SECTION 15

BUILDING SECURITY

15.0 BUILDING SECURITY

15.1 General

Security Design Philosophy

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

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 to sides at the bottom in after hours 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.

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.

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.