RMIT UNIVERSITY

Property Services

Design Standards Brief

Section 12 – Electronic Security

Issue 6

2009

12 CONTENTS

12.1 INTRODUCTION

The building security concept shall be established during the early stages of a project and the Design Team, including representatives from the Security Office, Projects and relevant consultants, shall develop a complete security system design relevant to the project.

- security classification;
- integration with the University's preferred Campus Security Access Control Management System (SACMS);
- integration with the University's Campus Video Management System (CVMS);
- alarm response by security protective personnel;
- minimisation of nuisance alarms;
- provision of electronic access cards;
- security programming for the project;
- satisfy the BCA for certification by the Project's Building Surveyor and the Disability Discrimination Act 1992.

The appropriate classification of security for the intended usage of the building or area, based on a security risk assessment, is the basis of the design of the building security system.

Where major building renovations, or changes in the usage of a building from low security to a more significant level are intended, a security design with the new security classification shall be provided.

See also **Section 8** for the University's Emergency Warning Intercom Systems (EWIS) and for Fire Alarms, keying details, **Section 14** for University Lighting requirements.

The University has retained several consultants, as advisers on future installation of security systems to ensure compliance & compatibility.

The Project Architect shall consult with the Service Project Manager, the Manager, Security Branch, Information Technology Services in particular networks and the appropriate Consultants on overall integration, design, electrical interfacing and cabling standards with the University's Campus SACMS and CVMS.

The project architect is to obtain recommendations from the University appointed Consultant and final certification from RMIT Security Manager that the details design is in accordance with the designing brief, is compatible with and does not compromise the existing installation.

12.2 SECURITY DESIGN PHILOSOPHY

12.2.1 Usage

The building and internal area usage, especially the vehicular and pedestrian traffic patterns, together with the emergency exit route arrangement shall be established at the commencement of the security design process. Personal safety is paramount and provision for a safe internal and external environment is an essential consideration in the design process.

Security design and equipment selection shall ensure that there is freedom of movement for all authorised access traffic but without causing nuisance alarms leading to unnecessary response by campus security personnel. All equipment used for RMIT security purposes shall be purchased new and be of the highest quality and standard. Any other equipment that falls below this standard will not be considered for use by the University.

Early consideration by the Project Architect should be given to the building façade and security envelope elements (doors, windows, walls, and the like) to ensure needed security envelope integrity to satisfy security classification criteria.

As far as possible, emergency exit passageways and doorways shall not be shared with other uses so that defence-in-depth security principles and envelopes can be implemented.

12.2.2 Security Classification

The basis of classification of buildings, or areas within buildings, is the degree of damage which could be caused to the University through personal injury; loss of, or damage to property (including intellectual data); damage to public image and standing; or interruption of critical services.

12.2.2.1 Classification Criteria

The following is a general list of buildings, together with security classification categories, to establish the security classification of buildings:

Storerooms containing radioactive material or dangerous chemicals	VERY HIGH
Computer Stores (with high value equipment critical to business operations)	VERY HIGH
Areas of substantial intellectual or monetary value (eg. 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 Centres & Plant, Student Records Office and PABX rooms)	HIGH
Areas in which critical building functions (eg. ITS Router rooms, main plantrooms	HIGH
Animal houses	HIGH

Areas in which critical administrative functions are carried out (eg. 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

THE MANAGER, SECURITY BRANCH SHOULD BE CONSULTED DURING THE DESIGN PHASE TO CONFIRM THE PROJECT REQUIREMENTS.

12.2.3 Security Envelopes

The security design for a project shall adopt defence-in-depth principles in developing multiple physical envelopes for buildings and areas with high security classifications.

Primary protection shall depend on physical envelopes and physical barriers (eg. walls, doors, and windows) with appropriate resistance to physical attacks, such that multiple envelopes provide total attack time delays that match security personnel response times at each campus/building.

Concealed point-type detection are preferred, whilst line and volumetric movement detection shall be applied only where necessary. These shall not be used to reduce the resistance to physical attacks of barriers. Any and all installations of these are to be based on the classification criteria and risk assessment guidelines.

