CURTIN UNIVERSITY

PROJECT DELIVERY GUIDELINES

SECURITY INFRASTRUCTURE DESIGN GUIDELINES

000327

Curtin University

Details of revisions			
Level	***Details***	***Date***	***Initial***
1	*Initial version prepared for Project Delivery Guidelines from Security Infrastructure Design Standard v4.0*	*Nov-16*	*RPS*
2	*Update of technical details and specifications 3.5*	*Sept-18*	*TC*
3	*Inclusion of section 5 Physical Hardware Requirements in consultation with Security, Maintenance and Building Operations Portfolio Managers*	*Sept–20*	*TC*

CONTENTS

1 INTRODUCTION

Curtin University has a strong commitment to the security of its buildings, land and spaces, and for the personal safety of all users of these areas. This commitment supports Curtin's vision for a safe and caring connected community. Key elements and strategies are applied to the planning and designing of buildings and areas and, with the complementary operational, technical and physical security measures, provide an integrated security management system.

1.1 PURPOSE

This Guideline:

- outlines the University's approach to the design and implementation of security
- outlines the minimum requirements for security equipment and technologies for specific areas at Curtin University sites.

Curtin University requires all consultants, contractors and University staff involved with decision-making that may impact on the security design of its buildings, facilities or spaces to demonstrate a level of security awareness and an understanding of security-related issues.

This document serves as a reference for:

- facility planning to identify the security requirements of University lands
- facility planning to identify the security requirements of University buildings
- physical security to identify minimum criteria for buildings
- security technology to identify minimum criteria for buildings.

The Project Delivery Guidelines have been prepared in consultation with Curtin University subject matter experts and stakeholders. It is recognised that the subject matter of Guidelines will not always be suitable for all project elements and departures from the Guidelines may be required or desirable. Departures from Guidelines must be agreed upon in consultation with the relevant University Guideline subject matter expert. Departures must be recorded in a project register and recorded and reviewed in the Project Control Group meeting minutes under its own meeting agenda item "Project Delivery Guideline Departures". Where the University subject matter expert identifies that a departure adds ongoing value to the University, the subject matter expert will update the relevant Guideline.

1.2 SCOPE

This document applies to both new building construction and refurbishment of existing buildings. In the case of refurbishment, all existing security devices within the project area of scope must be made compliant, unless otherwise approved by Security Infrastructure. That is, affected doors, cameras, intercoms and other such devices relating to security infrastructure will need to be replaced to meet the requirements in this guideline.

1.3 POLICY PRINCIPLES

1.3.1 DISABILITY AND ACCESS INCLUSION PLAN

Curtin University believes in creating equitable and inclusive access for people with a disability to its facilities, services, events and academic programs on all its Western Australian campuses.

The *Universal Design Guideline* has been developed to reflect a commitment to equity and inclusion for all by embedding Universal Design principles into project planning, design and delivery guidelines. Consultant architects, designers and engineers should make themselves familiar with the particular requirements of the *Universal Design Guideline* before responding to a project brief.

1.3.2 HEALTH AND SAFETY

Curtin University is committed to providing and maintaining high standards of health and safety in the workplace and will:

- ensure compliance with relevant legislation and the University's Health and Safety Management System
- promote an organisational culture that adopts health and safety as an integral component of its management philosophy
- ensure that health and safety is part of the business planning processes and that it is adequately resourced by all areas
- maintain an effective mechanism for consultation and communication of health and safety matters
- maintain an effective process for resolving health and safety issues and managing health and safety risks
- provide appropriate health and safety training
- regularly review health and safety performance to monitor the effectiveness of health and safety actions and ensure health and safety targets and objectives are met.

A copy of our Health and Safety Management Standards can be found at: https://healthandsafety.curtin.edu.au/local/docs/HSManagementStandards.pdf

1.3.3 GREEN STAR – COMMUNITIES

It is Curtin University policy that all new or refurbishment projects on site should support its status as Australia's first university to achieve a 5-star Green Star — Communities rating from the Green Building Council of Australia (GBCA). Designers should understand and incorporate the Green Star criteria into designs and specifications in order to maintain and enhance Curtin's Green Star status. Information on the criteria can be found in the *000325 PDG Green Star – Communities Design Guidelines.*

1.4 RISK MANAGEMENT APPROACH

This document is limited to the generic risks posed against Curtin University that are considered to apply to all its sites. Specific future risks to the University cannot be identified and subsequently cannot be catered for specifically here.

It is the responsibility of the Project Manager to profile the risks of respective buildings/areas through the User Requirements Study to ensure the security design meets their needs whilst still adhering to the requirements of this guideline. This may necessitate the development of a specific risk assessment and/or security concept plan.

The design and planning shall comply with international and national standards, state and local statutory requirements, and building and fire regulations.

1.5 LICENSING, CERTIFICATIONS, REGISTRATION

CONSULTANTS/DESIGNERS

It is mandatory that:

- the design consultants of security systems intended for installation at a Curtin University site shall be licensed security consultants
- the employers of such consultants shall be licensed security agents.

Unlicensed external personnel and companies are not permitted to provide security design and or installation work at Curtin University.

Note: It is illegal in Western Australia for a company or individual to design, specify, recommend or install security measures without the relevant licence(s).

SECURITY COMPANIES

Shall be licensed security agents and registered through the Curtin Company Registration and Inductions scheme https://properties.curtin.edu.au/workingwithus/inductions.cfm.

SECURITY CONTRACTORS

- Contractors/subcontractors who conduct works at Curtin shall hold current licences in accordance with the Western Australian *Security and Related Activities (Control) Act 1996*.
- shall be registered and inducted through the Curtin Company Registration and Inductions scheme https://properties.curtin.edu.au/workingwithus/inductions.cfm
- hold relevant certification to install and/or maintain specific equipment/systems.

1.6 RELATED DOCUMENTS

This Guideline must be read in conjunction with *000328 PDG Security Infrastructure Technical Requirements*. The specifications provides the installation requirements and device types for all University security equipment and must be reviewed during the development of any technical security specifications and prior to any works involving security devices or for security installations.

If clarification is required on any area of this document, contact Security Infrastructure, securityinfrastructure@curtin.edu.au.

1.7 DESIGN RESPONSIBILITIES

The security works shall be designed and carried out acknowledging that in most cases these facilities are public environments and all services provided shall be fit for the purpose of their intended use.

Each system and item of equipment is to be complementary in performance and duty, and shall interface with each other to operate in the most efficient manner. This shall include the interface between the various systems, as well as all interfaces to the Curtin University network.

The design and installation (including all equipment proposed for the supply and installation of the integrated security system and the devices installed by others requiring connection to the security systems provided as part of a contract) shall be capable of meeting the technical and performance requirements set out in the *000328 PDG Security Infrastructure Technical Requirement*s.

2 DESIGN STANDARDS OVERVIEW

2.1 CURTIN UNIVERSITY

Security staff essentially provide the physical presence on all Curtin University sites. The security measures and technologies employed are aids for the security staff who implement and oversee the security.

UNIVERSITY LAND

Most Curtin University sites are situated on lands that are primarily considered to be public open space. Although the roads and pathways giving access to University lands are not able to be secured in the traditional sense, these points of entry should be monitored by both fixed and pan-tilt-zoom (PTZ) CCTV cameras that will assist in identification and investigation.

UNIVERSITY BUILDINGS

While this document does not specifically address the existing buildings or proposed construction of buildings; consideration is to be given to the access and egress points for generic security requirements.

As buildings are refurbished or newly constructed the following shall occur:

- The University requirements are to be identified and any security-related matters are to be identified and referred to Security Infrastructure (SI) for approval.
- A building-specific risk assessment shall be developed for review and approval by SI.
- Building-specific security concept plans and drawings shall be developed for review and approval by SI. Where the project reflects the refurbishment of an existing building or space, then two drawings shall be provided. The first shall show the existing devices and highlight any device that is earmarked to be removed. The second shall show all new devices and any existing device that is being replaced.
- The final design specifications that address the technical specifications for security services and technologies to be installed are to be approved by SI.

When preparing the security design for a building or area, consideration must be given to allow for a system that will provide the level of protection — applied in both managerial and technological terms — to satisfy varying levels of risk. The security and safety aspects of the University buildings, in general, must be designed as a platform that can evolve in a manner that will not only match the current level of risk, but will also satisfy the requirements of Curtin University in maintaining the level of functionality with education and research being achieved in a relatively seamless manner.

2.2 SYSTEMS INTEGRATION

All electronic security systems shall be fully integrated through the utilisation of the existing security management system (SMS), access control systems and digital video management system (DVMS) via the Curtin local area network (LAN).

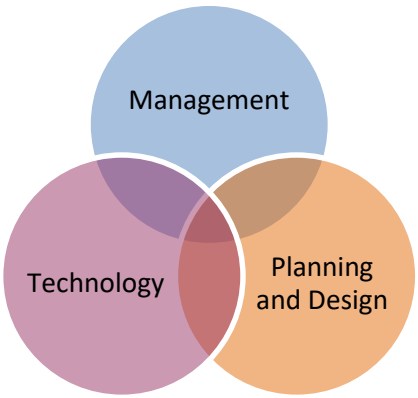
The SMS shall provide the functionality for all systems and be capable of bi-directional communication with all relevant subsystems and field equipment over the existing Curtin LAN.

