Line Diagram	00MISC-SC-ST0006
Curtin University – Security Actuated (Swing) Door Standard Requirements	00MSIC-SC-ST0007
Curtin University – Security Actuated (Swing) Door Mimic Panel Line Diagram	00MISC-SC-ST0008
Curtin University – Security Typical Auto Door Mimic Panel	00MISC-SC-ST0009
Curtin University Architectural – Security Building Intercom (CAP) Totem	00MISC-SC-ST0010
Curtin University Architectural – Security Building Access Totem Details	00MISC-SC-ST0011
Curtin University Architectural – Security Vehicle Access Totem Standard	00MISC-SC-ST0012
Curtin University Security Standard CCTV Telecommunications Outlet Location	00MISC-SC-ST0013

APPENDIX C FACTORY ACCEPTANCE TESTING

Where an alternative device or system is requested by the contractor, Curtin may require substantiation that it is appropriate and able to integrate with the existing security management system (SMS) prior to approval.

This may require the contractor to demonstrate the adequacy of the equipment or system by means of factory acceptance testing.

The factory demonstration shall include, as a minimum:

- operational samples of all equipment proposed to be supplied
- an operational model (limited in scale) of the sample equipment to demonstrate the functionality of each subsystem and the effective integration with the security management system
- the operational model shall demonstrate the overall alarm handling, monitoring, reporting and methodology of operation of the proposed device or system.

FACTORY DEMONSTRATION TEST SPECIFICATION

When required, allowances are to be given for the following personnel to attend the factory acceptance testing:

- Curtin University – Operational Technology
- Curtin University – Transport, Security and Parking
- Curtin University – Technology and Systems
- the head contractor
- the contract superintendent.