Electronic access control shall be applied at controlled portals through security envelopes, with entry/exit audits (with or without keying of PIN codes) and/or dual custody programming, for high and very high security areas within buildings.

12.2.4 Safety and Other Considerations

Security design should be cognizant of all safety and other considerations:

- after dark personal safety inside and outside buildings, carparks and building surrounds;
- communications and CCTV cameras for areas where distress conditions may occur, eg lifts;
- safety beams for vehicular gates and bi-parting doors;
- door furniture appropriate for use by disabled persons;
- long access time delays for disabled persons using electronic access control doors;
- emergency break-glass units where electronic access control is applied to exits from high security areas;
- automatic unlocking of emergency exit doors in the event of a fire alarm or building evacuation;
- re-entry requirements for locked fire stair doors on high rise buildings;
- fail-safe operations and battery backup for secure locking in the event of mains power failure.
- CCTV cameras for pedestrian audit at high security controlled portals, prevention of theft, assessment of duress alarm conditions, fire stairwell doors use for cross-over in high rise buildings.

12.2.5 Security Access Control Management System (SACMS)

The University has an extensive Campus-Wide Perimeter Security Access Control Management System, which is managed and supervised from the City Campus Security Control Centre by the Manager, Security, and his team of security personnel. The system monitors all building perimeter security, and electronically controls all after-hours access into buildings via electronic proximity cards.

24-hour security alarm and electronic access control monitoring/reporting may be made available to University Users upon request and authorization by the RMIT Security Manager or Security Services.

12.2.5.1 Overview and Architecture

The SACMS provides RMIT security management and personnel with:

- A security control centre in the City campus, that is capable of allowing the on-duty security staff to monitor and keep under surveillance the entire RMIT buildings' access and security for which they are responsible, with a minimum of effort and fatigue and with maximum efficiency;
- a central SACMS network that allows individual internal building security access control systems to be 'connected' as departmental sub-systems with full internal security management and administration by departmental key control officers from within the building, and full remote monitoring, audit trail recording and operational control from the central SACMS security control centre by the RMIT security manager and his team of security personnel at all times;
- a number of advanced security database querying, reporting and customisation facilities for the Security Manager and his personnel to rapidly, effectively and efficiently review and investigate security incidents, supervise response/patrol operations, and implement pre-programmed access control measures; and
- an advanced security-and-systems-access assignment management facility. This facility has a sophisticated permission and restriction system, allowing the Security Manager to administer the centralised SACMS and departmental sub-systems. The Security Manager will assign authorised personnel (including security personnel, departmental key control officers, some users with assigned security responsibilities) with individual security control and monitoring capabilities for their respective parts (i.e. areas down to a single door or intrusion detection device) of any building(s).

12.2.5.2 Architecture and Communication Protocols

The SACMS workgroup comprises a workgroup with multiple network/application servers, operator/administration workstations, SACMS standalone Ares Challengers (CH#), and 4-Door Controllers (4DC#), and Data Gathering Panels (DGP#).

The SACMS workgroup servers act as an integrated SACMS network and security access control application server, that can connect up to 79-82 (each) Challengers (based on the practical experience of several other Universities) via a combination of dialup modem, leased direct line, radio based Mobile Data network and Ethernet LAN connections to the University campuses in Victoria. Its software comprises an industry standard Networking Operating System (NOS) running on industry standard PC compatible hardware supporting a SACMS application operating systems (SACMS AOS).

The SACMS workgroup server and workstations (SACMS workgroup) operate their own standalone multi-tasking, multi-level priority interrupt NOS and Workstation Operating System) (WOS) on RJ45 Category 6 UTP Ethernet LAN or better, over the RMIT ITS LAN/WAN network.

12.2.6 Campus Video Management System (CVMS) Compatibility and Security Management Issues

The University has multiple Campus-Wide Video Management Systems (CVMS), which are managed and supervised from the City Campus Security Control Centre by the Manager, Security, and his team of security personnel.