2.3 METHODOLOGY APPROACH

The University's approach to the implementation of security, and in particular to the physical concept, design and evaluation process is based upon the philosophy that security is generated by three elements. The three elements, as represented below, are dependent on each other and therefore must be compatible.

2.3.1 MANAGEMENT

This refers to how buildings, spaces and facilities are organised relative to security, the individuals involved in obtaining and then maintaining a secure environment and their responsibilities/duties. Management of security must be considered the most important element in ensuring that University buildings and areas provide a secure environment where staff, students and visitors feel safe and valuable equipment, information and property is secure.



2.3.2 PLANNING AND DESIGN

This refers to security that is provided through the planning and construction of buildings and the thoughtful design of spaces and open areas. It also considers physical barriers, entry controls and secure areas for items and equipment. It includes all services to the building and recognises the traffic patterns of pedestrians and vehicles.

Planning and design also considers the principles and philosophies associated with the study of Crime Prevention Through Environmental Design (CPTED), with these being:

- natural surveillance

- natural access control
- territorial reinforcement.

CPTED considers internal and environmental features such as:

- building setbacks
- landscaping (including and excluding trees and shrubbery)
- footpaths
- public access
- lift lobbies
- reception areas
- corridors
- car parks
- lighting.

All of the above are to be considered during the design of security applicable to either the refurbishment of an existing building or area, or the planning for construction of a new building or area.

2.3.3 TECHNOLOGY

This refers to the systems and/or equipment that are provided to assist in the management of security required to meet identified risks.

The three elements must be considered to ensure University land and buildings are compatible with the intended function and align to the security requirements highlighted in the user requirements study. Therefore, the aim should be to ensure the maximum utilisation of a building subject to the individual security requirements. Excessive technology must not be employed such that it detracts from the intended function of a building and thereby becomes a hindrance.

2.3.4 OTHER ASPECTS

Further considerations with the design of security include:

- Flexibility – the security services must be flexible and adaptable so that the building can evolve with the campus, allowing any investment made to continue to provide the greatest value for many years.
- Maintenance – buildings must have the capacity to be maintained in an appropriate and cost-effective manner. The required philosophy must provide a design to facilitate maintenance with minimum interference to the functional specification of a building.

Any decision shall also reflect the cost of ongoing maintenance; recognising the needs of this issue for the future. This applies specifically to the integration of improved equipment. Recognition is required to allow for possible future inclusion of new technologies that may evolve.

2.4 SECURITY INFRASTRUCTURE

The role of Security Infrastructure (SI) at Curtin University is to ensure that the security design and installation of any electronic security adheres to the specifications, policies and procedures set down by the University and meets the University's needs and requirements.

SI conducts the User Requirements Study with the client (end user), which provides key data for the planning of operational and security requirements, and the impacts at the functioning level.

The integral role SI plays with its responsibilities and activities during the phases of the project is shown in Figure 1. SI role.

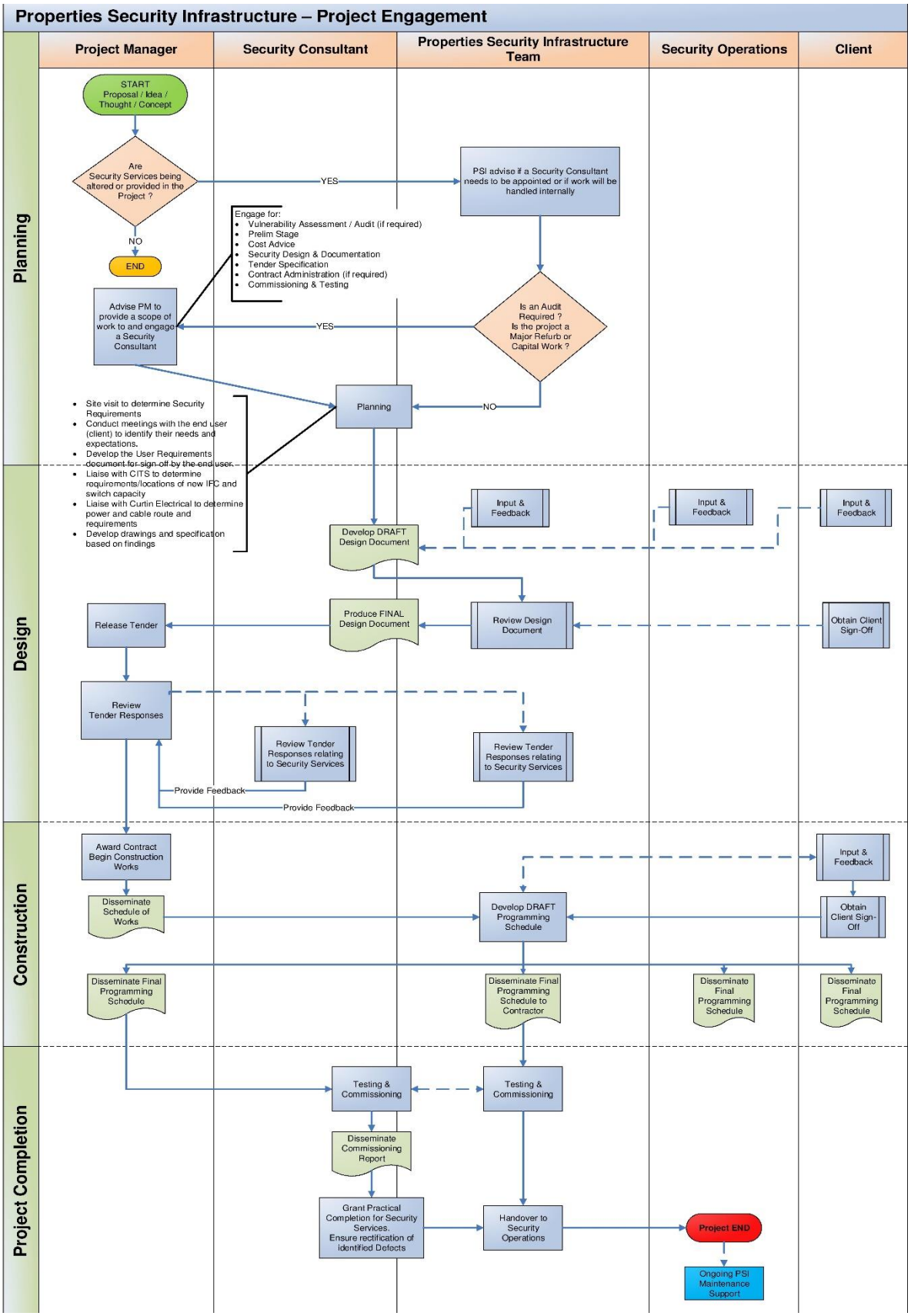


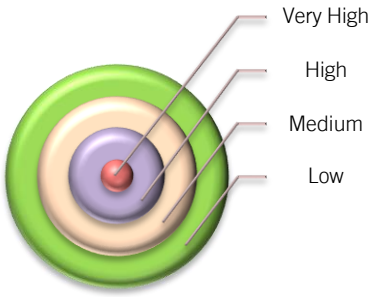
Figure 1. SI role

2.5 LEVELS OF SECURITY CONTROLLED SPACES

The University lands and buildings are used for a variety of activities. These utilise social gathering points, public open and private spaces and areas of restricted access for staff and/or students. Some require a higher level of security.

2.5.1 GENERAL

The applied standard for the University is based on four defined levels of security. These are known as the "rings of security".



The rings of security are applied to the University's lands and buildings, as shown in the below table.

Level of Security	Rating	Classification	Space / Area Type
Level 1	Low	Open Public	Pubic Space Car Parks Pathways Free Access Stairs Free Access Lifts
Level 2	Medium	Managed Pubic Space	Main Foyers Internal Open Stairs Uncontrolled Access Lifts
Level 3	High	Private	Managed Student Space Managed Staff Areas
		Restricted Vertical Access	Controlled Access Stairs Controlled Access Lifts
Level 4	Very High	Plant and Equipment Spaces	Services Plant Electrical (Low and High Voltage) Store Rooms Server and Communications Rooms
		High Security Spaces	Laboratories - Hazardous Specialist Computer Areas Hazardous Areas Student/Staff Records Chancellery and other areas as identified within the User Requirement Study

To enable the levels of security to be clearly understood, generic space drawings should be created to clearly identify the levels of security and controlled spaces in keeping with the above table.

3 SECURITY DESIGN DETAILS

3.1 OVERVIEW

The planning for and security design of any Curtin University space or building shall aim to:

- reduce the risk to the Curtin Community of being involved in criminal or anti-social behaviour
- reduce the potential for reward from engaging in a criminal or anti-social act
- increase the effort required to engage in a criminal or anti-social behaviour
- increase the Curtin Community's sense of personal safety when using Curtin University buildings, facilities and spaces
- increase the likelihood of identifying persons engaging in criminal or anti-social behaviour.

3.1.1 PUBLICLY ACCESSIBLE AREAS

These areas are classified as general landscape areas, car parks, ovals and other public areas where little, if any, security control can be enforced. Limited controls can be put in place to prevent entering or travelling through such areas.

