SECTION 15

BUILDING SECURITY

Table of Contents

Version	Date	Authors	Summary of Changes
P1	16/05/14	WA	Preliminary Issue for Review
2	19/8/14		Issue to web

15.0 BUILDING SECURITY

15.1 General

Security Design Philosophy
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.

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.

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

- after dark personal safety inside and outside buildings, car parks and building surrounds;
- communications and CCTV cameras for areas where distress conditions may occur, e.g. 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.

Intrusion and Duress Alarm System
Provide intrusion and duress alarm system with compatibility and capacity for future connection to the Electronic Access Control system. The system shall include perimeter and space protection. The system and detectors are to be specified by the Security Manager JCU (telephone 4781 4363).

Laminated security services plans indicating locations of all detectors, alarms, control panel, etc. in relation to the floor plan shall be mounted on the wall adjacent to the control panel. Specifications for proposed system and detectors should be submitted to the Security Manager JCU.

This design standard outlines the security considerations which are applicable to the design stage of a building. It has been prepared on the understanding that the University will be the sole occupant of the building. If a commercial shared tenancy is contemplated then additional advice should be sought from the Security Section. The philosophy behind these recommendations is:

- To combine like areas in function to the one area or cell-like areas. This allows for easier methods of securing areas and enhances the "need-to-know" principle of security. In areas such as laboratories, the economics of concentrated locations support security considerations.
- To enable the efficient upgrading of the security of the building or the individual cells within the building.

15.2 Peripheral Security

External Area

The external area should have the public access area well lit for the dark hours. There should be some form of delineation between the public area of the building exterior and the private area, whatever that may be. This can be in the form of well placed shrubbery or change of paving, employing the principles of CPTED .The delineation need be indicative only and may take the form of a sign rather than for example a formal impediment. Perimeter doors and other ground level points of potential access should be illuminated for safety and security purposes during the hours of darkness.

Basement and Visitor Parking

If basement parking is to be allowed, then this should occur in such a manner as to preclude people or goods from entering the remainder of the building without passing the reception point or main access foyer. Access to the basement should be to authorised vehicles only. Basement parking should be controlled and a boom gate should be included in this design. How protected this is will be dependent on the risk posed by the use of the building. Visitor parking, if it is to be provided, should be external to the building and should not be immediately adjacent to or within the building fabric.

Plant Rooms

Plant rooms should be located and designed in such a way as to be secure stand-alone entities. These rooms should be located in such positions that workers need not enter any secure area to access plant rooms. This could require the plant rooms to be located on the perimeter of the building. Internal walls should extend slab to slab and grilles should be provided over any ducting which penetrates the floor, walls or ceiling. Plant rooms should be designed without windows. Doors should be solid core and locked in accordance with Doors, Hardware and Locks Section and fitted with blocked plates over the lock and striker plate.

Air Handling - Unless a very good argument to the contrary exists, air intake should be high up on the building. The exhausts can be at ground level if required.

15.3 Perimeter Security

Main Entry Doors

To secure the building after hours, all perimeter openings should be locked. Where electronic access control is in use, the system will be programmed to secure these doors on a basis of a time schedule

provided by the occupants. All new buildings will include at least one electronically accessed controlled door and all perimeter doors will be electronically monitored by reed switch. In existing buildings where electronic access control systems are not utilised, the main entry doors should be secured with a Mortice dead latching lock.

Emergency Exits
Emergency exists forming part of the perimeter of the building should have the following characteristics:

- Single leaf solid core door, hung to open out
- Fitted with approved hinge bolts
- If connected to the access control system to allow monitoring of doors then the electric locks should be wired into the building fire panel to allow fail safe operation of the doors in a fire alarm situation.
- Fitted with a door-closing mechanism
- No furniture should exist exterior to the door except a blocker plate.

If the building is classified as very high security the matter should be referred to the Security Manager for a specific design brief.

Perimeter Doors
External perimeter doors should have the following characteristics:

- Hang to open out.
- Fitted with fixed pin hinges.
- Fire escape doors, and plant room doors must be fitted with blocker plates,
- Glass (where used in doors) should be approved impact resistant glass, refer to section 11.11 below.
- Except for plant rooms all other external doors must be connected to the access control system to allow either electronic card swipe operation or the electronic monitoring of door security status via reed switch.
- All electronically controlled perimeter doors must be capable of being manually locked and remaining secure in the event of a power outage lasting several days. Electromagnetic locks are not to be used in perimeter doors under any circumstances.

