Property Services

Keying & Locking Specification Guidelines

including

Intruder Alarms

Schedule of amendments to description hierarchy:

Date	Ver.	Cla.	By	Amendment
Nov 2000	1.0		BR	Original draft
26 May 2009	2.0	all	BR	General update to all sections
27 May 2009	2.1	2.3	BR	Statement added on plant room, service duct and auto door keying
31 Aug 2011	2.2			'AMS' changed to 'Property Services'

INDEX

1 Purpose of Guidelines

The purpose of these guidelines is to regulate the standard of design criteria for supply, installation and maintenance of door hardware components and alarm systems.

2 Design Philosophy of Door Security

The keying structure in most buildings can be considered as typical hierarchical master key systems. Various keying and locking systems are in use within University buildings. There is a diversity of systems used because of the evolution of keying systems within the University and because previously, no standard was set as a matter of policy.

The majority of keying systems installed are 'restricted security systems' (ie; keying systems that are registered, therefore keys can only be cut by locksmiths upon presentation of appropriate approved signatures)

Perimeter doors to the majority of major buildings are fitted with electric locks and electronic access systems. Property Service's intention is that all buildings will eventually be fitted with these systems.

The original policy for buildings first fitted will electric/electronic systems specified that only one door would be nominated and fitted with a manual key over-ride system. This was to allow building access in case of electric/electronic system failure. Although sound in principal, this policy proved to be unworkable when individual, non-keyed door unit's failed.

It is the intent of these specification guidelines that all perimeter doors to buildings be fitted with manual key over-ride locks in conjunction with the electric/electronic systems where possible. Tamper alarm functions on electric locks and latches shall be kept to a minimum for simplicity of maintenance and reduction of false alarms.

2.1 Master Keying Principals

The common application of a system using a keying hierarchy (master keying) results in the reduction of the number of keys any individual requires to access various areas within the University, or indeed within one building.

On the Sandy Bay campus it is policy to use the University BiLock keying system to doors to the perimeter of buildings. The use of this system is becoming more widespread as time goes by and the system is now applied to several major buildings in the University.

Internal doors of buildings should be fitted with alternative proprietary keying systems and this is encouraged to provide 'best of breed' and 'value for money'. This aids in providing value for money when replacing locksets after lost or stolen keys are reported. (See also 4.9)

Keying systems should be selected for their virtual infinite combinations of master keying profiles and flexibility of use on all types and styles of locking

hardware. These range from simple desk and filing cabinet drawer locks to the more complex range of door hardware.

The University locking and keying structure is available as a separate restricted document to approved personnel, consultants and contractors.

Master keying structures for new building construction and building refurbishments must be approved by Property Services key management staff.

2.2 Master Keying Exclusions

Keying of rooms and areas 'off' the master key structure is **not permitted**. This is primarily due to Fire Brigade access requirements and University Security policy.

Non-registered keying systems may have keys cut without the appropriate approval and authority, thus making the security of buildings extremely difficult to control. These types of key structures are not approved.

2.3 Master Keying Restrictions

Various areas or spaces on campus can be 'out of bounds' for staff, students, maintenance staff and/or the public. These areas have been master keyed onto special restricted access keys. In some cases this is due to legislation requirements but more likely because of the personal risk that these areas pose.

Typical areas include:

- Radioactive Material Store Facility;
- Passenger and Goods Lift Motor Rooms;
- High-level access doors and panels through external walls;
- Examination paper security rooms;
- Cleaners stores;
- Security Node rooms;
- IT Node Rooms;
- Transmission towers;
- Gas stores;
- Areas that are deemed to be of high safety risk; and
- Confined space zones.

For specific maintenance reasons, some spaces and equipment are 'keyed alike' to allow maintenance service personnel easy and restricted access. These areas can be opened by a GMK or higher cut key.

These include:

- All plant rooms;
- Service ducts; and
- Automatic door controllers.

2.4 Tamper Alarms

Electronic door hardware can be purchased with a considerable number of tamper alarm functions. Wherever possible these functions should be kept to a minimum to help overcome nuisance/false alarms generated at the monitoring control room. Fully equipped tamper alarm locks can be quite expensive, almost one third more expensive than the model with basic functions. The only tamper alarm function that is required on most locks is the 'door ajar' reed switch function. All other options should only be taken up if it can be proven beneficial to the security of the space. '*Don't connect it just because you can*'

3 Description of Existing Systems

3.1 Keys and Cylinders

Several types of keying systems are installed into buildings. Keying systems normally have 'Design Registration' with the key manufacturer for a defined period of time. Design Registration limits who may cut keys for the system.