Although the assessed level of security risk for these areas is considered low, various forms of anti-social behaviour may occur, and as such these events could affect the image and reputation of the University. These areas need to be considered and to assist in their security, general CCTV surveillance should be provided to both open areas and buildings.

In areas that allow large gatherings or are co-located near public transport pick-up and set-down points, PTZ cameras should also be considered.

3.1.1.1 Main vehicle entry points

The main entry points to the University should be covered by fixed cameras that can adequately capture the vehicle entry and exit lanes. These will be able to capture the vehicle type, registration and where possible, the vehicle occupants. Where these points are co-located near large open spaces a PTZ camera should also be considered.

3.1.1.2 Secondary vehicle entry points

At locations that are not deemed to be main entry points to the University, but vehicles access is still possible, a CCTV shall be located at a point upon that entry path that allows for the vehicle type and registration to be captured prior to the vehicle entering a car park or turning onto a secondary road.

3.1.1.3 Pedestrian access

All pedestrian access points to University land shall have sufficient CCTV coverage that will capture all pedestrian traffic at a point on the entry path prior to a pedestrian being able to enter a building or move onto a secondary path.

3.1.2 APPLICATION OF CPTED PRINCIPLES

The application of crime prevention through environmental design (CPTED) principles should also be considered to assist in reducing the likelihood of criminal activity, vandalism and anti-social behaviour.

Below are a number of strategies for publicly accessible open spaces:

- making the doors that secure emergency escape routes and that do not provide access to the building proper monitored (alarmed) to detect forced or unforced entry. This includes doors that may provide access to areas or critical importance that should be controlled and monitored via the security management system (SMS).
- making other doors including plant rooms, perimeter services ducts and building emergency escape doors for a building controlled and monitored via the SMS
- having CCTV coverage of specific controlled doors/areas, intercom points and dedicated safer pathways provided in a cost-effective manner
- having levels of lighting in public spaces and landscaped areas compliant with the relevant Australian standards and being at such a level to provide for safe and secure passage at all times. Consideration should also be given to enhanced lighting in areas that are covered by CCTV.
- designing landscaping such that it does not provide hiding places or obstruct views of the building perimeter for security patrols or CCTV
- conducting security patrols at random intervals with an increased frequency in the evenings.

3.1.3 LANDSCAPED AREAS

Landscaped areas around the campus are to be regularly maintained to ensure the size and height of trees and shrubs are kept to a minimum.

Shrubs planted at ground level should not exceed 500 mm in height when fully mature.

Shrubs in planter boxes should not exceed 700 mm in height.

The canopies of all trees must clear the ground or planter boxes by 1,800 mm to provide clear lines of sight.

Lighting should be provided during the hours of darkness. The use of effective lighting can deter vandalism, anti-social behaviour and provide lighted walkways to provide safe passage for all persons at the University. This includes lighting for those areas that may lead into dead spaces.

As a minimum, lighting levels should adhere to the relevant Australian standards. The types of illumination should be consistent for the area and requirement for that area to provide an even spread of illumination.

Shrubs and lighting should complement each other to ensure required lighting levels are achieved.

CCTV coverage should be provided for areas where high pedestrian traffic occurs including safer walkways, or if the area is being repurposed, where the expected pedestrian traffic will occur.

3.1.4 SECURITY LIGHTING

The *000312 PDG Electrical Services Guidelines* should be referenced when considering lighting requirements. The lighting design for all Curtin University buildings, facilities and spaces need to meet Curtin University requirements or Australian standards (whichever are higher). When designing the lighting for an area, consideration towards CCTV-sympathetic lighting should be employed to ensure any CCTV is not blinded during the hours of darkness.

3.1.5 SERVICE ROOMS, RISERS AND CUPBOARDS

The areas referred to in this section are ones common to Curtin University and not specific to a particular building. These areas include:

- plant rooms e.g. mechanical, hydraulic
- communications infrastructure
- power reticulation
- stand-by generators.

Access to dedicated rooms/spaces shall be controlled by having the main entry door access controlled and monitored via the SMS. The provision of access control to cupboards and risers should be considered however, unless specifically requested by the technical stakeholder group, there is no current requirement for this level of control.

The below table shows the application of control measures to these spaces.

Table 1. Control measures for service rooms

Curtin University Service Room, Risers and Cupboard		
Room Type	**Internal/ External Door**	**Access Control Requirement (see 3.5.5 Door Classifications)**
Plant room	Internal	mechanical key lock, reed switch, door sounder, door closer, (see SM Door)
	External	electric lock, card reader, reed switch, door sounder, door closer (see EN Door)
Electrical switch room	Internal	electric lock, card reader, reed switch, door sounder, door closer, (see EN Door)
	External	electric lock, card reader, reed switch, door sounder, door closer, (see EN Door)
Comms room	Internal	electric lock, card reader, reed switch, door sounder, door closer, (see EN Door)

Curtin University Service Room, Risers and Cupboard		
Room Type	**Internal/ External Door**	**Access Control Requirement (see 3.5.5 Door Classifications)**
	External	electric lock, card reader, reed switch, door sounder, door closer, (see EN Door)
Plant riser	Internal	mechanical key lock
	External	mechanical key lock, reed switch, door sounder, door closer, (see SM Door)
Electrical riser	Internal	mechanical key lock
	External	mechanical key lock, reed switch, door sounder, door closer, (see SM Door)
Comms riser	Internal	mechanical key lock
	External	mechanical key lock, reed switch, door sounder, door closer, (see SM Door)
High-voltage electrical room	Internal	electric lock, card reader, reed switch, door sounder, door closer, (see EN Door)
	External	electric lock, card reader, reed switch, door sounder, door closer, (see EN Door)

All services and storeroom doors that are monitored but do not have access control should have the following signage installed.

3.1.6 SERVER ROOMS

Computer (server) rooms housing equipment such as security, communications and building management systems (BMS) equipment are important to the daily operation of the University. To appropriately secure these rooms, the following should be considered:

- provision of electronic access control
- intrusion detection
- CCTV coverage where the plant is deemed as critical infrastructure
- external glazing having a nominal thickness of 6 mm, intruder-resistant glazing.

3.1.7 STAIRCASE CONTROL

Staircases throughout the University provide access to:

- public areas
- staff and authorised persons areas.

STAIRCASES – PUBLIC AREAS

These staircases essentially have two functions: to provide pedestrian access between floors and to provide egress in the event of an emergency.

Control of these staircases includes the following conditions:

- free entry/egress during the times of high movement e.g. 8 am to 8 pm
- secure access between 8 pm to 8 am and be restricted to emergency egress only
- secure access at all times and used for emergency egress only.

Note: The above times are indicative only. Times should reflect actual needs while maintaining the integrity of the building's security design.

Securing staircases late in the evening is intended to prevent them from becoming places for anti-social behaviour. Access during times when the staircases are secured would be via dedicated lifts that service the building. Alternatively, one staircase could be made available for access should the need arise, with the remaining staircases secured.

Lifts are not to open onto any building controlled space that may be secured during nominated periods, unless access control to each level is provided to the lift.

STAIRCASES – STAFF AND AUTHORISED PERSONS AREAS

It is preferred, from a security point of view, that all staircases that are secured at all times will have one primary function; to provide emergency egress from the upper floors of the building occupied by authorised staff and persons. It is, however, acceptable that a building may be designed to utilise the emergency stairs for movement between floors. In this instance, the access control shall be provided internally in the stairwell to prevent access onto the individual floor unless authorised. Access into the stairwell from the floor shall not be prohibited.

3.2 SECURITY PLANNING

This section shall be used to plan the security management of all buildings.

- All security devices, both internal and external, will be allowed for within the project budget.
- The perimeter treatments and all points of entry to the building or area shall be considered to be external, and as such must meet the minimum requirements for security as stated within this document.

- Internal electronic access controls and security equipment shall be provided within a building to the separate departments, or to the secure critical, hazardous or sensitive areas.
- Additional security services may be requested by individual departments during the planning phase of a project. These additional items are to be funded by the requesting department.
- While the physical security of all buildings and areas is deemed to be the responsibility of Curtin Security, the security of offices, stores, workshops, workrooms or any other internal spaces is the responsibility of the department(s) occupying the building.
- During the planning phase of any project, for a building or area, responsibilities should be clearly defined and understood by the building occupants in order to manage their understanding and expectations on security and how the installation of electronic security can be successfully utilised.
- Primarily, the system in use is a security management and access control system (SMS/ACS) that provides automatic locking of buildings at predetermined times and monitors the perimeter security status after hours. The security system and facility planning is to be designed so it is not necessary for the secure status of a building to be physically checked when an alarm reports electronically. That is, all perimeter doors must be capable of being electronically controlled in respect of their locked/unlocked and open/closed status and reporting through the security management system.
- The level of security provided to a building may not be what "should be" applied but what is practical given the operational profile and available funds. Therefore, the minimum requirements shall be applied.
- Main-entry doors and/or heavy traffic doors should be under the supervision of receptionist or administrative staff.
- After-hours entry doors shall be:
  - under video surveillance and have an intercom device present
  - capable of universal access and conform to the relevant specifications for accessibility.
- Access controlled main-entry doors and heavy-traffic doors shall be automatic sliding doors.
- Emergency stairs should not be used for vertical movement between floors or for general egress. In the event that emergency stairs are used for these reasons, movement shall be restricted to staff and authorised persons only (where possible) and not to students/visitors. Access back onto each floor shall be controlled.
- Upon entry to an emergency stair, exit shall only be permitted from the ground floor emergency escape door, or as required under the National Construction Code (NCC).
- Emergency escape doors, that are used to exit a building, shall have an audible 'door open too long' alarm. This alarm shall be monitored by the SMS.