These systems record (locally) and monitors the campus grounds and street, car parks, building perimeter after-hours entrances, internal corridors, security zone cross-overs and high security

rooms/areas using time schedules, video motion detection and security intrusion alarm interfaces.

Video screens are used to display views of critical security areas and high volume traffic (pedestrian and vehicular) of the campus/building entrances.

12.2.6.1 Overview and Architecture

The CVMS provides RMIT security management and personnel with:

- a security control centre in the City campus, that is capable of allowing the on-duty security staff to monitor all cameras and a majority of the RMIT campus, buildings and levels.
- a central CVMS network that allows monitoring of live views and access to video recordings of locally recorded network video recorders/servers (NVSs) via a dedicated CVMS VPN through the RMIT ITS LAN/WAN across the City, Bundoora and Brunswick campuses, from video workstations in the security control centre;
- distributed IP-based cameras (both integrated network cameras or analog-to-IP cameras) connected to local NVRs/NVSs, Syndec or better, for local standalone recording;
- for specific applications (eg RMIT Art Gallery) local video workstation is used to provide local live view camera surveillance and review;
- very strict control of access to video recordings are maintained by RMIT Security as part of the University CCTV policy and compliance with State laws.

12.3 APPLICATION TO BUILDING DESIGN & SERVICES CO-ORDINATION

The security classification shall be determined at the commencement stage in the design of a building and refurbishment areas, and if necessary through a security risk assessment.

Design principles relevant to security include:

- incorporation of disabled electronic access control facilities into the design (ie. to select the most suitable bi-parting electrically operated doors, door furniture, electronic card readers, long unlock times; heights of operating equipment; signage);
- passenger lift control functions;
- design of the shell of the building;
- design of internal User areas;
- design of multiple security envelopes;
- design of vehicular loading areas;
- security of accessible low-level windows etc.;
- combining all high-security functions to one area of a building but away from external walls of single storey buildings and floors over car park areas;
- unlocking of emergency exit doors in event of a fire alarm or evacuation;
- plant room and other service access without setting off nuisance alarms;
- selection and design of doors that require electronic access controls;
- design of fire- and smoke- doors which need to be held open and automatically closed on fire alarm or security lock-up after hours;
- courtesy reminders (eg buzzers) to users to close doors, especially fire doors;

- external lighting design.

12.3.1 Building Facade

While security design would not place restrictions on the overall schemes of a project, it shall be noted that uninterrupted external sides are more suitable for a building than sides with recesses, alcoves, or columns etc.

If gates and grilles are installed on the building perimeter, design should restrict openings to less than 150mm in high security buildings.

12.3.2 Building Access

In principle, all people entering and leaving a building or internal security envelopes shall pass through the same single access point through the security envelope.

Public access shall be limited to one door, unless traffic density, building disability and safety require overriding the principle of a single building entry.

Public shall have no access to roof levels and all trades personnel must undergo on site safety induction.

12.3.2.1 Electronic Security on Access Controlled and Monitored Doors

A) Type AEL - One-Side Access Controlled Door - Swing Doors (Electric Lockset)

These doors shall have the following existing hardware/features,

- ENTRY: Proximity card reader installed on the unsecured side of the door
- EGRESS: Free handle (preferred) within the lockset (or egress button) at the secured side of the door
- Electric mortise lock (normally fail-secure (locks on power loss) type, but where applicable fail-safe (unlocks on power loss) type on emergency exit door with exit sign on insecure side of a corridor door/ on high rise fire stairwell door for cross-over purposes as required under BCA)
- Lockset LED furniture plate indicating Access/Secure status of lockset
- Lockset reed switch door, inside free handle, key cylinder operation monitoring
- Local door alarm sounder (for 1st Stage DOTL alarm, silenced during building fire alarm) (also 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)
- Fixed-type hinges on doors which swing outward into the insecure side
- 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
- For very high security install “dog-bolts” into hinge-side edge of swing doors

B) Type A.ML - One-Side Access Controlled Door - Swing Doors (Magnetically Locked)

These doors 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
- Single Mag-lock (Where applicable on main entry or corridor doors with emergency exit sign, auto release on building fire alarm or operation of emergency break-glass unit(s) / on high rise fire stairwell door for cross-over purposes as required under BCA) (Where applicable, change to double mag lock on double swing door or additional single mag lock on fixed leaf of double 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) (also 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)
- PROJECT ARCHITECT - To specify and provide:
    - 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
    - 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

NOTE: Any Type A.EL and A.ML Access Controlled Door shall be pre-cabled with additional reader cabling (and emergency break-glass unit on the egress side) such that an additional Egress Proximity card reader can be installed without future cabling.

