RMIT UNIVERSITY

Property Services

Design Standard

Volume Nine: Electronic Security

Issue 7

December 2016

RMIT University

Design Standards – Volume Nine Electronic Security

December 2016

Version Control

This document will be updated and re-issues to reflect approved change to content, and is subject to version control. The version record and status is documented below

Document Change History [1]:

Version	Date	Author	Comments
7.0	12/12/2016	Property Services	Complete review of standards

Owner

The overall responsibility for these standards resides with RMIT University Property Services, Facilities and Asset Management Service Line.

Review

This Document is reviewed every 12 months to reflect any changes in technology or utilisation.

Given RMIT will, in 2017, commence a program to change out the electronic access control systems across RMIT Melbourne campuses. This Design standard shall be reviewed following the selection of the systems to replace current system in place.

[1] Printed copies of this document are considered uncontrolled and may not reflect the most recent revision

Table of Contents

1. Introduction

1.1. Background

This document details the minimum RMIT design requirements for electronic security. It forms part of the suite of RMIT Design Standards set out below. All volumes of the standards are available on the RMIT Property Services Design Standards web page.

- Volume One Introduction
- Volume Two Architecture and Planning
- Volume Three Electrical Systems
- Volume Four Fire Protection Systems
- Volume Five Hydraulic Systems
- Volume Six Mechanical HVAC Systems
- Volume Seven Vertical Transportation Systems
- Volume Eight Building Management Systems
- Volume Nine Electronic Security
- Volume Ten Communications
- Volume Eleven Audio Visual
- Volume Twelve Landscape
- Design Standards Checklist

This document should be read in conjunction with *Volume One - Introduction,* which provides context on the organisational and governance arrangements that apply to the design and construction of new facilities and describes the key principles that underpin the requirements of the Standards:

- Safety
- Accessibility
- Innovation
- Student Experience
- Maintainability and Serviceability
- Modularity and Standardisation
- Reliability
- Compatibility
- Sustainability
- Heritage
- Life Cycle
- Precinct Wide Solutions

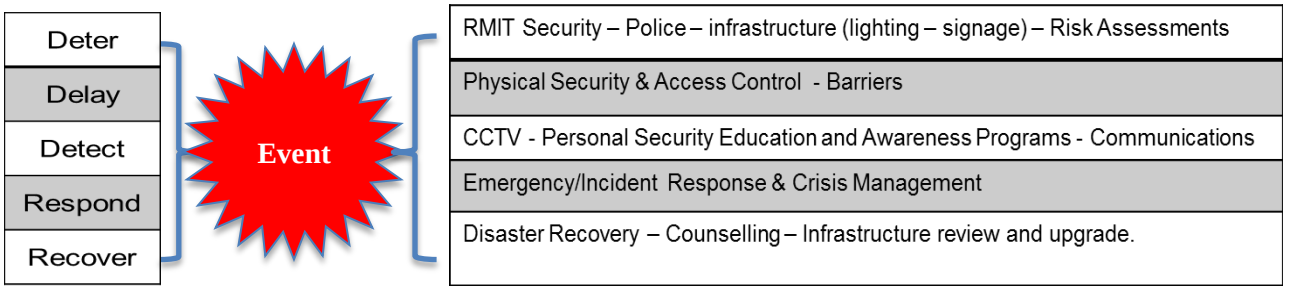
1.2. Purpose

The purpose of this brief is to set out the minimum requirements for the design and specification of electronic security services including:

- Security Access control doors
- Security Access control locks
- Security Cupboards and Risers
- Security Access Controlling equipment
- Security Access Cards
- Security System Programming
- CCTV Camera Requirements
- CCTV Camera Placement/Required field of view
- CCTV Recording
- Documentation
- Commissioning, Testing & Validation

The aim is to achieve the maximum possible consistency and standardisation across the l services systems on the RMIT University campuses in the protection of RMIT students, staff, property and information.

Australian Standard HB167:2006 - Security Risk Management sets out a methodology for RMIT to utilize in managing and mitigating security related risks. This methodology should be considered in all aspects of security management systems.



Any design aspects not specifically addressed by this brief shall be identified by the consultant during the design process and shall be brought to RMIT University's attention for resolution.

1.3. Demonstrating Compliance with the Standards

Designers are required to confirm compliance and justify any proposed deviations by completing the Design Standards Checklist.

All deviations must be approved by RMIT prior to commencing design. Unless a robust justification is provided for deviations from the Standards, it is unlikely that approval will be given.

Design Standards compliance is achieved through completion of the Design Standards Checklist and endorsement by RMIT of any proposed non- compliances.

2. Electronic Security Design Standards

2.1. General

All active Security, Access Control and CCTV Systems shall be designed, installed, commissioned and maintained in accordance with the current release of the performance provisions of the Building Code of Australia (BCA) and current relevant Australian Standards to achieve the most suitable security solution for each project.