Such doors shall not be fitted with a handle or type of grip that allows the door to be opened from the outside.

- Student computer labs shall be accessible from the central core only. The remainder of the building shall be secured after hours, controlled via electronic access control and complemented with effective CCTV coverage of the labs.
- Seminar rooms shall be accessible from the central core only. The remainder of the building shall be secured after hours, controlled via electronic access control and managed by the SMS on a time schedule.
- Lecture theatres and rooms shall be accessible from the central core only. The remainder of the building shall be secured after hours, controlled via electronic access control and managed by the SMS on a time schedule.
- Separation between staff, research personnel, graduates and undergraduates should be considered during planning.
- Access to sensitive areas (i.e. hazardous areas, laboratories, specialist computer areas, Chancellery and other areas as identified within the User Requirements Study) is to be strictly controlled. Special key sets, intrusion detection and/or access control may be considered for control of these areas.
- Meeting rooms are to be situated adjacent to entry foyers or publicly accessible areas of the core with the remainder of the building being secured after hours.
- Other external features may need to be considered when designing security including:
  - non-climbable downpipes and structures
  - window locks and restriction of window access on the ground and first floors
  - door types and door vents to prevent access through the door
  - landscaping to enhance security
  - application of CPTED principles to the building.

3.3 UNIVERSITY BUILDING OPEN TIMES

The University has a diverse work environment catering to staff, students, visitors and businesses needs and it is recognised that the expectation of when a building is open can vary from building to building dependent on the business activities of the building occupants.

The University has identified three main business areas to categorise most buildings:

- administrative
- teaching and/or research
- tenanted or leased spaces.

3.3.1 ADMINISTRATIVE

Buildings that are administrative shall have the perimeter doors with an opening time of 8 am and a closing time of 5 pm; Monday to Friday, except on University observed public holidays and shall remain closed (secured) at all other times.

Some service-based areas may be required to stay open longer (e.g. to 7 pm). These will be assessed on an individual basis; however, the above times should prevail, where possible.

3.3.2 TEACHING AND/OR RESEARCH

Buildings that have teaching and/or research spaces within them shall adhere to the same timeframes as administrative buildings; with the exception of the main entry and the internal doors leading to these specific areas. These doors shall have an opening time of 7.00 am and a closing time of 9.30 pm, Monday through Friday, except on University observed public holidays.

3.3.3 TENANTED OR LEASED SPACES

Those areas that fall under tenanted or leased spaces shall open and close at times specified by the occupant or as per the lessee agreement. All tenanted spaces must be able to be adequately 'closed off' from the remainder of the building to ensure the security of the building. It is strongly advised that all tenanted spaces be located on the ground floor or form part of the perimeter of a building that can be made accessible without the need to enter the building proper.

For University observed public holidays, all doors shall remain closed and locked until the next scheduled opening time, unless prior arrangements have been agreed with Curtin Security.

3.4 TECHNOLOGIES

As highlighted previously, there are several security systems utilised by Curtin University and all are, or are in the process of being, integrated via a high level interface (HLI) to the SMS. The access control system (ACS) acts as the security management system (SMS) for Curtin University.

3.5 ACCESS CONTROL SYSTEM

The access control system (ACS) utilised by Curtin University is the Gallagher FT Access Control System. All electronically controlled areas report to security via this system. The Gallagher FT ACS is the only system to be used when providing electronic access control.

All perimeter doors shall be Gallagher FT hard-wired connected doors, without exception.

Where the physical aspects of an area or building may make it impossible to provide a full hard-wired security solution, the University may choose to allow the use of one of two wireless type solutions. Both of these must be approved by Security Infrastructure in writing during the design phase. These systems are: Salto XS4 and AssaAbloy Aperio.

3.5.1 SALTO XS4

This type of access control solution is currently used in student housing areas and shall not to be considered for any other scenario. This system uses a combination of the Gallagher FT ACS (installed on the main entrances and flats) and Salto XS4 systems (installed on bedroom doors).

The Salto XS4 solution is not to be used on external doors.

3.5.2 ASSA ABLOY APERIO

The use of this type of access control solution shall be considered for internal doors where it is either physically impossible to provide conventional access control to a door (using the Gallagher FT ACS), or there are other factors limiting the use of the Gallagher ACS, such as a heritage-listed building. The exception to this would be all future data cabinets.

Where a new data cabinet is being installed, or where directed by either Security Infrastructure or Curtin IT Services, the cabinet shall be provided with a KS100

cabinet lock that shall be directly connected to the Curtin local area network (LAN) via a power over ethernet (POE) switch.

3.5.3 DOOR TYPES

To ensure that any door that is to be electronically controlled is capable of providing the functionality and alarm reporting required by the University, specific door types have been developed and must be used. All door openings should meet the minimum requirements for universal access.

AUTOMATIC SLIDING DOORS

When installing, the specific drawings for automatic sliding doors should be referenced. These drawings show the requirements for interfacing between the fire indicator panel (FIP), the automatic door mimic panel interface and the access control system (ACS).

Where the door pelmet exceeds 3 m in length, the pelmet shall be installed in sections no longer than 3 m. This is to ensure ongoing maintenance inspections and rectifications works can enable a single operator to remove the pelmet safely.

Note: When installing a perimeter door, and when in FIRE mode, the door shall automatically allow exit, but only allow entry to authorised persons via the ACS. No perimeter door shall "drive open" in FIRE mode. When installing an internal door, the door shall allow traffic flow in both directions, unless otherwise required (where the door acts as a smoke barrier or leads to high security areas).

SINGLE-LEAF DOOR

Single-leaf doors installed on campus must comply with the requirements for access control to ensure that they can be retrofitted with electronic access control without the need to replace the door. The specification for all doors can be requested from drawingservices@curtin.edu.au.

DOUBLE-LEAF DOOR

Double-leaf doors on campus must have an active leaf that complies with the requirements of a single-leaf door. When providing access control to a double-leaf door, the inactive leaf must have an ADI lockable strap bolt installed on the lower portion of the door as per the manufacturer's requirements. It shall also have a cylinder appropriately keyed to the Curtin University Great Grand Master Key (GGMK) system.

As a minimum, the ADI bolt must be installed on the secure side of the inactive leaf with a 450 mm bolt and the top of the door must have a skeleton strap bolt installed.

Where required, the inactive leaf can be provided with an electronic lock to allow both doors to be controlled via the ACS. If this installation has been approved by Security Infrastructure, an ABLOY EL402 solenoid lock must be installed in place of the ADI bolt and skeleton strap bolt.

ACTUATOR DOORS (EQUITY ACCESS)

Any door provided with an actuator to allow equity access must use a door actuator that is capable of being controlled via the access control system. The lead contractor must ensure the door being fitted with an actuator is fit for purpose.

When installing, the specific drawings for actuator doors should be referenced. These drawings show the requirements for interfacing between the fire indicator panel (FIP), the automatic door mimic panel interface and the access control system (ACS).

Note: Where ever possible, actuators must not be used on a perimeter door, however, where no other possible solution allows, when installed as a perimeter door and when in FIRE mode, the door must allow exit, but only allow entry to authorised persons via the ACS. No perimeter door shall "drive open" in FIRE mode. When installing an internal door, the door shall allow traffic in both directions, unless otherwise required (where the door acts as a smoke barrier or leads to a high security area).

EXTERNAL GATES (SWING)

External gates that are required to be access controlled must be constructed of a solid steel frame to the same design requirements as a single-leaf door.

EXTERNAL GATES (SLIDING)

Where external sliding gates that are to be provided with access control are installed, the gate must allow for the full monitoring and control of the gate via the access control system. The following should be considered:

- Use of a PE Safety Beam Curtain – single PE Beams (or combinations of) are not to be installed.
- Vehicle entry/exit card readers must be installed on the approved Vehicle Entrance Totem.
- If installed, the vehicle exit loop must be controlled via a timed schedule from the Security Management System and exit after hours is only permited via a valid card reader.
- If a Campus Assistance Point is to be included, a VSL-361W+ Intercom Unit shall be used and CCTV must be provided that is able to view the intercom point and the gate entrance.

ROLLER DOORS/SHUTTERS

Where a roller door or shutter is required to be monitored, it shall be provided with heavy reed switches at both sides of the door to allow monitoring of the closed state. Where a roller door is to be provided with access control, the required motor and interface controls shall be provided as part of the roller door or shutter. All roller doors that form part of the perimeter to a building must be fully access controlled and PE Beam Safety Curtains must be installed. Single PE Beams (or combinations of) will not be accepted. Where installed in a public space, consideration must also be given to providing a light and sounder to warn the public of the roller shutter closing. The sounder and light should operate for a minimum of ten seconds prior to the roller shutter closing.