Reception Areas
Depending upon the client assessed risk, the building for high security areas, if the assessed risk is sufficiently high, a reception area should be incorporated. Reception areas within the building should be protected by a counter wide enough and or high enough to inhibit direct physical contact.

Reception areas should face the public area and should form a part of the working hours perimeter of the secure area. Access from the public area to the secured working area should be through doors controlled from the reception area and/or by an electronic access system. The working hours perimeter walls and partitions shall be constructed to exclude the public from the secure working area, should extend slab to slab.

Provided it incorporates a high level of protective measured equivalent to those of the internal data rooms the reception area can house the local control panels for any intrusion alarm system if they are inside the protected area, as well as overnight key storage facilities.

Loading Dock Access Openings
Loading dock vehicular areas should be secured by roller shutter doors locked both sides at the bottom in after hour situations. Access from the basement to the reception area need not be secured but should funnel people into the public areas so that the receptionist has control of entry to the working area.

Stores Delivery and Dispatch
Delivery vans and trucks should not be permitted inside the building. The loading bay must, therefore, be provided off one of the peripheral walls. This bay should have external access to a truck standing area via a steel roller shutter or panel lift door, and internal access to the stores area via a second steel door of similar construction or of solid core timber.

The double door feature should provide an airlock for the unloading of goods. Unloading of goods should be supervised by an authorised member of staff. A single door should be provided for access into the airlock from the building interior. This door must be treated for security purposes as a perimeter door.

If a stores holding area is required in the delivery and dispatch area then either a separate storeroom should be designed in a fashion similar to that outlined earlier in "Plant Rooms", or a compound should be constructed in accordance with the design outlined in relation to "Sensitive Waste".

15.4 Offices

Public Area
Offices and facilities which the public are likely to frequent should preferably be grouped near the reception area. This is to keep public movement through the building to a minimum.

General Offices
Offices selected by management on the basis that high security is required for those offices should utilise slab to slab partitioning, solid core doors and hinge bolts. Consideration should also be given to the electronic detection of intrusion into these offices.

High Security Spaces
Where possible, high security spaces or facilities should be grouped or clustered and consideration should be given to the use of electronic access controlled doors into either the group area, individual offices, or both. This section applies to offices for Head of School and above, secure laboratories, specialist spaces and the like.

15.5 Functional Areas

As far as possible, valuable or operationally important equipment should not be located in rooms which are easily accessible from the street or from parts of the building which have general public access.

Cash Handling Area
Cash transactions should be kept to a minimum amount necessary and should be held, counted and transferred away from public view. If cash is to be held on the premises, the following recommendations should apply.

- The floor should be designed for loading of whichever commercial money safe is selected.
- Entry into the money area should be strictly supervised and should be through a two-door interlock portal.

- If money is being paid out then secure enclosures can be incorporated into the design. This should include a counter and screen incorporating laminated impact resistant glazing and a stainless steel cash draw.
- The counter front and top should be solid and homogeneous in strength to the glazing. In addition, an electronic hold up alarm and CCTV camera should be installed and any signage about this area should indicate it as a financial services area and not refer to the words cash or cashier

In all cases where a cash-handling facility is being located in a building, the Security Manager should be consulted concerning detailed security design.

Exam / Confidential Records Storage

The perimeter of the storage room should extend slab to slab. Entry to and from the storage area should be through a single point fitted with a solid core door that is electronically access controlled. A monitored electronic intrusion alarm system should also be installed. Windows should be secured.

PABX Room

The PABX area should be in a dedicated room with a single entry point. Where possible, PABX rooms should be of slab-to-slab concrete construction. Doors should be solid core and fitted with hinge bolts, and any inactive leaf should be secured at top and bottom with "Dalco, model 1801, 450mm" skeleton bolts and floor plates, or equivalent. Consideration should be given to the use of electronic access control systems for all PABX rooms.