A list of preferred Security Contractors is available from RMIT Associate Director

Risk reporting & Compliance on request. All Security contractors must meet the

following requirements.

1.1.1. All integrators and installers shall hold relevant Security Licenses (Private Security Act).

1.1.2. All installers must know, and all works must meet, relevant industry standards including:

Australian Standards:

- AS3000 Wiring Rules
- AS3080 Telecommunications Installations
- AS4410 Limits of Electromagnetic interference
- AS4510 limits of electromagnetic interference for semi-conductors devices
- AS3145 Approval and Test Specification for radio interference suppression devices
- HB 167 Security Risk Management

Australian Communications Authority:

- All current ACA guidelines and regulations

1.1.3. Only licensed Forcefield installers are permitted to work on and program the Forcefield Security System. Installers must be a minimum of Tier 2 Certified and all other contractors connecting to any part of the security system shall be a minimum of Tier 1 Certified.

Should RMIT change the base systems only authorized integrators and maintenance providers shall be authorized to work on or in the system.

1.1.4. Only certified Avigilon installers are permitted to work on and program the CCTV system. Technicians must be certified with Avigilon and approved by RMIT

2.2. Security Design Principles

The security design concept needs to be established during the early stages of a project and RMIT Security are required to be included in project meetings and be able to contribute to the Design Team effort, and work with representatives from Property Services Project team and stakeholder consultants, to develop a security system design relevant to the project.

The design and construction must take into account the existence of security personnel and security technology capabilities.

Requirement	
2.2.1.	Crime Prevention through Environmental Design (CPTED) is to be utilised where appropriate.
2.2.2.	A Threat, Vulnerability and Risk assessment must be undertaken to deliver a security risk rating in accordance with Australian Standard AS/NZS ISO 31000:2009: Risk management - Principles and guidelines and HB 167:2006 Security Risk Management NB: Risk ratings for RMIT buildings are provided in Table 1.
2.2.3.	RMIT Security services current technology capabilities are to be utilised via: • Integration with the Access Control System (Tecom/Forcefield) • Integration with the CCTV System (Avigilon) • Integration with the Alarm (intrusion and duress) System (Tecom/Forcefield) • Integration with the Help Point System (Jacques Technology)

Table 1: RMIT Building Risk Rating

Building	Rating
Storerooms containing radioactive material or dangerous chemicals	Extreme
Computer Stores (with high value equipment critical to business operations)	Very High
Areas of substantial intellectual or monetary value (e.g. computer software design, saleable medical research, etc.)	Very High
Places handling substantial quantities of money	Very High
Sensitive waste storage	High
Areas in which critical infrastructure functions are carried out (e.g. University ITS Data Center & Plant, Student Records Office and PABX rooms)	High
Areas in which critical building functions (e.g. ITS Router rooms, main plant rooms	High
Animal Houses	High
Areas in which critical administrative functions are carried out (e.g. Office of the Vice Chancellor)	Medium
Computer Laboratories, with proposed 24 hour access (with an installed equipment cost of $200,000+)	Medium
Lecture theatres (with an equipment cost of $200,000+)	Medium
Council Chambers (Building No. 1)	Medium
Front office receptionists	Medium
Buildings with high neighboring crime rate	Medium
General Academic & Administrative Offices	Low

2.3. Security access control doors

Construction of access portals, including door frames, shall cater for security door hardware and furniture, and of such design as to withstand the physical impact of door closings due to moderately incorrect air conditioning balance, or subject to windy conditions around external doors.

Selection of door locksets and particularly door closers shall depend on the type, size, weight and operation of the doors. Sufficient design shall go into the selection of correct door closers to minimise nuisance alarms and door maintenance.

Requirement	
2.3.1.	Manual lock-up of doors by RMIT security personnel shall be avoided.
2.3.2.	Frameless glazed doors, doors with a short back-set, and doors with 180 degree swings shall be avoided.
2.3.3.	Perimeter doors shall be designed to be more resistant to physical attacks e.g. no external furniture; stainless steel construction and metal strips/blocker plates to resist manipulation of the lockset deadbolts.
2.3.4.	Where double swing doors are kept open during business hours, the doors shall have magnetic door-hold-open devices which can be released when electronic lock-up controls operate to allow free flow of pedestrian traffic.
2.3.5.	Where swing doors, particularly double doors, require free access from both sides during public hours, magnetic locks with bond sensors shall be used. If these doors are on an emergency exit route, then emergency break-glass units shall be installed on the inside.
2.3.6.	For very high security, install “dog-bolts” into hinge-side edge of swing doors.
2.3.7.	**For ease of Servicing and Maintenance, access controls shall align with the model used throughout RMIT in accordance with the ‘Type of Door Guideline’ provided in** Table 2 below.

