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
	05/05/15	Manager, Infrastructure Services	Updated with JCU Manager Security comments and cross referenced with other sections
V3	17/07/18	Manager, Infrastructure Services	2018 general review update
V4	21/03/22	Manager, Security TSDIS	2022 general review update

15.0 BUILDING SECURITY

This document is a section of the James Cook University (JCU) Design Guidelines and is not to be read in isolation. Consultants and Contractors are required to comply with all sections of the JCU Design Guidelines.

15.1 Approvals Required during Design

Approval shall be obtained from the Deputy Director – Planning and Development in Estate Directorate for:

- The building and internal area usage, especially the vehicular and pedestrian traffic patterns, together with the emergency exit route arrangement,
- Emergency exit requirements is the building is classified as having elevated security requirements,
- Loading Dock Access Openings with roller shutter doors,
- Any cash handling area(s),
- The proposed use of Laminated Impact Resistant Glass,
- The proposed use of Crimsafe, or proven equivalent mesh screens,
- The proposed use of exposed cabling with sample/colour specification sheet,
- The proposed high value, portable asset tracking system.

Approval shall be obtained from the Manager, Security in Estate Directorate for:

- The proposed intrusion and duress alarm system, including perimeter and space protection,
- Any tenancy requirements,
- External perimeter doors requirements when the building is classified as very high security,
- All Security Cameras (Internal and External) quanta and locations, usage of, camera views, installation location.
- Physical mounting infrastructure for security devices

Approval shall be obtained from the Head, Digital Infrastructure Solutions in Technology Solutions for:

- Variation from JCU Design Guidelines Section 26 Communications
- Variation JCU Tendered standing offers for Security Devices (Security Cameras, Door access hardware, etc)

15.2 General

The building security concept shall be established during the briefing 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 and include this in the briefing documentation.

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 SD process and signed off by the Deputy Director – Planning and Development. 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 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.

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.

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

- after dark personal safety inside and outside buildings, car parks and building surrounds;
- communications and security 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 multiple storey buildings;
- fail-safe operations, connection to essential power and battery backup for secure locking in the event of mains power failure
- Security cameras layout shall consider the surrounding buildings, access way, path and roads to ensure it fully integrates with the existing
- Security 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 multiple storey buildings.

15.3 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 actual project requirements and detectors used are to be determined at an SD stage in consultation with – and approved by - the JCU Manager, Security.

The system and detectors are to be compatible with and able to interface to the current latest site-wide access control system.

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.

This design standard outlines the security considerations which are applicable to the design stage of a building on the understanding that JCU will be the sole occupant of the building.

If a commercial shared tenancy is contemplated then additional advice should be sought from the JCU Manager, Security. 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.

15.4 Peripheral Security

15.4.1 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 as noted in Section 6 of these design guidelines. 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 as references in Section 14 and 25 of these design guidelines.

15.4.2 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 is to be external to the building and should not be immediately adjacent to or within the building fabric.

15.4.3 Plant Rooms

Plant rooms design requirements are detailed in the Section 30 and the engineering sections of these design guidelines.

15.5 Perimeter Security

15.5.1 Main Entry Doors

To secure the building after hours, all perimeter openings should be locked as per the requirements of Section 14.

15.5.2 Emergency Exits

If the building is classified as having elevated security requirements, the matter should be referred to the Deputy Director Planning & Development for a specific design brief in the early briefing stages of the project.

15.5.3 Perimeter Doors

External perimeter doors should comply with the requirements in Section 14 of these design guidelines unless the building is classified as very high security when the JCU Manager, Security should be requested for a specific design brief in the early briefing stages of the project. All perimeter doors shall have reed switches connected to the EAC.

15.5.4 Reception Areas

If identified as a risk mitigation measure in the early design stages, 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.

15.5.5 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 as per Section 14 with approval by the Deputy Director, Planning and Development. Access from the basement to the reception area need not be secured if access to the basement is controlled but should funnel people into the public areas so that the receptionist has control of entry to the working area.

15.5.6 Stores Delivery and Despatch

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 despatch area then either a separate storeroom should be designed.

15.6 Offices

15.6.1 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.

15.6.2 General Offices

Offices selected by the risk management process 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.

15.6.3 High Security Spaces

Where possible, high security spaces or facilities should be grouped or clustered. The use of electronic access-controlled doors into either the group area, individual offices, or both shall be

mandatory. This section applies to offices for Heads of College and above, secure laboratories, specialist spaces and the like.

15.7 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.

15.7.1 Security Equipment

Generally, the electronic security and control equipment shall be co-located with the TSDIS active equipment within secure dedicated TSDIS rooms. Please refer to JCU Design Guidelines Section 26.

15.7.2 Cash Handling Area

Only if approved by the Deputy Director - Planning and Development.

15.7.3 Exam / Confidential Records Storage

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

15.7.4 Communication Rooms

The Communication Rooms shall be in a dedicated room with a single-entry point. Where possible, the 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.