Systems have been installed at various times as buildings were constructed or renovated. As some buildings are quite old, the registrations within these buildings are soon to expire.

The most recently installed system is the 'BiLock Keying System'. The BiLock system is now the University standard on the Sandy Bay campus for the external / perimeter doors for new works on buildings. In time the older keying systems will be phased out of service.

3.2 Swipe and Proximity Cards

Both swipe and/or proximity access card readers are installed in a considerable number of buildings. As with keys, there are several electronic control systems installed. The majority are either 'Cardax' or 'Tecom' controls.

3.3 Locks / Hardware

Door hardware varies from building to building. This has mainly come about from individual building contracts with the architects and/or designers having personal preferences for fit out.

3.4 Electric Locks

A variety of electric locking systems are used on University campuses. These consist of electromagnetic contacts, electromagnetic shear locks, electric strike plates and electric mortice locks. Tamper alarms on these systems can be complex or simple depending on the specific areas security requirements.

3.5 Door Closers

Similarly with the above mention hardware, door closers are many and varied in brand and style. The University's maintenance section has moved towards standardising these fixtures to force economies in parts replacement and adjustment procedures. All doors fitted with electric locking/latching devices must have door closers installed to provide an aid in the lock down process.

4 Keys and Access Cards

4.1 Master Key Structure and Key Issue

See the UTAS 'Key and Access card Control Policy'

Where a master keying structure is in place for a building, only the building Fire Warden shall be entitled to posses a Building Master Key (GMK). This is issued for the purpose of checking all rooms in a building in the event of a fire alarm or building evacuation. All other building occupants may posses a School or Section Master Key (MK) or lower level cut key depending on authorisation of entry.

The following general rules apply:

GGMK	(Campus ***Great Grand Master Key***) Only issued to Security and Fire Brigade
GMK	(Building or Precinct ***Grand Master Key***) Only issued to Security, Building Fire Wardens and Emergency staff.
MK	(School or Section ***Master Key***) Issued to Executive Deans, Heads of Division, Heads of School and Heads of Section and their senior executive staff members.
CK	(Doors and Door Groups ***Change Key***) Issued to staff.
IK	(***Individual Door Key***) Issued to staff.

It is the intent of these specification guidelines to key all perimeter doors to a building on a separate key cut. The purpose of this is to reduce the cost of re-keying the building to regain security if a key set is lost or stolen. (In most cases, only half dozen doors will require re-keying as opposed to the full section or building)

4.2 Issue of Restricted Access Keys

Special restricted access keys (See Masterkeying Restrictions 2.3) will be issued to individuals who are authorised to use secured master keys. Anyone taking custody of a special restricted access key will be required to sign a statement acknowledging the responsibility for the special care and use of the key.

4.3 Issue of Proximity Access Cards and Fobs

See the UTAS 'Key and Access card Control Policy'

4.4 Key and Card Returns

See the UTAS 'Key and Access card Control Policy'

4.5 Record Keeping

See the UTAS 'Key and Access card Control Policy'

4.6 Key Stamping and Identification

The methodology for the identification and stamping of keys is controlled by Property Services and shall remain confidential and not available to staff, students or the general public.

4.7 Security of Keys and Cards

See the UTAS 'Key and Access card Control Policy'

4.8 Lost, Stolen or Non Returned Keys and Cards

See the UTAS 'Key and Access card Control Policy'

4.9 Transfer of Keys and Cards

See the UTAS 'Key and Access card Control Policy'

4.10 Request for Key or Card Issue Form

Requests for keys or cards shall be made on the appropriate form. (Print a 'Request for Key or Card Issue Form' from the Property Services Website)

5 After Hours Access and Egress

5.1 Access

See the UTAS 'Key and Access card Control Policy'

.

Programmed proximity access cards or fobs may be purchased from Property Services to allow access to nominated zones that are fitted with electric locking systems.

If users have been granted keys and they are entering buildings that are fitted with key access, then access is unrestricted to that person subject to approval from Head of School or Section.