3.5.4 DOOR CONFIGURATIONS

All buildings have unique entry/exit requirements; however, there are common perimeter door configurations used throughout the University. A summary of door configurations is shown in Table 2: Door configurations and described below:

DOOR CONFIGURATION 1

An automatic sliding or bi-folding door – free entry/exit during business hours and access controlled after hours. In FIRE mode, this door shall be configured to meet the University's automatic door interface requirements (document *000328 PDG Security Infrastructure Technical Requirements*). The door must always allow egress but only allow re-entry to authorised persons.

DOOR CONFIGURATION 2

An automatic sliding or bi-folding door – passageways and internal automatic sliding doors shall operate as required by the end user. In FIRE mode, this door shall be configured to meet the University's automatic door interface requirements (document *000328 PDG Security Infrastructure Technical Requirements*). The door shall allow entry and egress in both directions, unless the door is required to remain closed and locked to ensure the containment of hazards or the protection of a highly secure area.

DOOR CONFIGURATION 3

A hinged door fitted with an automatic actuator – free entry/exit during business hours and controlled after hours. IN FIRE mode, this door shall be configured to meet the University's automatic door specification (document *000328 Security Infrastructure Technical Requirements*). The door must always allow egress but only allow re-entry to authorised persons.

DOOR CONFIGURATION 4

A hinged door fitted with an automatic actuator – passageways and internal doors shall operate as required by the end user. In FIRE mode, this door shall be configured to meet the University's automatic door interface requirements (document *000328 Security Infrastructure Technical Requirements*). The door must allow entry and egress in both directions. This door cannot be used where the containment of hazards is required.

DOOR CONFIGURATION 5

A hinged door with an external (insecure side) card reader and a free handle egress. It provides controlled access in and free egress at all times (access control can be applied at all times or after hours only). The lock on this door needs to be configured as 'fail secure' if located on the perimeter of a building and 'fail safe' if internal, unless otherwise approved by Security Infrastructure (SI).

DOOR CONFIGURATION 6

A hinged door locked from both sides with an internal emergency door release unit (EDRU). It provides emergency egress only (locked from the inside and outside at all times). The door will automatically unlock during a fire alarm. Although typically installed as a Fail Safe door, where used on a perimeter door this door must be configured as Fail Secure.

DOOR CONFIGURATION 7

This is the same configuration as Door Configuration 3; however, it is required to provide free entry/exit during business hours and emergency egress after hours. This door must be configured as 'fail safe' to allow egress during a fire alarm. However, this door will allow entry into the building during a fire alarm. Given the risk to personal injury, life and building security during a fire alarm activation, use of this door configuration requires approval from SI supported by documented reasons for its use.

DOOR CONFIGURATION 8

A hinged door that allows egress only and has no external door handle to allow re-entry. This door is primarily used at fire stair exit points and plant/electrical spaces. Typically, this door has an electronic panic bar exit device and is provided with a door closer, door sounder, and a reed switch.

Table 2: Door configurations

	Door Configuration 1	**Door Configuration 2**	**Door Configuration 3**	**Door Configuration 4**	**Door Configuration 5**	**Door Configuration 6**	**Door Configuration 7**	**Door Configuration 8**	**Door Configuration 9**
Description	Automatic sliding or Bi-Folding door (Perimeter and secure areas)	Automatic sliding or Bi-Folding door (Passageways and internal doors **ONLY**)	Actuator door with external card reader and push button and/or card reader exit. (Perimeter door)	Actuator door (Passageways and internal doors **ONLY**)	Hinged door with external card reader and free handle exit	Door or Barrier with NO card reader. May be controlled by a timed schedule or alarm zone. Can be controlled from the ACS. An EDRU or Panic Release Bar (PRB) provides emergency egress only	Hinged door locked from both sides with an internal PRB provides emergency egress only	Hinged door providing free egress with no re-entry External face plate and cylinder only	Door or Barrier which is manually controlled – Monitored by the ACS and may be on an alarm schedule
Typical Door Classification	EN	EN	EN	EN	EN	SC	FE	FE	SM
Provides building access	Yes	N/A	Yes	N/A	Yes	No	No	No	No
Meets NCC requirements for emergency egress	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encourages building occupants to use dedicated egress paths (in particular at night)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Reduces re-entry into a building during a fire alarm activation	Yes	N/A	Yes	N/A	Yes	Yes	Yes	Yes	N/A
Allows re-entry during a fire alarm activation to authorised personnel via the access control system	Yes	N/A	Yes	N/A	Yes	No	No	No	No
Lock function	Fail Secure	Fail Safe	Fail Safe	Fail Safe	Fail Secure	Fail Safe	Fail Secure	Fail Secure	Not Controlled

The design of entry/egress paths to a building shall adhere to the following points.

- Configuration 1 should be used for dedicated building main entry/exit doors.
- Configuration 2 should be used for internal automatic doors only, except on rooms/areas that require a higher level of access control, i.e. the door is to remain locked and only allow authorised swipe card access at all times. See Configuration 1.
- Configuration 3 should only be used where no other solution is possible. Configuration 1 must be used unless it is physically impossible to install.
- Configuration 4 should only be used where no other solution is possible. It is always preferable for Configuration 2 to be used.
- Configuration 5 should be used for all internal doors unless the User Requirement Study has provided grounds for a higher level of security to an area/room.
- Configuration 6 should be used where the door or barrier restricts access to an area during scheduled times or is a physical barrier between two areas. An EDRU or PBR must be installed when this door or barrier prevents egress via a marked evacuation path. This door will be unlocked from the outside during a fire alarm activation.
- Configuration 7 should typically be used on the inactive leaf of service room double leaf doors or egress doors that are not required for re-entry. This door will remain locked from the outside during a fire alarm activation.
- Configuration 8 should be used where the door is not required for access but is required for emergency egress only, e.g. fire exit stairs.
- Configuration 9 should be used on internal service room doors that are not required to be access controlled, internal cupboards and risers, and any other location which might require to be monitored by the ACS but not controlled.

3.5.5 DOOR CLASSIFICATIONS

Door classifications and their requirements are described below with Table 3. Door Classifications providing further detail and associated access control equipment.

ENTRY CARD READER WITH FREE EXIT (EN)

The EN type door is the most commonly used door type.

The EN type door is monitored and controlled by the SMS/ACS and provides controlled entry (as configured by an ACS schedule), to the building or area by card reader with free egress at all times.

Monitoring of the door barrier or gate is for open/closed status, locked/unlocked status, door open too long and forced door alarms.

SECURITY MANAGED AND CONTROLLED DOOR (SC)

The security managed and controlled door, barrier or gate is installed by a third party and provides control of entry at the nominated points. The SC type door is monitored and controlled by the SMS/ACS and provides entry and egress as configured by an

ACS schedule. The timeframe for the schedule shall be determined by the User Requirements Study and must be agreed to by SI.

Monitoring of the door, barrier or gate is for open/closed status, locked/unlocked status, door open too long and forced door alarms.

SECURITY MONITORED DOOR (SM)

The security monitored door, barrier or gate is installed by a third party and controlled by others (using a mechanical key).

The SM type door is monitored by the SMS/ACS only. Monitoring of the door is for open/closed status and door open too long alarms.

Note: This type of door should only be used to monitor internal barriers such as reception windows, roller shutters, riser cabinets and the like. It must not be used on any door which give access to the building proper or to a door which is accessible from the outside of the building.

EMERGENCY CONTROLLED OR FIRE EXIT DOOR (FE)

Emergency or fire exit doors are located at emergency stairs and may control entry into or exit from the stair area.

The FE type door is monitored and controlled by the SMS/ACS and provides entry and egress as configured by an ACS schedule. The timeframe for the schedule shall be determined by the User Requirement Study and must be agreed to by Security Infrastructure (SI). Typically this door is fitted with an Electronic Panic Release Bar (PRB).

Monitoring of the door is for open/close status, locked/unlocked status, door open too long and forced door alarms).

ENTRY AND EXIT CARD READERS (EE)

Entry and exit card readers are placed on doors controlling areas of high risk and there is a legal requirement to monitor all movement in and out of the area.

The EE type door is monitored and controlled by the SMS/ACS and provides controlled entry and exit by card reader only.

Monitoring of the door is for open/close status, locked/unlocked status, door open too long and forced door alarms.

EE type doors must only be used if an audit trail of all movement into and out of a building or area is required, or for an emergency evacuation report.

Note: The use of this door type requires approval from SI and Health Safety & Emergency Management (HS&EM) and must be supported by documented reasons for its use.

ACCESS CONTROLLED LIFT (CL)

To provide better control of vertical transport in a building, card readers may be incorporated into the lift to provide floor selection as identified during the User Requirements Study. This may be controlled at all times or only during specified hours of the day.

The lift contractor is required to provide additional cables in the lift trailing cable for power and data to the lift car card reader.

An interface connection between the ACS and the lift control unit is required to provide monitoring of floor selection.

Table 3. Door Classifications provides a general overview of the types of door classifications and associated access control equipment that is required to provide access control and/or monitoring of building doors, risers and equipment cupboards.

When identifying a door classification, the use of either a 'fail safe' or 'fail secure' electronic lock is to be determined and recorded against the door in the door schedule. The use of 'fail safe' locks must only be used on internal doors or as directed by SI.