Table 2: Type of Door Guideline

Door Type & Requirements	Application

<u>Type A - Access Reader IN and or IN/OUT</u>
One-Side Access Controlled Door (swing door) with electric lockset shall have the following hardware/features:
• Entry: Proximity card reader installed on the unsecured side of the door, in case of in/out reader second card reader to be installed on secure side
• Egress: Free handle (preferred) within the lockset at the secured side of the door
• Electric mortise lock (normally fail-secure locks on power loss) type:
  • Where applicable fail-safe (unlocks on power loss) type on emergency exit door with exit sign-on in secure side of a corridor door.
  • Lockset reed switch door, inside free handle, key cylinder operation monitoring
• Electromagnetic locks can also be used for this type in high traffic areas
• Local door alarm sounder (for 1st Stage DOTL alarm, silenced during building fire alarm and silenced during 2nd Stage DOTL alarm)
• Reed switch door monitoring (where applicable additional reed switch on fixed leaf of double door)
• Concealed top and bottom deadbolts on fixed leaf on double swing doors, preferably lockable if exposed
• ADI or other University approved Blocker plate installed (where applicable on external perimeter doors)
• Door frames to be sufficient width and strength to accept electric mortise lockset to ensure “knuckles” are not scrapped when lockset handle is used in access operation
• Glazed windows in door to be of impact resistant type i.e. at least 6mm laminated glazing securely installed into the door body
	Electric Mortise are used for office spaces and classrooms
	
	Card reader in/out are used for High risk or High Security area

Door Type & Requirements	Application
<u>Type B – Access Reader IN Only</u> One-Side Access Controlled Door (swing door) with Electronic Magnetic lock shall have the following hardware/features: • Entry: Proximity card reader installed on the unsecured side of the door • Egress: Egress pushbutton installed on the secured side of the door • Integral mag lock LED indicators showing lock/unlock status of mag-lock(s) • Integral mag lock bond sense monitoring; lock bonding when lock is powered • Emergency break-glass door release unit on egress side of door (where applicable on both sides of emergency exit corridor doors) • Local door alarm sounder (for 1st Stage DOTL alarm, silenced during building fire alarm and silenced during 2nd Stage DOTL alarm) • Reed switch door monitoring (where applicable additional reed switch on fixed leaf of double door) • ADI or other University approved Blocker plate installed (where applicable on external perimeter doors)	Type B doors are specified for electronic magnetic lock installs in areas such as entry points to a Building reception area or high traffic/use office/classroom.
<u>Type C – Egress only no Access reader</u> Emergency Exit Controlled Door (swing door with electric lockset) shall have the following hardware/features: • Entry: No entry except via lockset key switch on the unsecured side of the door • Egress: Free or fixed spindle handle within the lockset at the secured side of the door • Electric mortise lock (normally fail-safe unlocks on power loss type) • Lockset reed switch door, inside free handle, key cylinder operation monitoring • Local door alarm sounder (for 2nd Stage DOTL alarm, silenced during building fire alarm) • Reed switch door monitoring (where applicable additional reed switch on fixed leaf of double door) • ADI or other University approved Blocker plate installed (where applicable on external perimeter and fire stairwell doors)	Type C doors are used in corridors and internal stairwells that are opened via time-zones, push to exit to allow egress out after hours.

Door Type & Requirements	Application
Type D – Monitored Door No Access Reader Emergency Exit Controlled Door (swing door with magnetic lock). shall have the following hardware/features: • Entry: No entry from the unsecured side of the door • Egress: No egress from the secured side of the door • Mechanical lockset: Mechanical dead latching mortise lockset with no handle on unsecured side and free handle on secured side of the door • Integral mag-lock LED indicators showing Lock/unlock status of mag-lock(s) • Integral mag-lock bond sense monitoring; lock bonding when lock is powered • Emergency Break-glass door release unit on egress side of door (where applicable on both sides of emergency exit corridor doors) • Local door alarm sounder (for 2nd Stage DOTL alarm, silenced during building fire alarm) • Reed switch door monitoring (where applicable additional reed switch on fixed leaf of double door) • ADI or other RMIT University approved Blocker Plate installed (where applicable on external perimeter and fire stairwell doors)	Type D doors are used for Fire Exits and Fire Stairwells.

Door Type & Requirements	Application

Type E - Security Monitored Door
These Doors shall have the following hardware/features:
• Local door alarm sounder (where applicable, but for 2nd Stage DOTL alarm, silenced during building fire alarm)
• Reed switch door monitoring (where applicable additional reed switch on fixed leaf of double door)
• ADI or other RMIT University approved Blocker plate installed (where applicable on external perimeter and fire stairwell doors)
• Project Architect - to specify and provide:
  • Mechanical lockset: mechanical dead latching mortise lockset with no handle on unsecured side and free handle on secured side of the door
  • Where applicable, lockable deadbolt on fixed leaf on double swing doors
  • Where applicable fixed-type hinges on doors which swing outward into the unsecured side
  • Where there is no alternative to a mag lock, a door head and frame must be sufficient width and strength prevent buckling when Z-brackets need to installed
  • Glazed windows in door (non-fire corridor doors) to be of impact resistant type i.e. at least 6mm laminated glazing securely installed into the door body
	Type E doors are used for alternate points external of internal exit/entry doors.