All other access shall be arranged through the University's Security Section.

5.2 Egress

After hours egress shall be through a door nominated for this purpose. If the door is fitted with an electric locking system, the door will have a green EXIT push button clearly marked and mounted in close proximity to the door opening. All other perimeter doors shall remain securely locked after normal hours.

Nominated egress doors shall have appropriate internal and external lighting and will normally exit onto a 'Safe Walk' zone.

Nominated egress doors shall be motorised (preferably sliding) with electric locks fitted where possible to facilitate the automatic re-locking of the zone after a person exits. (Manual doors can easily slip out of closer adjustment and stand ajar in windy conditions, thus leaving the building insecure).

6 Construction and Hardware Installation Issues

6.1 Types and Styles of Locks and Hardware

Styles of hardware shall be consistent with existing fittings within a building complex. Where possible, all hardware should be selected from the 'standard' range offered by suppliers, and replacement components should be available off the shelf. One-off or purpose made fittings should be kept to an absolute minimum.

6.2 Positioning of Locks and Hardware on Doors

All electric locks and latches shall be fitted/installed in the 'near central' height position of the door. This offers the most stability and structural integrity to the locked door and frame as a unit against an attempted unauthorised entry.

Fitting of electromagnetic locks to the head region of a door assembly shall only be allowed if central zone fitting cannot be achieved.

6.3 Equipment Cupboards and Cabinets

Cupboards and cabinets that are to contain audiovisual or other expensive equipment shall be constructed of a metal framework with covering panels that will not allow unauthorised entry. The metal framework shall be rigid in construction and be securely bolted to the floor of the room.

Locks to doors and panels shall be of the Security Deadlock variety, similar to a '*Lockwood 303 Single Cylinder Deadlock*', masterkeyed to the University system.

All concealed hinges to equipment cupboard doors shall be bolted through the panel with smooth heads on the outer side and lock nuts on the inside. The second leaf of the hinge shall be welded or bolted to the metal framework of the cupboard.

7 Intruder Alarms Systems

7.1 Intruder alarms

The Door Access Control systems (DACS), Closed Circuit Television (CCTV) and Intruder Alarm Units (IAU) provide an integrated and highly sophisticated security network for the security of people and their property on the University campus. The systems are monitored twenty-four hours day by the University's own fully equipped Central Monitoring Stations.

Help point telephones and CCTV systems are being developed and placed in strategic locations along developed lighted safe walks.

All intruder alarms shall be installed and connected to the University central monitoring systems. Local alarms/sirens and/or flashing lights may be installed in some areas in parallel to the connection to the central monitoring system.

Persons accessing alarmed areas should familiarise themselves with alarm control functions. Some systems 'auto-reset', however others are designed to be manually set by the users. Persons commonly using alarmed areas are responsible for the setting and integrity of the system.

(System specifications are available from Property Services)

7.2 System Access Codes

Three levels of access codes shall be programmed into all systems.

- ***Master Codes*** that can override and disable all other settings and allow system parameters to be programmed.
- ***Service Agent Codes*** that allow general programming and maintenance.
- ***User Group Codes*** that allow activation and de-activation functions.

All access codes shall be supplied to Property Services as part of the 'As Installed' documentation during installation.

The Master codes shall not be passed on to the Service Agent or User Groups.

If a change occurs with Service Agent or User Groups, then new access codes shall be programmed into the system with copies passed to Property Services for safe keeping and record updating.

7.3 Backup systems

All intruder alarms shall operate normally for a minimum of twelve (12) hours in an armed position if mains power fails. All stand-by batteries and back up systems shall be installed in a position that is accessible, therefore enabling regular servicing of the units.

Servicing requirements shall form part of the 'As Installed' documentation.

7.4 Tamper Alarms

Electronic door hardware can be purchased with a considerable number of tamper alarm functions. Wherever possible these functions should be kept to a minimum to help overcome nuisance/false alarms generated at the monitoring control room. Fully equipped tamper alarm locks can be quite expensive, almost one-third more expensive than the model with basic functions. The only tamper alarm function that is required on most locks is the 'door ajar' reed switch function. All other options should only be 'taken up' if it can be proven beneficial to the security of the space. '*Don't connect it just because you can*'