C) Type B.EL – Emergency Exit Controlled Door - Swing Doors (Electric Lockset)

These doors shall have the following hardware/features:

- ENTRY: No entry except via lockset keyswitch 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 LED furniture plate indicating Access/Secure status of lockset
- 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)
- PROJECT ARCHITECT - To specify and provide:
    - 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
    - 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 (non-fire corridor doors) to be of impact resistant type i.e. at least 6mm laminated glazing securely installed into the door body

D) Type A.ML – Emergency Exit Controlled Door - Swing Doors (Magnetically Locked)

These doors 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
- Single Mag lock (where applicable on fire stairwell or corridor doors with emergency exit sign, auto release on building fire alarm or operation of emergency break-glass unit(s) / on high rise fire stairwell door for cross-over purposes as required under BCA). Where applicable, change to double mag-lock on double swing doors or additional single mag-lock on fixed leaf of double 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 University approved Blocker Plate installed (where applicable on external perimeter and fire stairwell doors)
- PROJECT ARCHITECT - To specify and provide:
    - Where applicable, lockable deadbolt on fixed leaf on double swing doors
    - Where applicable fixed-type hinges on doors which swing outward into the insecure side
    - Door head and frame to be sufficient width and strength to accept mag-lock to 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

NOTE: Any Type B.EL and B.ML Access Controlled Door shall be pre-cabled for future additional card reader and electric lockset cabling.

NOTE: All Type A and Type B Controlled doors shall be controlled by GE (GE Security) Intelligent 4-door controllers.

E) Type C – 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 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;

NOTE: RMIT security division is continually upgrading the standard of technology used and is currently considering innovation such as Hio-lock technology.

12.3.3 Physical Barriers & Doors

Physical barriers, including walls and doors, designed to form security envelopes shall be of sufficient resistance to physical attacks, such resistance being appropriate for the category of security classification for the protection of the person and assets within.

Within false ceilings, physical barriers with mesh sizes no more than 150mm shall be constructed to resist physical attacks, if the security classification warrants it.

12.3.3.1 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. Frameless glazed doors and doors with short backset shall be avoided.

While security design would not place restrictions on the overall design of door and other access portals, it shall be noted that more detailed design are required when security envelope doors are also fire and/or emergency exit doors and may involve electronic access controls.

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. (Refer **Clause 2.12.3** for locking details.)

Doors with 180 degree swings shall be avoided.

Preference should be given to designing outward swing doors, which are more resistant to physical attack, provided hinges are of the fixed type, and high security protected, backed up by dog bolts on the hinge side.

Use of appropriate security and safety signage is preferred over active devices to obstruct non-emergency egress through emergency exit doors. The Manager, Security, shall be consulted when active devices are designed.

Perimeter doors shall be designed to be more resistant to physical attacks, eg no external furniture; stainless construction and metal strips/blocker plates to resist manipulation of the lockset deadbolts.

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.

Manual lock-up of doors by University security personnel **shall be avoided**.

Where possible, electrically operated locksets with free inside handles shall be preferred, and electric strikes avoided.

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

12.3.3.2 Electro-Mechanical Doors

Whenever electro-mechanical operated bi-parting doors are considered, the Design Team shall also consider emergency exit requirements by designing outward opening swing doors near the bi-parting doors.

The Manager, Engineering and Maintenance and Manager Security Branch shall be consulted on the selection and installation of an electro-mechanical operated bi-parting door.