Telecommunications MDF's or IDF's should be located and designed in a fashion similar to that outlined earlier in "Plant Rooms" section above

15.6 Fire Escape Stairs

Unless it is absolutely unavoidable, fire escape stairs should not be the principal inter-floor access stairs within a building. If it is intended that fire stairs be available for use by staff as inter-floor access, then the fire doors should be operable from both sides, but should be capable of being locked against entry to the floors from inside the stair well, while always giving free egress from the building. Access from the car park areas to the external fire escape doors should be direct and unhindered. It must not, however, be possible to gain access from the basement to the building interior by the fire escape stairs. Entry into the building interior from these stairs should therefore be protected by a fire door with furniture only on the secure stair side and this door must be fitted with a door closer. Egress should be in accordance with the NCC

Waste Compound - If required, the waste compound should be constructed from slab to slab partitioning or lightweight masonry. A solid core door should be incorporated in the design.

15.7 Recommended Laminated Impact Resistant Glass

Only a guide and glazing specification should consider security aspects in very limited instances.

15.8 Grilles and Mesh Screens

Depending on application Crimsafe – window mesh screens or equivalents may be considered for use on advice of the Security Manager:

Refer Crimsafe web site for local supplier details: http://www.crimsafe.com.au/

Should Grilles be required they must be constructed to the following detail:

12mm diameter bright steel bars spaced at not more than 120mm centres. Cross bar is to be 50mm by 6mm spaced at not more than 400mm centres. Grilles should be fitted inside the windows and secured by masonry anchors or similar, to which the mesh should be spot welded.

15.9 Electronic Access Control System

All external doors used for after hours access, telecommunications rooms, particular amenities (e.g. kitchenette adjacent to conference room), computer labs, and 24 hour access rooms identified in room data shall be card accessed (using staff/student identification cards). James Cook University utilises **DSX Access Control Systems**. The preferred card reader is the Dorado Magnetic Stripe reader. Other readers may be specified in special circumstances. Common Rooms (Lecture, Tutorial, Conference and Meeting) shall have the provision for future connection to Electronic Access Control System.

Cabling
All exposed cabling is to be run inside tubular conduit unless specifically approved in writing by the Security Manager. All data communications cabling within the ceiling space is to be installed in conduit and fastened securely. All cables to be shielded earthed and clearly marked to the Security Manager's approval.

Equipment Install Heights
Top of user accessible items to be no higher that 1300mm and no lower than 1000mm.

15.10 CCTV Standards

CCTV cameras are to be installed as determined by a needs / use analysis. This will be completed as a consultative process with the Security Manager JCU and stakeholders. All cameras are to be wired to a secure location and connected to a DVR, approved by the Security Manager JCU to permit local recording and remote monitoring. The approved DVR for JCU is the iWatch DVR. Contact JCU Security Manager to determine minimum storage requirements.

IP Addressable cameras are not to be used without prior approval Security Manager JCU

Cameras shall be configured to operate on a 24 hour basis under varying light levels and environmental conditions and shall be identified through the use of a text generator to provide identification which is displayed with the recorded view from the camera.

PTZ cameras shall be capable of 360° continuous rotation Tilt rotation shall be 90° down and 60° up from the horizontal. The pan tilt mechanism shall have minimum pan speed of 7°/sec and tilt speed of 2.5°/sec.

Locations
Camera locations are individually determined based on factors including required field of view, ease of access for maintenance and difficulty of access for vandal attack purposes. In centrally funded projects camera locations will be as determined by the Security Manager following a risk assessment process.

CCTV Recorder Programming
Digital Video Recorder (DVR) Programming

Each DVR is to continuously record images to its hard drive and is required to store 14 days worth of images from 16 cameras, each recording at a minimum of 2 frames per second. They shall be

installed so as to facilitate playback of recorded images without interruption to the recording operations.

Recorded video shall be stored for a minimum of 14 days.

Long Term Image Storage
Images from each DVR are to be capable of being saved and transferred to others by means of keyboard control, for archive or for police evidentiary purposes. Still images from each DVR are to be capable of being printed on a photographic or standard colour printer.

Control Equipment

The Control Equipment hardware and software is to be approved by JCU.

Monitors
To be flat, high quality display screens.

15.11 Asset Tracking System Standard

Philosophy
High value, portable assets may be protected at JCU within designated areas through the employment of the approved asset tracking system. The University Security Manager will determine the risk and need for installation of this system within centrally funded projects. For school or faculty funded refurbishments, the head of the organisational area will determine the risk and need.