2.4. Security Access control locks

Supply and install electric locks as required to the access controlled doors. Electric mortise locks and electromagnetic locks; shall comply with the following specifications.

Requirement	
2.4.1.	Electric mortise locks are preferred for use in all office, classroom and computer laboratories. Model shall be: • Electronic mortise Lockwood 3572, 3582 fail safe or fail secure • With bi-colour LED integrated into the lock escutcheon plate furniture on the entry side
2.4.2.	Electromagnetic locks shall be used on all 'double doors' and can be used on single doors if approved by Security. Model shall be specified as follows: • Electromagnetic locks shall be Padde EML-6 for single doors and Padde EML-10 for double doors or approved equivalent. • When a break glass release is operated or when the fire alarm is activated, both leaves of the lock shall release.
2.4.3.	Electric strikes are only used in specific circumstances and settings, when and where applicable; guidance should always be sought from Security Services prior to specifying electric strikes. If specified, the model shall be: • *Padde ES 9000* Power to lock (fail safe) and 12 volt DC continuously rated, or approved equivalent
2.4.4.	Motorised Doors (door actuator) where required shall provide: • The ability to physically monitor the doors when open and closed • Installation of a separate electric lock (positive locking) • The ability to monitor the status of the electric lock • The ability for automatic movement sensing devices to be disabled when the doors are in access control or secure mode • Automatic safety reversing of the doors • Self-checking safety PE beams • A controller and interfacing relays capable of providing remote access control functions such as "Auto", "Open and Stay Open", "Lock" and "Local-Manual" Where applicable in emergency exit doors, the door contractor shall provide an 8-hour UPS for maintaining secure operations when the mains power fails; after which the door shall be unlocked and opened by hand.
2.4.5.	Where there is no door closer or if the door closer is deemed by the Security Contractor to be unsuitable, then the Security Contractor shall install a new door closer. Door closer shall be *Dorma TS 83* series or comparable.

2.5. Security Cupboards and Risers

The security cupboard(s) shall be located at a central location, preferably in a RMIT ITS communications room or in adjacent cupboards, and shall be accessible to authorized staff only via an ASO key.

Requirement	
2.5.1.	Door locks are to be keyed for an ASO key.
2.5.2.	Security cupboard(s) would typically consist of the following equipment: • Tecom-Challenger (CH#) wall cabinet 350mm(H) x 455mm(W) x 75mm(D) • Tecom-Challenger 4-Door Controller (4DC#) wall cabinet 395mm(H) x 590mm(W) x 80mm(D) • Tecom-Challenger Data Gathering Panel (DGP#) wall cabinet 350mm(H) x 455mm(W) x 75mm(D) • Tecom-Challenger Power Supply -Battery Units (SPSUB#) wall cabinet 230mm(H) x 240mm(W) x 90mm(D) • CCTV Network Video Recorder Server (NVS) 700mm(H) x 1000mm(W) x 150mm(D) • CCTV Power Supply 12VDC 10Amp 8-Hour Battery-Backed Unit (CPSU-10/53) 300mm(H) x 460mm(W) x 150mm(D)
2.5.3.	A typical cupboard, accommodating security and CCTV wall cabinets, shall be not less than 2000mmH x 1800mmW x 1000mmD in size. Larger cupboards shall be 2000mmW and 2400mmW for accommodating larger quantities of equipment.
2.5.4.	The cupboard is to have sufficient natural air ventilation via dust proof mesh vents near the top and sides of the cupboard.
2.5.5.	The general illumination level of cupboards shall be 400 lux and they shall be equipped with additional emergency light fittings.

2.6. Security Access Controlling equipment.

NB Subject to a pending review of RMIT electronic access control systems and an outcome in relation to the potential replacement of the current system the details in respect to this standard may change. The current platform will remain and be maintained in a mode pending the outcome of the review.

The current electronic access control system consists of the following.

Manufacturer: Interlogix

Brand: Tecom-Challenger

Software (head end): Forcefield

Door controllers: Interlogix Tecom Intelligent 4 Door controller

Door card readers: Interlogix Multiclass - Multi Format (Tecom, HDI)

Requirements for access control systems are detailed in the following table.