12.3.3.3 Security Installation

With the more extensive use of electronic access control in security applications, security design should allocate adequate space for location of security panels, major trunk cabling in vertical risers and horizontal duct-ways or cable-trays. Cable access to doors and other intrusion detection points shall be concealed in walls and door frames, with appropriate block-outs provided in the construction of door frames and doors.

Early consideration shall be given to the provision of a single electrical sub-circuit for security panels and other security equipment. Location of security panels will be in accordance with criteria as specified by RMIT Security division in particular the height, space and expansion of the panel.

12.3.4 High Security Areas/Rooms

High security rooms with high value/critical equipment and information/archives shall be provided with:

- Type A.EL access controlled door with fail-secure lockset;
- Where applicable an egress card reader to provide full audit trails;
- Emergency break-glass door release unit on egress side of door;
- An additional single mag-lock (where applicable auto release on building fire alarm or operation of emergency break-glass unit). Where applicable, change to double mag-lock on double swing door or additional single mag-lock on fixed leaf of double door;
- Integral mag -ock LED indicators showing Lock/unlock status of mag-lock;
- Integral mag-lock bond sense monitoring. Lock bonding when lock is powered;

- Door head and frame to be sufficient width and strength to accept mag-lock to prevent buckling when Z-brackets need to installed
- PIRs installed inside the room
- Room alarm sounder installed inside the room
- Access/Secure indicator panel next to card reader
- Blue flashing light box on outside of door
- OPERATION:
- **Normal** operation using Type A.EL functions with mag lock in access mode, PIRs disarmed, room sounder silenced.
- **After hours** operation with mag lock in secure mode, PIRs armed, room sounder activate on any alarm detection in the room. Triple badge on the entry card reader to arm/disarm room intrusion detection devices (PIRs).

12.3.5 Plantrooms

Where possible, access to plant rooms shall be by request via security office, so that service personnel do not need to enter a secured area to access the plant room, eg. external door away from the main building for plant rooms on ground levels; or separate direct access for plant rooms on building roof levels.

Critical plant rooms in high security buildings or plant rooms requiring frequent service visits shall be electronic access controlled.

12.3.6 External Lighting

The main external entrance to a building shall be well lit after dark. External lighting shall be controlled by a photo electric cell not by a time clock. The location or placement of lighting fittings is critical, where it is intended that CCTV cameras are installed, in particular with use for low-light cameras. Lighting for CCTV day/night cameras is preferred given their self-adjusting features to the surrounding light exposure.

The security lighting from the building shall extend to the appropriate Campus Security Light Corridor. (Refer to the Services Project Manager and Manager Engineering & Maintenance and Manager Security Branch for details).

Perimeter doors and other ground level points of potential access and egress shall be well illuminated by security lighting after dark.

12.4 SECURITY & ACCESS CONTROL – PRINCIPLES APPLICABLE

12.4.1 Building Perimeter

Buildings shall have at least one electronic security access control system, which shall provide intrusion alarm monitoring and electronic access control of all building perimeter doors, gates and openings. The equipment for this system shall be the GE Challenger series system comprising: Challenger Panel, 4-door Controllers, Data Gathering Panels, Lift Controllers, etc., complete with Ethernet interface to the University Ethernet Communications Network, managed and operated by the University. Connection ports into the University Ethernet Communications Network shall be carried out by the University and co-ordinated through the Manager, Security Branch and other approved consultants.

12.4.2 Internal Area Security

If spare capacity in the Challenger Panel permits with the approval of the Manager, Security, the building Challenger system may be extended to provide intrusion alarm monitoring and electronic access control of internal building areas, otherwise additional Challenger Panels shall be allowed by the Project Design Team.

Non-Challenger Panels may be used for internal areas provided such panels are proven to be fully compatible with the ARES headend protocols and applications via the Ethernet communications backbone. Non-Challenger Panels may also be used for internal areas if there are intentions for connection and 24-hour alarm monitoring and response by the main control room and University security personnel.

12.5 ELECTRONIC SECURITY & ACCESS CONTROL SYSTEMS SPECIFICATIONS

12.5.1 Installation

In general, electronic security shall be installed by a specialist Security Contractor. The Security Contractor shall tender direct to the University, and be nominated as a specialist subcontractor to the Main Contractor.