Table 3. Door Classifications

Legend – Development Classification									
Classification	Description	FHE	CR	RS	EL	PT	EDRU	DS	DC
Entry card reader only and free handle exit (EN)	Access controlled door with entry CR, RS, EL, PT, EDRU, DS, DC	YES	1	1	1	1		1	1
Entry and Exit card reader (EE)	Access controlled door with entry and exit card readers (CR), reed switch (RS), electric mortise lock (EL), power transfer devices (PT), emergency door release unit (EDRU), door sounder (DS), and door closer (DC)	NO	2	1	1	1	1	1	1
Fire Exit door (FE)	Access controlled door fitted with RS, EL, PT, DS, DC, Electronic Panic Release Bar (PBR) and may include an entry CR.	NO		1	1	1		1	1
Security Controlled door (SC)	Security Controlled door/barrier managed by a schedule fitted with a RS, EL, PT, EDRU, DS, DC	YES		1	1	1	1	1	1
Security Monitored door (SM)	Security Monitored door with mechanical (key) locking, RS, DS, DC			1				1	1
Access controlled lift (CL)	Controls lift operation as programmed by lift - CR		1						

3.6 INTRUSION DETECTION SYSTEMS

Prior to including an intrusion detection system (IDS) in a building's security design, the security design team must consider and document:

- the usage of a building

- the requirement for an IDS
- local audible alarm announcement – considering both nuisance alarms and local response
- a building user IDS management plan
- a security alarm response plan (any plan must be approved by Curtin Security prior to being implemented).

The IDS shall be managed, controlled and connected to the Gallagher FT ACS.

The University requires the use of passive infrared (PIR) detectors to provide volumetric trap detection of selected areas. The success of these detectors, measured in terms of low false alarm rates and nuisance alarm rates, is dependent on the manner in which the detectors are installed. To maximise the effectiveness of these detectors, consideration shall be given to the following:

- PIR detectors shall be positioned to face away from direct sunlight, objects of high temperature or where there is likely to be rapid changes in ambient temperature.
- Where possible, PIR detectors shall be installed in a way that they are less vulnerable to tamper and vandalism. This includes the use of tamper alarm circuits.
- PIR detectors shall not be installed in outdoor environments, unless it is specifically designed for outdoor use.
- Where possible, PIR detectors shall be positioned so that people in the field of view are required to walk across the face of the unit as opposed to towards it.

The dedicated intrusion alarm devices shall have the ability to be armed/disarmed via the following methods:

- scheduled times that are programmed via the SMS/ACS
- remotely via the SMS/ACS
- by the remote arming terminal (RAT)
- by the Gallagher FT card reader (card reader with keypad).

The IDS shall be armed either locally by the building user(s) or via a schedule controlled by the SMS/ACS. Where the building user(s) is/are required to arm/disarm the IDS, a Gallagher FT remote arming terminal shall be installed in a common space at the building entry and the IDS configured into zones for each area/department.

Remote arming terminals are not to be installed external to a building.

Where the User Requirements Study has identified the need for building users to be able to disarm or interrupt the automatic arming of a zone, a Gallagher FT T20 card reader shall be provided to allow the disarming of the zone via the University access control card. Where this type of installation is to be implemented, the IDS shall annunciate locally for a minimum of 30 seconds prior to entering the armed state.

At no time shall the IDS be configured to automatically disarm.

3.7 AREA STANDARD REQUIREMENTS FOR SECURITY DESIGN

The following section provides a detailed breakdown of the types of control measures that shall be included in the various area types on Curtin University campuses for both building and open spaces.

AREA 1 – OPEN SPACES (PUBLIC SPACE)

Control measures required:

a) CCTV surveillance of pedestrian corridors, gathering points and emergency evacuation areas with sufficient resolution to provide facial recognition of persons at a distance of ten metres from entry points.
b) Where possible, cameras shall be mounted on buildings. Poles shall only be used when there is no building mounting option available.
c) As a minimum, 75 per cent of identifiable gathering spaces must be covered by the CCTV installation.
d) External cameras must be mounted at a minimum height of four metres. If this is not possible then they must be mounted in vandal-proof housings. CCTV below this height, and within five metres of a building main entrance, must be of a dome type, within a suitable vandal-proof housing.
e) Unless otherwise specified, no camera shall have the heater or blower modules connected.

AREA 2 – PEDESTRIAN PATHWAYS

Control measures required:

a) Main pedestrian pathways shall have general CCTV coverage along the path with the ability to track a person of interest via the digital video management system (DVMS) both during and post event.
b) On the Bentley Campus, at the intersections of key pedestrian paths and The Corso, Main Street or the Living Knowledge Stream, CCTV coverage shall be installed and adequate lighting provided to enable recognition of a person at a distance of ten metres.
c) On the Bentley Campus, at the identifiable edge of the North, Central and South neighbourhoods along the three main pedestrian pathways, at least one pan tilt zoom (PTZ) camera shall be deployed, as well as a fixed camera.

AREA 3 – MAIN BUILDING ENTRANCES

Control measures required:

a) Doors deemed to provide 24-hour access to a building shall be considered the main entrance to a building and shall be fitted with an automatic door.
b) A building shall have no more than three main entrance points. These should be orientated to lead onto main pedestrian pathways in the most common direction of travel towards either public transport or car parking facilities.
c) No after-hours access point shall lead to an area of heavy vegetation, minimal light or other such areas that do not conform to providing a naturally safe and inviting feeling or with basic CPTED principles.

d) A Jacques intercom or campus assistance point (CAP) shall be installed at all main entrance points.
e) Intercom points shall have coverage from CCTV that are capable of providing visual identification of persons and of viewing the main entrance door.
f) Building entrance points shall be provided with adequate lighting as per Section 4.1.4 Security Lighting.

AREA 4 – ENTRY FOYERS AND PUBLIC INTERNAL SPACE

Control measures required:

a) Internal CCTV shall be a dome-type camera, capable of allowing visual identification of a person entering a building. The designer/installer shall avoid positioning and aiming cameras directly at entrance points to avoid issues with backlighting.
b) Natural gathering points and seating spaces that are within public internal spaces should be covered by adequate CCTV surveillance.

AREA 5 – CAR PARKS (OPEN SPACE)

Control measures required:

a) CCTV coverage of car parks should be provided to cover the entrance to the car park at the main vehicle entrance point. This should be via a fixed camera adequately housed in an approved camera housing.
b) Where ticket machines are utilised, CCTV coverage of the area should be provided.
c) Adjacent to all ticket machines, a campus assistance point (CAP) should be mounted on an approved totem.
d) Each CAP shall have a dedicated camera to view it and be capable of providing recognition of the caller.
e) In larger car parks (greater than 100 car bays), at least one pan tilt zoom (PTZ) camera shall be installed in a position to allow at least 90 per cent coverage of the car park. This is in addition to any other required fixed cameras.

AREA 6 – BIKE STORAGE AREAS

Control measures required:

a) Bike storage facilities shall be provided with electronic access control to the entrance point for each bike storage facility.
b) CCTV coverage providing visual identification of persons at no less than five metres shall be provide to all entrance points to a bike storage facility.
c) Open area bike racks shall be provided with adequate CCTV coverage.

AREA 7 – LECTURE THEATRES

Control measures required:

a) Lecture theatres are to be provided with electronic access control.

b) CCTV coverage that is capable of covering at least 90 per cent of the room with one camera providing visual identification of persons entering and leaving the space should be provided.
c) Lecture theatres are scheduled as per the Curtin University's CATS schedule within the access control system (ACS). Access to these spaces when locked is restricted to University maintenance staff, other services areas and emergency services personnel only. Staff and students are not given access to these spaces unless they are booked and the opening of the space is scheduled.

AREA 8 – CENTRALLY ALLOCATED TEACHING SPACES

Control measures required:

a) Centrally allocated teaching spaces (CATS) shall have electronic access control provided to all doors giving access to these spaces. For each space, only one of the doors needs to be fitted with a card reader, and it should be the main entry. The remaining doors that follow the main entry door, can be security controlled.
b) CATS with a seating capacity greater than twenty shall have CCTV coverage provided capable of covering at least 90 per cent of the room, with one camera capable of providing visual identification of persons entering and leaving the space.
c) CATS that contain high value and/or easily removable and attractive equipment shall be treated as per part b.
d) CATS are scheduled as per the Curtin University's CATS schedule within the access control system (ACS). Access to these spaces when locked is restricted to University maintenance staff, other services areas and emergency services personnel only. Staff and students are not given access to these spaces unless they are booked and the opening of the space is scheduled.

AREA 9 – SCHOOL TEACHING SPACES TUTORIAL ROOMS

Control measures required:

a) These spaces do not require any form of electronic access control or CCTV coverage, unless specifically requested.

AREA 10 – PLANT, ELECTRICAL AND SERVICE ROOMS

Control measures required:

a) See Section 3.1.5 Service Rooms, Risers and Cupboards.

AREA 11 – LIBRARIES AND HIGH TRAFFIC PUBLIC SPACES

Control measures required:

a) Where the entrance to these spaces is located at the perimeter of a building, the entry/exit path shall be treated as a main building entry. See Area 3 – Main Building Entrances.
b) At least 75 per cent of the interior space shall be provided with CCTV coverage with at least one camera providing visual identification of person entering and leaving the space at no more than five metres from the entry/exit point.

c) Any area that is specifically designed as student hot-desk work stations must be covered by CCTV.