Must be connected to the University’s current EAC.

Telecommunications MDF’s or IDF’s should be located and designed in as per Section 26 of these design guidelines.

15.8 Fire Escape Stairs

Fire escape stairs should not allow uncontrolled access from basements to the building interior.

15.9 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.

15.10 Recommended Laminated Impact Resistant Glass

Only for use in very limited instances and with the approval of the Deputy Director – Planning and Development during SD.

15.11 Mesh Screens

Depending on application - Crimsafe or proven equivalent mesh screens may be considered for use on advice of the Deputy Director Planning & Development during SD design phase.

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

15.12 Electronic Access Control System

Please contact JCU Manager, Security for latest specifications of the EAC. The EAC controllers shall be wall mounted in the communications room. Dedicated power and data outlets are to be provided to each control panel. Please refer section 26 for clearance and communication requirements.

Where available, access control shall be connected to the essential power supply.

The controller enclosures are to be placed between 1,500 – 2,000mm affl to allow safe access without having to utilise a ladder. The battery controller box/panel must always be placed either underneath the main controller box/panel or beside it. This will avoid batteries leaking acid over the main controller box/panels.

Card readers shall be provided for all external doors and egress paths doors, after-hours access, communications rooms, computer labs, 24-hour access rooms, particular amenities (e.g. kitchenette adjacent to conference room) and other doors as nominated in the project room data sheets. Push button to exit shall be provided for all doors that do not have free handle to exit. All external doors are also to be provided with reed switches linked to the EACS.

All auto doors and egress doors shall have a minimum of 48-hour battery backup and be connected to essential power provided to the building.

Common rooms (lecture theatres, tutorial, conference, and meeting rooms) shall have the provision for future connection to the EACS.

15.12.1 **Cabling**

Exposed cabling shall be avoided. If approved, it is to be run inside tubular conduit unless specifically approved in writing by the Deputy Director Planning & Development during SD. For buildings with an elevated security risk exposed conduits are to be metal.

All data communications cabling within the ceiling space is to be installed; on cable trays, on dedicated catenaries or via fixed conduits and the like and be securely fastened. All cables to be shielded earthed and clearly marked to the requirements of Section 25 and 26 of these design guidelines.

Note the minimum cabling segregation requirements from other services in Section 25 of these design guidelines.

All IP/Networked items of the electronic security system such as door readers, cameras and the like are to be connected using the latest standard as per Section 26 of these Design Guidelines.

All other devices door locks, strikes, reed switches etc. are to be cabled with industry standard security cabling. Provide a sample/colour specification sheet of proposed cables for use on the project at early SD design stage for approval by Deputy Director Planning & Development.

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

15.13 Freezer Alarms

All critical cold-rooms, refrigerators and freezers must be monitored by the BMS for alarms such as over/under temperature as per requirements of Section 23 of these design guidelines.

15.14 Interconnection with other Building Services

In instances where an electronic security intruder detection system is proposed for a building then a simplified method of energy management system (See Section 25) shall be employed to turn off loads to non-critical areas such as lighting, air conditioning, hot water boilers etc. when the system is "armed".

Typically, a system consists of interposing relays employed in conjunction with the extra low voltage low wattage outputs on the security alarm panel connected to relays/contactors at the Building DB's.

15.15 Security Camera Standards

Security cameras positioned within the building or structure are to be installed as determined by room data sheets and a use analysis. This will be completed as a consultative process with the JCU Manager, Security, and stakeholders during DD. The location of all cameras is to be approved by the JCU Manager, Security. At least 1 camera is to be aimed at the entrance of the building.

All Security cameras and licensing shall be procured through JCU TSDIS via existing tendered standing offer.

IP Addressable cameras, Axis Manufacture, or approved equal, with local storage capability will be considered for use on new projects, however, approval must be sought at early SD design phase for the usage of, camera views, installation location and standard and configuration on to the network and are not to be used without prior approval from the JCU Manager, Security.

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.

The location of cameras positioned externally will be selected to provide focus on facial recognition ability of people entering and exiting the building through all access points as agreed during the SD design phase with the JCU Manager, Security. 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 JCU Manager, Security following a risk assessment process.

All camera cabling is to be run as per section 26 of JCU Design Guidelines. If the project is not on the major campuses, please contact TSDIS for a suitable solution. This is to be agreed during the SD design phase with the JCU Manager, Security.

15.15.1 **Security Recording**

The Queensland Government requires 30 days' worth of footage from all cameras.

All Security cameras additional storage may be required and shall be procured through JCU TSDIS via existing tendered standing offer.

15.16 Asset Tracking System Standard

High value, portable assets may be protected at JCU within designated areas through the employment of the approved asset tracking system. The JCU Deputy Director, Planning and Development will determine the risk and need for installation of this system after user consultation to determine the risk and need.