Installation work, cabling, testing, commissioning, handover, record keeping and practice shall conform at a minimum with the latest editions of the:

- Building Code of Australia;
- Applicable Australian standards, including AS 2201 (Security) and AS4806 (CCTV);
- RMIT University Design Brief - Electrical Services section
- RMIT University Design Brief - Communications section.

12.5.2 Security Cupboards and Risers

At least one separate security cupboard shall be provided for each building; others shall be provided according to the security equipment required for the building.

The security cupboard(s) shall be located at central locations, preferably right beside the ITS communications room or cupboards and shall be accessible to authorized staff only via a security ADS key.

A typical cupboard shall be not less than 2000mmH x 1800mmW x 250mmD in size and accommodate security and CCTV wall cabinets. Larger cupboards shall be 2000mmW and 2400mmW for accommodating larger quantities of equipment. The cupboard is to have sufficient natural air ventilation via dust proof mesh vents near the top and sides of the cupboard. The cupboards general illumination level shall be 400 lux and it shall be equipped with *additional* emergency light fittings and door locks to be keyed for a “ADS” key.

The consultant shall make a recommendation regarding the installation of smoke detectors in lieu of thermal detectors, before final approval is granted by the RMIT Security Manager.

Dedicated catenaries, pvc/galvanized conduits, cable trays shall radiate out from the security cupboard(s) to access all sections of the building to allow for future additions. Catenaries and conduits shall be sized according to security industry standards. If cable trays, the width of the cable trays shall be agreed on consultation with the Manager, Security, in any case, shall not be less than 150mm.

The consultant shall recommend the installation of suitable 8-hour battery backup 12vdc Power Supply Units (12vdcPSUs) to protect critical a) security equipment and devices to maintain full

security monitoring and access control operations; b) CCTV equipment, cameras and controller to maintain full camera, video recording operations and network data communications. The RMIT Security manager will approve the recommendation before proceeding.

Other required security cupboards of adequate size shall be provided on each floor level, together with dedicated cable riser ducts extending continuously to the full height of the building.

The riser and cupboard shall be dedicated to security cabling and security equipment only.

Cable trays for telephone and data networks shall be provided in each communications riser and sized for 30 percent expansion.

Eight 20A (SPA) double GPOs shall be provided in each security cupboard together with a locally switched fluorescent light fitting. Each double GPOs shall be supplied from a dedicated circuit. Additional GPOs may be required depending on security and CCTV equipment power requirements.

Where space is restricted the minimum width of the cupboard shall be 1000mm and the minimum depth 300mm – without compromising on appropriate ventilation requirements (see cabinet arrangement drawings attached) to accommodate Ares security and CVMS CCTV cabinets.

Number and size of security cupboards will depend on the security architectural design for the building.

Each riser cupboard shall be located in a secure section of the building and shall be accessible to authorised staff only.

Security cupboard(s) would typically consist of the following equipment:

- Ares Challenger (CH#) wall cabinet 350mm(H) x 455mm(W) x 75mm(D);
- Ares 4-Door Controller (4DC#) wall cabinet 395mm(H) x 590mm(W) x 80mm(D);
- Ares Data Gathering Panel (DGP#) wall cabinet 350mm(H) x 455mm(W) x 75mm(D);
- Ares Power Supply-cum-Battery Units (SPSUB#) wall cabinet 230mm(H) x 240mm(W) x 90mm(D);
- and/or
- CVMS CCTV Network Video/recorder Server (NVS) 300mm(H) x 460mm(W) x 150mm(D);
- CVMS CCTV Power Supply 12VDC 10Amp 8-Hour Battery-Backed Unit (CPSU-10/53) 300mm(H) x 460mm(W) x 150mm(D);

Each security cupboard(s) shall have floors and walls sealed with either appropriate paint and/or vinyl only.

Upon completion, and prior to hand over to the university, the security cupboard and security/CCTV equipment cabinets are to be fully cleaned and free from construction dust and debris associated with installation.