Requirement	
2.6.1.	All Security control equipment must be located in a secure area.
2.6.2.	Fire alarm connection required to allow Security doors to release on Fire alarm activation. In providing a Fire Alarm Interface: The Security Contractor shall provide cabling from the Access Control panel to the existing building Fire Alarm Panel. The Security Contractor shall liaise with relevant RMIT staff to facilitate final connection to the Fire Alarm Panel.
2.6.3.	Duress Alarms shall be: • Hard Wired: Honeywell 270R hold-up devices or approved equivalent • Wireless: Inovonics Wireless Eco Stream pendant style model number 123S + receiver panel
2.6.4.	Building controller/Challenger shall meet the following specifications: • Tecom Challenger V8 complete with master programming console (RAS Panel), • Communicate to the Forcefield Access Control Management system via a TCIP card - TSO898 allow for network connection that is dedicated to RMIT Security Allowance should be made for installation of all cabling from the control panel to the building network connection. *NB Challenger 10 can be used once Forcefield 7 upgrade has been completed.*

2.6.5. Door Controllers shall be type Tecom TS0866/67 and meet the following specifications:

- Fully intelligent devices capable of processing, transmitting and receiving alarm data from the system via the security network
- Be capable of storing access control data, time schedules etc. via 8 meg IUM, in the event of communications or power failure and shall update the system upon restoration of service
- Fitted with output control facilities, which shall enable activation of other peripheral field equipment either by automatic reaction to events or by operator intervention via the keyboard or mouse
- Validation and communication procedures shall be such as to check each Access Card presented against authorised data based information
- Access Card validation data and alarm status data shall be maintained locally and shall be capable of being updated via the operator's terminals
- Door Controllers shall be continuously polled by the system; when all access card data is valid, the reader terminal shall grant access; invalid data shall cause a real time exception report to be generated in the system and shall be logged and recorded on the systems data storage facility
- Door Controllers shall display mains fail and low battery conditions separately to the operator's terminals as an alarm with appropriate alarm text.

Requirement	
2.6.6.	Data Gathering Panels shall be of Tecom TS082x Series and meet the following specifications • Data Gathering Panels (DGP's) will facilitate the connection of alarm inputs from field equipment. • DGP's shall be semi-intelligent devices capable of storing alarm status data in the event of communications or power failure and shall update the control panels upon restoration of service; DGP's will also be fitted with output control facilities, which will enable activation of peripheral field equipment such as audible and visual indicators either by automatic reaction to alarms, or by operator intervention. • All critical circuitry associated will be installed within a secure area and shall be housed in a cabinet equipped with an anti-tamper device. • The installed system will be capable of being expanded to support additional inputs and outputs without the need for upgraded software or hardware. • DGP's shall display mains fail and low battery conditions separately to the system operator's terminals as alarm with appropriate alarm text.
2.6.7.	Access Readers shall meet the following specifications: • Access readers will be installed at the nominated doors as shown on the drawings/schedule, be vandal resistant and be Interlogix Multiclass-Multi Format (Tecom, HID) Smart Card proximity card readers compatible with the current RMIT proximity cards; Tecom GE Multiclass RP15 (DAS part number: S3198A). • Access readers shall be programmed within the system to provide a historical log indicating the direction of movement of a cardholder Construction of the reader shall be robust and of neat low profile appearance and be designed to protect reader components from environmental contamination. • Indication of whether access is granted or not shall be provided at the point of entry via an audible and visual indication.

Requirement	
2.6.8.	Door Release / Egress Buttons shall meet the following specifications: • SSE 4300 series with mushroom head pushbutton, Green in colour, mounted on a switch plate engraved with the wording "PRESS TO EXIT" using 5mm high Universal font. • Door release egress buttons shall be installed on the egress side of internal doors as nominated; on activation of the door release button, power will be directly interrupted to the associated electric strike; simultaneously the associated door alarm shall be deactivated for a period to allow entry through the door and the door to close whilst sending a door exit signal to the door controller. • Door release egress buttons shall be mounted at a height of approximately 1000mm above finished floor level and no more than 500mm from the door itself; the centreline of the door release egress button shall be equal to the centreline of the lock/latch assembly for the associated doors.
2.6.9.	Reed Switches shall meet the following specifications: • Sentrol 1078C or similar magnetic reed switches shall be installed on nominated doors; magnetic reed switches shall be end-on type and be flush mounted. • All reed switches mounted on pedestrian doors shall be located a minimum of 60mm but no more than 100mm from the edge of the door so as not to foul other equipment required to be mounted on that door. • Roller shutter doors and other non-standard door types shall be fitted with heavy duty robust reed switches as indicated on the drawings and shall be installed in a position so as not to be damaged by vehicles or other traffic. • Each reed switch shall be connected to an individual alarm input; the only exception shall be double sets of doors, where each leaf shall be alarmed, but connected to a single input.
2.6.10.	Sonalert Buzzers shall meet the following requirements: • Each Sonalert buzzer shall be flush ceiling mounted and complete with sound selection and level adjustment, be Radio Spares (RS 626-141) multi-tone sounders or approved equivalent. • Sonalert buzzers shall be located above each access-controlled door. • The sonalert buzzer shall sound if the door remains open longer than a predetermined period, alarm shall then be generated at the security control room. • The sonalert buzzers shall be capable of being isolated via the terminal and be disabled when the associated door is in access mode.