AREA 12 – LEASED, TENANTED SPACES (CURTIN UNIVERSITY-OWNED)

Control measures required:

a) Where the entrance to a leased space is located at the perimeter of a building, the entrance shall be treated as a security monitored door (under 3.5.5) and monitored via the security management system.
b) Where a tenanted space is capable of giving access to a building proper, such openings or doorways must be capable of being automatically secured, locked and monitored by the security management system at such times as the building may be secure but the tenanted space remains open.
c) Any requirement for intrusion detection shall be the responsibility of the tenant.
d) If required by the tenant, any internal intrusion detection shall be stand alone and will not be connected to the security management system. All costs associated with the installation of the IDS, programming, monitoring and ongoing service of the installation shall be met by the tenant.
e) It should be understood by the tenant that even though Curtin Security monitors the building perimeter, Security will not respond on behalf of the tenant.

AREA 13 – GENERAL STAFF OFFICES (INTERNAL PRIVATE SPACE)

Control measures required:

a) These spaces should be controlled by the use of mechanical lock and key.
b) Doors shall be capable of being retrofitted with a electronic mortice lock to allow access control of the space (if requested at a later date).

AREA 14 – RESTRICTED STAFF OFFICES (INTERNAL PRIVATE SPACE)

Control measures required:

a) Doors that provide a line of demarcation between general public and student access areas and those specifically designated for staff shall be fitted with electronic access control.
b) Doors that lead into an area, space or room being controlled by electronic access control must also be electronically controlled.
c) Once a door becomes electronically access controlled, the cylinder must be changed to the area access control key and not left on a building key.

AREA 15 – FIRE STAIRWELLS

Control measures required:

a) The landings to each floor level shall have CCTV coverage capable of visually identifying a person arriving or leaving at that stairwell.
b) Stairwells that are to be controlled must allow authorised persons entry onto each individual floor (unless unrestricted access is required under the National Construction Code).

c) Stairwells that exit directly outside of the building shall be provided with electronic access control and must provide free handle egress.

AREA 16 – LIFTS

Control measures required:

a) Lifts must be capable of being access controlled even if they are not initially required to be so.
b) Lifts that prevent access onto a secure floor shall have the card reader installed internally within the lift and shall restrict the ability to select a restricted floor level until an authorised card has been presented to the card reader. Upon validation of an authorised card, the lift panel shall accept the floor request for a period no less than ten seconds and no greater than twenty, once only.
c) Lifts that prevent access to all levels within a building can have a card reader installed that acts as the lift call button. The lift shall not be called to a floor until an authorised card has been presented to the card reader. Once called, the lift shall allow access to any level in the building.
d) If required for highly secure areas, a combination of points b) and c) may be installed.
e) Lift foyers shall have CCTV coverage capable of visually identifying a person entering or exiting the lift.

AREA 17 – CHEMICAL, GAS BIOLOGICAL LABS AND RESEARCH AREAS (RESTRICTED SPACE)

Control measures required:

a) Doors from public, managed public or private spaces shall have electronic access control.
b) Doors leading into clean rooms shall have electronic access control.
c) Doors leading into lab areas are to have electronic access control.
d) Office spaces within a lab may be under the control of a mechanical lock and key.
e) Required devices that regulate or monitor air quality within a lab must interface with the building management system and provide a contact relay to the intrusion detection system. This detection system shall provide any necessary alarm inputs to an external monitoring station via the security management system.
f) Any lab requiring such specialist devices must have CCTV coverage capable of viewing 95 per cent of the lab space.

AREA 18 – HAZARDOUS MATERIALS STORAGE

Control measures required:

a) Doors leading into a hazardous materials space shall have electronic access control.
b) Doors shall be solid core doors that meet the required Australian standard for the type of material being stored.
c) Intrusion detection shall be provided to the space and a specific alarm action plan is to be created that details:

- location of the alarm point
- hazards or other warnings
- first response actions to be taken by the responding security officer
- secondary actions to be taken
- required reporting and call out contact details.

d) At least 95 per cent of the interior space shall be provided with CCTV coverage with at least one camera providing visual identification of person entering and leaving the space at no more than two metres from the entry/exit point.

AREA 19 – GALLERY, ART STORAGE, ANATOMY STORES AND OTHER SPECIAL FACILITIES

Control measures required:

a) Perimeter doors shall have electronic access control and shall be monitored by the intrusion detection system.
b) Exterior windows that open shall have reed switches installed. These shall be monitored by the intrusion detection system.
c) At strategic locations throughout the facility, passive infrared motion detectors shall be deployed to detect the unauthorised movement of people in the building or area. In high security spaces, these shall be interfaced with the CCTV.
d) Storage areas shall be secure at all times. Intrusion detection shall be deployed within the space and have CCTV coverage of at least 80 per cent of the space, with at least one camera providing facial recognition of any person entering the space at no more than five metres from the entry point.

AREA 20 – DRUG CABINET AND STORAGE AREAS

Any drug that is restricted, not publically available or may be vulnerable to criminal or intentional misuse must be covered by electronic access control, intrusion detection and CCTV.

a) Storage areas must be housed within a secure area of the building.
b) Storage areas shall have electronic access control that is secure at all times. Intrusion detection shall be via the monitoring of all doors giving access to the space and via an internal passive infrared device that shall interface with the CCTV.
c) CCTV shall be provided to cover 95 per cent of the internal space, with at least one camera providing facial recognition of any person entering the space at no more than two metres from the entry point.

AREA 21 – PERIMETER DOORS

Perimeter doors to all Curtin University owned buildings must be connected to the security management system. Under no circumstances should a door rely on human intervention to ensure a door is secured and locked, i.e. no mechanical locking of perimeter doors.

AREA 22 – INTERLOCK DOORS

Where it has been identified that a door, or group of doors must remain locked until another door is made closed and secure, or, a piece of equipment is in the 'off' position, the doors shall be controlled by the security management and access control systems. Examples of these are:

- an airlock into an air tight space that requires one door to be closed before the next can be opened
- a door giving access to a laser lab that is required to remain locked if the laser is in operation.

AREA 23 – CURTIN UNIVERSITY LEASED PREMISES

Those areas that Curtin University may occupy but not own, shall be treated the same as a Curtin University owned building, to the extent that the lease may allow.

3.8 DIGITAL VIDEO MANAGEMENT SYSTEM

IndigoVision is the enterprise-wide digital video management system (DVMS) installed throughout Curtin University. The DVMS is based on utilising new internet protocol (IP) and existing analogue closed-circuit television (CCTV) cameras located throughout the University. CCTV footage is managed and reviewed via the IndigoVision control centre software and recorded on IndigoVision network video recorders (NVRs) via the University local area network (LAN).

Cameras that are installed to provide coverage of intercom points, entry/exit doors or other areas deemed to be high risk areas shall be able to initiate alarm views via the high level interface (HLI) between the SMS and the DVMS.

The following alarms shall be configured as and when required by SI:

- forced door alarms
- intercom call activation
- building fire alarm
- IDS alarm/camera movement (as requested).

New CCTV cameras installed for security purposes shall be IP-based and must be connected to the DVMS via the Curtin LAN.

Cameras connected to the DVMS must record to the IndigoVision NVRs at a minimum frame rate of 25 frames per second at 4CIF (common interchange format) resolution and provide a viewing stream frame rate of 13 frames per second at 4CIF.

Unless otherwise directed, all IndigoVision NVRs shall be located within dedicated Curtin University data centres and shall record each camera stream for a minimum of thirty-one days.

3.8.1 CAMERA INSTALLATIONS

The University has minimum requirements for where a camera is to be installed and the purpose of the camera. Table 4 provides assistance in identifying areas that are required to have CCTV. This does not mean additional coverage is not necessary. Each space should be reviewed as part of the security risk assessment specific to the project.

Table 4: CCTV camera installation guide

CCTV Camera Installation			
Location	**Camera Type**	**Purpose**	**Expected View**
All external cameras Cameras located externally shall be connected to the DVMS, without exception	Fixed or PTZ	To be clearly identified during the planning phase. This includes any camera being installed that may be required for maintenance purposes	As identified in the planning phase
Campus assistance points (CAP)	Dome or PTZ Consideration of a PTZ should be given if a large area of interest is located nearby or there is more than one CAP that can be captured by the one camera	Provide a clear image of the person initiating the call from the CAP and the surrounds. If located at a building entry, should also include the associated entry door	The immediate area surrounding the CAP which will be able to show other persons standing in the vicinity of the CAP Within 2–5 metres
Building foyers	Dome or fixed as appropriate	Provide general surveillance of the foyer	The foyer and where present, doors to lifts and stairs
Building lifts and stairs	Dome or fixed as appropriate	Provide general surveillance	The lift doors, stairs and the immediate area in each direction of the passageway Within 2–5 metres
University main vehicle entrances	Fixed and PTZ	Coverage of the entry and exit lanes	As per 3.1.1
Pathways of heavy pedestrian traffic or 'safer pathways'	Fixed and PTZ	Coverage of the pathways as per	As per 3.1.1

CCTV Camera Installation			
Location	**Camera Type**	**Purpose**	**Expected View**
Computer labs which are always accessible	Dome or fixed as appropriate	Provide general surveillance	Provide general coverage of the entire space
Teaching spaces which have valuable equipment necessary for the continued operation/use of the space, e.g. teleconferencing, movable screens or other electronic equipment	Dome or fixed as appropriate	Provide general surveillance	Provide general coverage of the entire space
Lecture theatres and any teaching space capable of seating more than 20 persons	Dome or fixed as appropriate	Provide general surveillance	Provide general coverage of the entire space
Laboratories where controlled or hazardous material is stored or used Note: If not able to be located in the space then at the first point of entry to the space	Dome or fixed as appropriate	Provide general surveillance	Provide general coverage of the entire space
Building Passageways	Dome	Provide general surveillance	Provide general coverage of all passageways to ensure a subject's movements can be tracked from the time of entering a building to the point of exiting. Cameras shall be installed in a manner that the views cross over to eliminate the potential for dead zones.