Security alarm conditions shall be raised for cabinet tampers, normal mains power failure, battery low/absent condition. The 3 monitored conditions may be series connected in each security cupboard

12.5.3 Minimum Performance Standards

Whilst the following performance criteria may apply in most applications, security design and implementation for each project may require higher standards or additional functions.

12.5.3.1 Battery Backup

Security, including CCTV and communication, panels shall be fully supported by battery backup for a minimum period of 8 hours for all security detection, access control, CCTV and communication functions, should normal mains power fail.

Motorised bi-parting main entry doors shall be fully supported by battery backup for a minimum period of 8 hours, should normal mains power fail to the doors.

12.5.3.2 Anti-Tamper

Critical devices, detectors, cameras (in high risk areas), signal processors/analysers, communication units, junction boxes, security/CCTV cabinets, riser cupboards and external pits shall be tamper resistant and/or fitted with tamper detection devices.

12.5.3.3 Cabinet Locksets

All mechanical locksets installed in equipment cabinets, panels, etc. shall be of the high security type, capable of taking security ADS cylinders obtained from the University Locksmith.

12.5.3.4 Security Intrusion Detection and Alarm

All detection circuitry shall use end-of-line supervision and provide 4-state monitoring with change of state detection when line conditions change by 25 per cent or 15 per cent for special risks.

Alarm contacts shall be of the magnetic reed type installed concealed within the door frame and operating via a concealed magnet recessed into the door. Due allowance shall be made for alarm contacts installed in steel frames. Heavy duty glass sealed reed switches of the biased security type shall be fitted to all roller shutters, fold up doors and any other heavy duty gates and doors. The Project Architect is to address the specialist fixings required on fire doors. Where the width of a vertical opening shutter exceeds three (3) metres, reed switches shall be fitted on both sides.

Line and Volumetric Movement Detectors shall be selected for their appropriateness to the specific detection requirement. They shall be tamper resistant and have sensitivity adjustments, high immunity to EMI and RFI, and fitted where applicable with a test indicator, which shall be disconnected during normal operation. For some types of detectors, particular attention shall be paid to eliminating the risk of false alarms from the effects of late afternoon or early morning sunlight, passing vehicle lights and/or operation of security flood-lights.

Duress and Hold-Up Actuators shall be push-to-activate type, self-latching and key-only-resettable, with the activating button sufficiently recessed within their housing to minimise accidental activation.

Local Audible Alarms shall be of pulsing sonalert or buzzer type, with volume level adjustment and mounted on a standard electrical mounting plate.

Door Detection and Processing Circuitry shall allow ‘Door Forced Open’ (in secure mode) and 2-stage ‘Door Open Too Long’ (DOTL) processing (in access or electronic control mode), so that on detection of 1st stage DOTL a local courtesy audible shall be activated to request Users to close the door, and on detection of 2nd stage DOTL an alarm shall be raised at the University security control centre. The local courtesy audible shall be silenced when there is a building fire alarm or during the 2nd stage DOTL alarm condition.

12.5.3.5 Electronic Security Access Control Systems

A GE Ares Challenger system for intruder detection and small building access control is currently installed in University Buildings.

Electronic proximity access cards are available from the Manager, Security in accordance with University policy. Quantities of access cards shall be determined as early as possible in the design process and notified to the Manager, Security.

12.5.3.6 After Hours Alarm Notification

Alarms shall simultaneously communicate direct to the University main control centre; alarm locally at each door; and to multiple local Ares RAS control panels.

12.5.3.7 Electric Mortise Locksets

Electric locksets shall be the "Power-On-to-Lock" in most cases, actively monitored for positive deadlatch operation, tamper resistant, fitted with tamper detection devices, adequately rated for continuous operation, fitted with heat dissipation plates where installed in timber doors, have bi-colour LED for lock status monitoring, and monitored separately for operation of inside handle and outside cylinder. The bi-colour LED is integrated into the lock escutcheon plate furniture on the entry side(s).

The electric mortise lockset manufacturer, Lockwood, sets a minimum door frame width of 130mm for accepting the locksets.

Fixings shall be stainless steel and appropriate for high usage, vibration and impact situations.