Requirement
2.6.11. Door Status Indicators shall meet the following requirements: • The door status plate shall comprise a Clipsal series 2000 electrical switch plate, white in colour and fitted with a green and red LED. The LED indicator panels will have one Red LED and one Green LED and be marked 'Security use only'. • The green and red LED's shall be connected and programmed via the Security System to reflect the locking status of the do or electric lock; when the door is unlocked the green LED shall be illuminated and when the door is locked the red LED shall be illuminated. • Door status indicators shall be mounted at a height of approximately 1000mm above finished floor level; the centreline of the door status indicator shall be equal to the centreline of the lock/latch assembly for the associated door.
2.6.12. Break Glass Release Units shall meet the following requirements • Break glass units shall be *KAC KW200/SW/B*, White in colour and not require undue force to break the glass. • On activation of a BG, power shall be directly interrupted to the door and an alarm shall be simultaneously raised on the security system indicating the type and location of the alarm. • Break glass units shall be engraved with the wording "EMERGENCY DOOR RELEASE - BREAK GLASS" or similar to accurately define the purpose of the device.
2.6.13. Movement Sensors (PIRS) shall be selected from the *Optex range* of Passive Infrared movement sensors and shall meet the following specifications: • Movement Detection Devices shall be either ceiling or wall mounted and shall comply with the recommendations of AS 2201.1. • Movement detectors shall be monitored by the Security System; detectors shall be selected and positioned so that minimum interference is created for the various uses of the area. • Each movement detection device shall be connected as an individual alarm input to the access control reader terminal and shall be monitored by the control panel and GE Forcefield monitoring system.

2.7. Security Access Cards

RMIT Security supplies the blank card stock used to create Security/ID cards for staff, students and the wider RMIT community.

Security access cards must meet the following requirements:

Requirement	
2.7.1.	Security Access Cards must: • Work with RMIT Transitional GE Multiclass readers • Work with RMIT ITS printer proximity card readers • Be able to be printed on one or both sides, including a Barcode and Photograph • Have a visible and unique card number for easy identification • Be encoded with set site code numbering as set out by HID and RMIT
2.7.2.	Cards will be delivered to RMIT Security first and not the end user to ensure management of sequential card numbering and issuance.
2.7.3.	Security Contractors must liaise with RMIT Security to determine end user programming requirements.

2.8. Security System Programming

The correct and consistent format for the programming of the inputs is important to the effective and efficient operation of the entire Security System.

For programming of input points in the Forcefield System, the following must be adhered to:

Requirement	
2.8.1.	Alarm Programming shall be programmed in accordance with the following: Example of PIR (motion detectors) • V 9.1.241C1/Rm031 Reception Example of duress alarms • DUR 36.3.250C65/Rm014A Rcpt Example of safety shower alarms • SS 3.4.16C35/Rm002
2.8.2.	DOTL Programming shall be in accordance with the following: Example of DOTL: • 94.2.28C9/Rm001 Gallery.
2.8.3.	Door Programming shall be in accordance with standard naming conventions: Standard naming is building number.level.door point number challenger number/room number and or descriptor plus * (for card reader) and ^ for Fire Door. Example: • 2.2.54C4/Rm01A Loans Store^*.
2.8.4.	Timezone programming shall be in accordance with the following: General timezones: • Example: *0800-1700 M/F = 8am to 5pm Monday to Friday. Asterisk * timezones can be used on all challenger and should not be edited. Specific room timezones: • Example: 2.2.54C4/Rm01A Loans Store tz . These timezones can be edited to suit clients instructions. Specific area/department times: • Example: Library times. Library times are agreed across multiple sites. Changing this timezone will affect all Challengers using these time-zones.
2.8.5.	Graphics Map Programming shall be standardised as follows: Building number and level: Example • 8001 = Building 80 level 1

2.9 CCTV Camera Requirements

Requirement	
2.9.1.	All cameras shall be at minimum **2MP** (Megapixels) approved Avigilon HD range cameras, and shall be of Avigilon model or of other if approved by RMIT security & compatible with Avigilon. For a current listing of preselected models please refer to camera equipment table below
2.9.2.	Cameras shall be: • Of vandal proof design where tampering or malicious damage can occur. • Installed at a height that is safely accessible for maintenance purposes **(3m FFL)** • Not to be fixed to heritage buildings without appropriate Heritage approvals Heritage building requirements should be adhered to where applicable.
2.9.3.	CCTV Commissioning tests shall include: • Camera Image quality and area of view including focal point • Preview of recorded footage ensuring recording standards are meet • Recording equipment settings • Verification by RMIT Security