4 IP INTERCOM SYSTEM

The IP intercom system is a Jacques 650 Series that operates across the Curtin University LAN and is seamlessly interfaced with the Gallagher FT System (SMS/ACS). Utilising voice over internet protocol (VoIP) allows intercom functionality and related intercom alarms and events to be supported through the Gallagher FT graphical user interface presented to operators.

4.1 MASTER INTERCOMS

There are currently two existing master intercom stations located within the Curtin Security office. Intercom calls are to be directed to the Gallagher FT Master Intercom Unit. In the event that the security Gallagher FT workstation (SMS/ACS) is offline, the calls shall be diverted to the existing Jacques IPM-650 Master Intercom Station.

4.2 SLAVE STATIONS

Slave stations, generally referred to as campus assistance points (CAP), shall be Jacques VSL-351 intercom stations connected to the existing Jacques 650 Series Master Station via the Curtin University LAN. Slave stations shall be located:

- at all main building entry points
- in locations where there is potential for a person to be trapped on a bridge
- in other locations identified during the User Requirements Study.

All external intercom stations shall be suitably weatherproofed and located on external walls in suitable recessed mounting boxes that include a rain 'drip' cover. The speakers shall have internal protection against water damage. Each slave station shall have a sign installed above it that clearly identifies it as being a CAP with the wording:

Campus Assistance Point – Push Button To Talk To Security. If the Emergency is Life Threatening Call 000.

4.3 VIDEO INTERCOM STATIONS

Video master stations are only to be installed when it is identified as part of the User Requirements Study that a need for a 'semi-stand-alone' intercom is required. This intercom allows visitors to contact department staff within a secure area, and permits the operator to remotely give entry to the visitors. All requests for this type of requirements must be approved by the Director, Operations and Maintenance in writing.

MONITOR STATIONS

Where installed, the Jacques 650 Series Video Intercom Monitor Station shall be the VMS-750 model, which shall receive all calls during the nominated business hours of the area after which time the calls shall be redirected to the security master station.

The monitor station can be installed with or without the optional handset (JHS-1). Upon receiving a call from the entrance station, the operator shall be capable of allowing entry by pressing the 'open door' button on the LCD screen.

ENTRANCE STATIONS

Where installed, the Jacques Entrance Station VES-75K shall be connected to the existing Jacques 650 Series Master Station via the Curtin University LAN. Entrance stations shall be located within two metres of the door being accessed controlled. Upon activation, the entrance station shall perform in one of the two following ways:

- During the nominated business hours of the area, the entrance station shall call the monitor station and provide a clear image of the caller displayed on the monitor station.
- After hours, the entrance station shall be diverted to call the master intercom station and behave in the same manner as a slave station.

Entrance stations must have signage provided to clearly identify them as being building intercoms.

Building ### DEPARTMENT NAME Intercom.
In case of a Life Threatening Emergency Call 000.

4.4 INTERFACE REQUIREMENTS

Intercom call information shall be logged within the Gallagher FT System (SMS/ACS). Each slave station associated with a door shall be programmed so that, when a call is initiated, the security operator is automatically provided with door controls via the ACS for the appropriate door and the appropriate camera is displayed via the IndigoVision system.

5 PHYSICAL HARDWARE REQUIREMENTS

This section describes the minimum requirements for those areas and spaces that do not require electronic access control but still require a physical means of controlling access to the space.

Interior furniture and cabinetry locks are excluded from this guideline.

5.1 DOORS

All new timber doors shall be constructed and installed in such a manner as to allow for the future provision of access control when required. Refer to the Curtin University Architectural Standard Door Detail (0000000-A-ST0001). All new aluminium doors shall be constructed using the design information provided on the Curtin University Security Standard Access Controlled Door Detail drawing (00MISC-SC-ST0003).

All new fire-rated doors shall be constructed and installed to meet the requirements of the space they are being installed in but should include the capability of being retrofitted with electronic access control without requiring recertification of the door fire rating.

All doors that give access to a space or room large enough for a person to stand inside and close the door shall meet current accessibility requirements with regard to circulation and shall allow egress via a single-handed motion. Typically these spaces shall use a Lockwood 3570 series mortice lock and Lockwood door furniture.

5.1.1 DOOR FRAMES

All door frames shall be constructed of the same material as the door being hung from that frame (to the extent possible) and shall be of adequate strength and rigidity for the size and weight of the door being installed on that frame.

5.1.2 DOOR TRANSOMS

Where a door is installed with a transom and glazing above, the transom installed shall be suitably sized to allow for future installation of an automated door opening device and provide adequate rigidity for the operation of such a device.

5.2 ACCESS PANELS

Access panels that provide access to plant, ducting or other such inspection points shall be provided with a locking mechanism capable of being keyed to the Curtin University Master Keying System. Standalone keying systems will not be accepted.

5.3 EQUIPMENT CABINETS

Equipment cabinets shall be provided with a locking mechanism capable of being keyed to the Curtin University Master Keying System.

5.4 LOCKING MECHANISMS

The following table provides guidance on the types of locking mechanisms that shall be used at Curtin University.

Any deviation from the prescribed locking mechanism as listed below must be approved by the Portfolio Manager, Security Transport and Parking (Physical Security Policy, Section 3.6).

Table 5: Locking Mechanisms

Space	Door/Panel/ Cabinet	Allowable Lock Type	Keying
General Office/Room	Door	Lockwood 3570 Series	As directed by Security Technical Office.
Plumbing	Access Panel	Dead Latch	Plant Key
	Inspection Panel	Dead Latch	Plant Key
	Riser Cabinet Door	Lockwood 3570 Series Mortice Lock or 100 Night Latch	Plant Key
Electrical	Riser Cabinet Door	Lockwood 3570 Series Mortice Lock or 100 Night Latch	Electrical Key
	Electrical Switch Cabinet	Carbine T or L Handle to suit	
Communications	Riser Cabinet Door	Lockwood 3570 Series Mortice Lock	Comms Key
	Equipment Enclosure	Carbine T or L Handle to suit	
Fire Services	Hose Reel Cupboards		NONE
	Fire Panel Cupboards		NONE
	Fire Booster Cabinet		NONE
Toilet/Shower Cubicles	Door	Metlam Indicator Set (Vacant / Engaged)	NONE

Mechanical digital locks are not to be installed at any time. Where multiple users need access to a space, electronic access control shall be provided.

5.5 DOOR HINGES

The door hinge shall be suitable to the weight and type of door being installed.

All aluminium-framed doors shall use a face-fixed, interfold, reinforced hinge.

All timber-framed doors shall use a butt hinge as a minimum.

A minimum of three hinges will be provided to all doors.

Oversized doors shall have at least one additional hinge provided to the top of the door. These should also utilise ball bearing-type hinges wherever possible.

With the exception of toilet cubicles, all door hinges shall have non-removable pins.

5.6 PADLOCKS

All padlocks shall answer to the Curtin University Great Grand Master Keying System. Any gate where it is required for a non-Curtin entity to provide their own lock can be achieved by interlocking the two padlocks together.

ABBREVIATIONS

Abbreviation	Term
ACS	Access Control System
BMS	Building Management System
CAP	Campus Assistance Point
CCTV	Closed-Circuit Television
CIF	Common Interchange Format
CL	Controlled Lift
CPTED	Crime Prevention Through Environmental Design
CR	Card Readers
DC	Door Closer
DS	Door Sounder
DVMS	Digital Video Management System
EDRU	Emergency Door Release Unit
EL	Electric Mortise Lock
EX	Exit Card (Reader)
FE	Fire Exit
FIP	Fire Indicator Panel
GGMK	Great Grand Master Key
HLI	High Level Interface
IDS	Intrusion Detection System
IP	Internet Protocol
LAN	Local Area Network
NCC	National Construction Code (formally BCA)
NVR	Network Video Recorder
PT	Power Transfer (device)
PIR	Passive Infrared (movement detector)
PTZ	Pan Tilt Zoom
RAT	Remote Arming Terminal
RS	Reed Switch

Abbreviation	Term
SC	Security Controlled
SM	Security Monitored
SMS	Security Management System
SI	Security Infrastructure
VoIP	Voice over Internet Protocol

REFERENCES

Title of reference document
000312 PDG Electrical Services Guidelines
000325 PDG Green Star — Communities Design Guidelines
000328 PDG Security Infrastructure Technical Requirements
Universal Design Guideline – Built Form
Physical Security Policy