Cabling between door frame and door leaf shall be via Abloy 8810 lead covers (or equivalent) with fire resistant sleeving for the cables in the transfer spring.

12.5.3.8 Electromagnetic Locks

Electromagnetic locks shall provide a minimum holding force of 1300 pounds, and 1500 pounds in high security areas. They shall be of efficient power consumption, robustly constructed, fully concealable, tamper resistant. Their mounting design shall ensure automatic compensation for normal door wear, sag, warpage and misalignment. These locks shall be fail safe in operation without residual magnetism, and equipped with inbuilt visible lock status indicator and anti-tamper switch for separate remote monitoring.

12.5.3.9 Motorised Doors

The door actuator shall provide:

- the ability to physically monitor the doors when open;
- the ability to physically monitor the doors when 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 a 8-hour UPS for maintaining secure operations when the mains power fails; after which the door shall be unlocked and openable by hand.

12.5.4 Security & CCTV Equipment (Hardware)

The following security hardware and equipment are conditionally University-approved. They may not be suitable for all applications and therefore should be applied with due care.

Where no University-approved hardware is listed herein or considered to be unsuitable for application in a particular project, the consultant shall propose additional, equivalent, better or newer hardware for approval by the University, particularly the maintainers of the security systems.

12.5.4.1 Door Strikes, Electric Locksets, and Magnetic Locks

Electric mortise dead latches shall be specified from the University-approved range of equipment;

Magnetic locks shall be from the University-approved range of equipment.

12.5.4.2 Electro-Mechanical Door Actuator

Door actuators shall be specified from the University-approved range..

12.5.4.3 Proximity Card Reader

Where required the Consultant may provide a recommendation for a range of equipment for approval by the RMIT Security Manager.

12.5.4.4 External Key Override Switch

Where key override switches are required the Consultant may provide a recommendation for a range of equipment, which shall be approved by the University Locksmith.

12.5.4.5 Request-To-Exit Push Button

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.6 Duress Hold-Up Button

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.7 Door Reed Switches

Reed switches shall be specified for all doors associated with the security installation. Reed switches may be recommended from the University approved range.

12.5.4.8 Emergency Breakglass Units

Where required the Consultant provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.9 Passive Infrared Detectors

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.10 Ceiling surface mounted 360 deg PIR

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.11 Wall surface mounted curtain PIR

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.12 CVMS Fixed View Colour Network Camera

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.13 CVMS 10xOptical Zoom Pan-Tilt-Zoom Colour Network Camera

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.14 CVMS 26xOptical Zoom Pan-Tilt-Zoom Colour Network Camera

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.15 CVMS Colour Network Encoder/Server

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.16 CVMS Network Video Server/Recorder (NVS)

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.4.17 CVMS Network Switch

Where required the Consultant may provide a recommendation for a range of equipment which shall then be approved by the University.

12.5.5 Security Notes on Unshielded Twisted Pair (UTP) Data Cabling

12.5.5.1 UTP Cable Installations

All UTP cables shall be in accordance with the standards setout in the **RMIT Design Brief – Communications Section 10** except that:

For security integrity, the RMIT ITS Ares LAN data port shall terminate into a Telecommunication Outlet inside the Ares Challenger panel;

For security integrity, the two(2) RMIT ITS CVMS CCTV LAN data ports shall terminate into two(2) Telecommunication Outlets inside the CVMS NVS cabinet;

For security integrity, all other UTP cables for CVMS CCTV equipment shall terminate directly into the RJ45 connectors in the network cameras, video encoders/decoders, NVS (ie network switches, computers, and the like), workstations, LCD screen, and the like.

The following sections in the RMIT Design Brief – Communications sections are to strictly adhered:

Performance requirements, in particular the documentary evidence;

UTP distance manual;

Commissioning test results;

Cable labeling;

Testing;

As-Installed drawings and manuals;

Certification and guarantee.

12.6 OPERATIONS & MAINTENANCE MANUALS

Detailed instructions shall be included in the tender specifications for the preparation and supply of RMIT Operation and RMIT Maintenance Manuals.