2.10 CCTV Camera Placement

Placement of all new CCTV cameras will be subject to the requirements of the project in consultation with RMIT Security Services. The purchase or installation of any CCTV camera must be authorised by the Associate Director Risk Reporting & Compliance or the delegate Manager Security Operations

Cameras must be located and selected according to the following:

Minimal Camera Requirement	
2.10.1.	**Internal cameras at building entrance**: Cameras shall monitor pedestrian traffic entering or departing through a building entrance. Recording angle must be set to view face/head of building entrants. Minimum requirement will be **2MP** Analytic camera for facial recognition or unless alternative model provided by RMIT
2.10.2.	**External cameras at building entry and exit points**: Cameras shall monitor pedestrian traffic entering or going past building entry points. Recording angle must be set to view face/head of building entrants. Minimum requirement will be **2MP** Analytic camera for facial recognition or unless alternative model provided by RMIT
2.10.3.	**Reception areas and premises where monetary transactions take place:** Cameras shall monitor activity at University reception areas and areas where monetary transactions take place and/or where there are interactions with members of the public. Image must be able to view person/s entering/leaving area of interest minimal **2MP**

2.10.4.	**<u>Areas of critical infrastructure or where livestock or dangerous chemicals are housed:</u>** Cameras shall monitor activity in areas containing animals, equipment, information technologies or communication networks which, if rendered inoperable for an extended period, would significantly impact on the functioning of the University.
2.10.5.	Areas containing objects of high value or desirability: Cameras shall monitor activity in areas containing objects of high value or desirability and include computer labs, specialist classrooms, teaching spaces or storage areas; cameras are predominantly used to monitor activity and provide evidentiary material in the event of theft.
2.10.6.	Designated safer walkways and zones: Cameras shall monitor traffic along designated safer walkways, and light corridors and heavy traffic routes; Multisensor 9MP or 12MP type cameras shall be considered. PTZ (Pan Tilt Zoom) Camera's may be used but only with agreement by RMIT
2.10.7.	Areas subject to petty theft, vandalism, or graffiti: Cameras shall monitor activity in areas where there is a history of criminal damage or where temporary installations may pose a risk; such areas may include library spaces and other student study areas, 24 hour computer labs and high profile buildings; CCTV must provide evidentiary material in the event of a theft or other criminal activity.
2.10.8.	Car park entrances and exits: Where applicable (please refer to RMIT Security Management team for recommendation), cameras shall capture vehicle number plates, facial identification of pedestrian traffic, remote monitoring of traffic flows (vehicle and pedestrian) and assist remote management of vehicle access. Where possible, Licence Plate Recognition (LPR) cameras shall be used. For LPR recording, the angle must be set to best view License plate. For Facial Identification purpose – Analytic cameras shall be used where necessary.
2.10.9.	Vehicle access points to the campus: Where applicable (please refer to Senior Security Manager for recommendation), cameras shall capture vehicle number plates, facial identification of pedestrian traffic, remote monitoring of traffic flows (vehicle and pedestrian), and assist remote management of vehicle access. Where possible, cameras of High Resolution (5MP minimum) shall be used or LPR cameras if requested by RMIT
2.10.10.	Other: Cameras shall monitor activity in areas of high pedestrian traffic and usage; such areas may include cafeterias, retail areas, public gathering spaces, lift lobbies and building foyers. 2MP or above dependent on required area of interest

2.11 CCTV Recording

All CCTV recording equipment shall meet the following below requirements

Requirement	
2.11.1.	The CCTV system shall have capability for fail over capacity to ensure that any failure of high and medium risk areas will failover and recording is maintained.
2.11.2.	Equipment is to have a storage capacity of 30 days minimum; new installs using existing equipment shall ensure the 30 day storage is retained.
2.11.3.	Recording shall be at a rate of 25fps (12fps minimum if authorized by RMIT Security).
2.11.4.	Cameras shall be set to record 24/7.
2.11.5.	Cameras shall be connected to **RMIT- ITS** network and must meet ITS cabling standards of KRONE CAT6A Cabling. Refer to ITS Cabling Standards
2.11.6.	Security contractor must ensure that all new CCTV installations have the appropriate camera and or software licenses required to capture onto RMIT's CCTV software platform.
2.11.7.	Cameras shall be set for Motion detection recording, allowing 10 seconds of pre-recording and 15 seconds of post recording.
2.11.8.	Camera shall be set for Alarm/Event recording, allowing 30 seconds of pre-recording and post recording.

Requirement for approved hardware supply

2.11.9. All NVRs are to be Avigilon branded and sourced via the official Australian distribution channel. Critical recorders must be selected from the following list in accordance with a validated Avigilon system design:

- **AVG-HD-NVR3-32TB**
- **AVG-HD-NVR3-48TB**
- **AVG-HD-NVR3-56TB**
- **AVG-HD-NVR3-84TB**

The above models come with Dell Pro Flex support (immediate 4hr dispatch, direct Tier 2 support) – only available via Avigilon.

For situations that do not require Pro Flex support, the following NVR models can be used:

- **AVG-H-NVR-2-21TB**

Avigilon appliance and edge NVRs may be used but must be have direct approval by RMIT for each individual case where these may apply.

Details of the service tag attached to each NVR must be supplied to RMIT staff as part of the commissioning and hand-over process.

2.11.10. Commissioning of Avigilon NVRs must include setup of the Gateway and must comply with RMIT Security and ITS specification.
Refer to ITS Spec's for networking requirements

2.11.11. Commissioning of Avigilon NVRs must also include setup of the ALL relevant **ENTERPRISE LICENCES** that must be included in ALL RMIT CCTV related project/s **Licences are either in 1, 4 or 8 channel preferences**

AVG-2C-H3A-D1	Avigilon 2MP HD Indoor Dome Camera, Analytics, WDR, D/N, H.264, 3-9mm, Light Catcher
AVG-2C-H3A-D1IR	Avigilon 2MP HD Indoor Dome Camera, IR, Analytics, WDR, D/N, H.264, 3-9mm, Light Catcher
AVG-2C-H3A-DO1	Avigilon 2MP HD Outdoor Dome Camera, Analytics, WDR, D/N, H.264, 3-9mm, Light Catcher
AVG-2C-H3A-DO1IR	Avigilon 2MP Outdoor IR Dome Camera, Analytics, WDR, D/N, 3-9mm, Light Catcher
AVG-2C-H3A-DP1	Avigilon 2MP HD Pendant Dome Camera, Analytics, WDR, D/N, H.264, 3-9mm, Light Catcher
AVG-2-H3-D1	Avigilon 2MP D/N Indoor Dome, H.264 (1080p), Zoom 3-9mm f/1.2 Auto focus P-iris lens
AVG-2-H3-D1-IR	Avigilon 2MP D/N IR Indoor Dome (1080p), H.264, Zoom 3-9mm f/1.2 Auto focus P-iris lens
AVG-2-H3-DO1	Avigilon 2MP D/N Outdoor Dome, H.264 (1080p), Zoom 3-9mm f/1.2 Auto focus P-iris lens
AVG-2-H3-DO1-IR	Avigilon 2MP D/N IR Outdoor Dome, H.264 (1080p), Zoom 3-9mm f/1.2 Auto focus P-iris lens
AVG-2-H3-DP1	Avigilon 2MP D/N Pendant Dome, H.264 (1080p), Zoom 3-9mm f/1.2 Auto focus P-iris lens
AVG-9W-H33MHDC1	Avigilon 9MP HD Multisensor Dome Camera, 3 x Image Sensors, In-Ceiling Mount, 2.8-8mmf/1.3
AVG-9W-H33MHDO1	Avigilon 9MP HD Multisensor Outdoor Dome Camera, 3 x Image Sensors, 2.8-8mmf/1.3
AVG-9W-H33MHDP1	Avigilon 9MP HD Multisensor Dome Camera, 3 x Image Sensors, Pendant Mount, 2.8-8mmf/1.3
AVG-3C-H4A-BO1IR	Avigilon 3MP Bullet Camera, WDR, Light Catcher, IR, Analytics, 3-9mm
AVG-3W-H3-BO1-IR	Avigilon 3MP IR Bullet Camera, H.264, Zoom, WDR, 3-9mm f/1.2 Auto focus P-iris lens
AVG-5L-H4A-BO1IR	Avigilon 5MP Bullet Camera, Light Catcher, IR, Analytics, 4.3-8mm
AVG-5L-H4A-BO2IR	Avigilon 5MP Bullet Camera, Light Catcher, IR, Analytics, 9-22mm
AVG-5-H3-BO1-IR	Avigilon 5MP IR Bullet Camera, H.264, Zoom, 3-9mm f/1.2 Auto focus P-iris lens

Avigilon - HD PTZ Cameras 2 Megapixel Cameras	
AVG-2W-H3PTZ-DC	Avigilon 2MP In-Ceiling Dome, H.264/MJPEG (1080p), WDR, D/N, 20x Zoom
AVG-2W-H3PTZ-DP	Avigilon 2MP D/N Pendant Dome, H.264 (1080p) WDR, PTZ, 20x Zoom

Avigilon - HD PTZ Cameras 1 Megapixel Cameras	
AVG-1W-H3PTZ-DC	Avigilon 1MP In-Ceiling Dome, H.264/MJPEG (720p), WDR PTZ, D/N, 20x Zoom
AVG-1W-H3PTZ-DP	Avigilon 1MP D/N Pendant Dome, H.264 (720p) WDR, PTZ, 20x Zoom

GREEN highlight indicates ANALYTIC STYLE CAMERA