

Key and Access Card Control Policy

Approving authority	Vice President (Corporate Services)
Approval date	4 July 2016
Advisor	Director, Campus Life N.Collier-Jackson@griffith.edu.au (07) 373 57592
Next scheduled review	2019
Document URL	http://policies.griffith.edu.au/pdf/Key and Access Card Control Policy.pdf
TRIM document	2016/0000096
Description	This policy defines the procedures for key and access card control for security purposes throughout the University, including the issuing of locks and keys, the responsibilities associated with maintaining security, and details of actions to be taken to re-pin locks or when keys are lost or stolen.

Related documents

[Incident/Hazard Report Form](#)

[Griffith University Key and Access Card Control Plan](#)

[Griffith University Key and Access Card Control Guidelines](#)

Contact Security & Traffic Manager, Campus Life for the following documents:

Campus Life Lost Key Risk Assessment Work Instruction

Campus Life Lost key Assessment Proforma

[\[Purpose of Key Control\]](#) [\[Areas of Control\]](#) [\[Issue of Locks/Keys\]](#) [\[Key Control Elements/Areas\]](#) [\[Key Audits\]](#) [\[Key Responsibility and Security\]](#) [\[Tenants\]](#) [\[Ordering and Re-pinning of Locks\]](#) [\[Lost/Stolen Keys\]](#) [\[Information Pack\]](#)

1. PURPOSE OF KEY AND ACCESS CARD CONTROL

- 1.1 The University has a varied population of staff, students and individuals involved with the University who require access to different sections of buildings for various purposes. Notwithstanding this there is also a requirement to secure the University's assets and minimise the opportunity for theft and damage of assets. It is therefore essential that the University's electronic and mechanical security systems are consistent with such needs. The purpose of this policy is to regulate access to the University and make staff, students and individuals associated with the University aware of their respective responsibilities when assigned keys and access cards, or when managing keys or access cards on behalf of the University.
- 1.2 This Key and Access Card Control Policy applies to all individuals issued with Keys and Access Cards.

2. KEYING AND ACCESS CONTROL PLAN

- 2.1 The University has a varied population of staff, students and individuals involved with the University who require access to different sections of buildings for various purposes. Notwithstanding this there is also a requirement to secure the University's assets and minimise the opportunity for theft and damage of assets. It is therefore essential that the University's electronic and mechanical security systems are consistent with such needs. The purpose of this policy is to regulate access to the University and make staff, students and individuals associated with the University aware of their respective responsibilities when assigned keys and access cards, or when managing keys or access cards on behalf of the University.

- 2.2 The University uses mechanical locks to secure all rooms, switchboards and service risers. An electronic access control system is employed to supplement the mechanical locking system throughout the University and, where appropriate provide a more effective access solution for areas that:
- Are frequently inhabited eg, common use computer laboratories
 - Require restricted entry eg. research laboratories, data centres
 - Require additional security to protect the University's assets
- 2.3 The access control system is also used to secure and control access to external entry doors of most University buildings.
-

3. ISSUE OF KEYS AND ACCESS CARDS

3.1 The normal scale of issue for a Key is:

- **Room Key (Service level)** - One key per room occupant
- **Master Keys** - A set number of Master keys will be provided to the Element based on the keying plan for the building(s) occupied. Master keys are to remain on campus and secured in a key cabinet when not in use, and records maintained of usage.
- **Common Use Keys** – Common Use keys are those used for general office spaces, resource rooms, photocopy areas, tea/lunch rooms, etc and are issued to those people required to access and open up these common use areas before other building occupants. A key to these areas should also be kept in the key cabinet for short-term sign out and issue as required.
- **General Service Master Keys** - are only issued to Campus Life. Exceptions may be considered when a specific recommendation (accompanied by a risk assessment) is made by an Element's Director, Dean or Head of School/Department and approved by the Director Campus Life (or their delegate).
- **Grand Master keys** are issued to Security for issues to contractors to conduct their work, eg. maintenance, cleaning.
- **Great Grand Master keys** - are only issued to campus Security and the Fire Brigade
- **Switchboard and/or electrical service riser keys** will only be issued to Campus Life. Exceptions may be considered when a specific recommendation (accompanied by a risk assessment) is made by an Element's Director, Dean or Head of School/Department and approved by the Campus Facilities Manager (or their delegate).
- **Access Control Override keys** are issued to Security and Maintenance staff for emergency use only.

3.2 The normal scale of issue for an Access Card is:

- **Proximity (Access) Card** – One per individual

3.3 All Keys and Access Cards remain the property of the University.

The Campus Operations Coordinator will perform the initial key issue to the school/element Key Control Officer.

The Security and Traffic section will provide Access Cards to authorised Access Card Operators on request.

All keys shall be signed for by the recipient before issuing, and shall only be issued by a Key Control Officer.

The duplication of a University key/access card and or maintaining a 'spare' is prohibited, unless authorised by the Vice President (Corporate Services).

4. KEY AND ACCESS CARD CONTROL

A key component of managing access to and maintaining the security of the University's buildings is the effective management of Keys and Access Cards.

4.1 Ordering of Keys

The authority for ordering keys to be cut by the University's locksmith is as follows:

- Campus Keys (Great Grand Master) – Security and Traffic Manager, Associate Director Facilities Management
- Building Keys (Grand Master Key) – Security and Traffic Manager, Associate Director Facilities Management, Campus Facilities Manager, Security Systems Administrator, and Operations Coordinator
- Internal Areas (Master Keys) - Security and Traffic Manager, Associate Director Facilities Management, Campus Facilities Manager, Security Systems Administrator, Operations Coordinator, and Key Control Officers (Gold Coast only)
- Room Keys (Service level keys) - Security and Traffic Manager, Associate Director Facilities Management, Campus Facilities Manager, Security Systems Administrator, Operations Coordinator, and Key Control Officers

The University's locksmith will confirm prior to cutting a key that the staff member ordering a key is authorised to do so. Where the staff member is not listed as an authorised Key Control Officer the locksmith is required to confirm with the Security and Traffic Manager or the Security Systems Administrator the authenticity of the staff member requesting the key.

4.1.2 Ordering of Access Cards

Access Card operators are authorised to order Access Cards from the Security and Traffic section.

4.1.3 Storage of Keys and Access Cards

All keys not issued are to be stored in approved key cabinets. Key cabinets shall be kept locked at all times and keys for their operation are to be held only by the Key Control Officer and one other delegated officer authorised to operate the key cupboard for urgent requirements in case of absence.

Programmed Access Cards are to be stored in a secure area at all times.

4.1.4. Keys required to remain on University Grounds

Unless authorised in writing by the Director Campus Life or Vice President (Corporate Services) no Great Grand Master, Grand Master, Master keys or General Service Master Key are to be taken off the University site. Disciplinary action may follow if this level of key is taken off site without authorisation and dismissal may result from any loss of such keys taken off site.

4.1.5 Lost or Stolen Keys and Access Cards

If a key is lost or stolen, and after a 24 hour period are still not found, a report must be made to the Campus Facilities Manager on a Campus Life Lost Key Assessment Proforma. A detailed statement outlining the events that occurred resulting in the key/s becoming lost or stolen must be provided. This may result in either a re-key of the area that the key opens or a new key(s) being cut for the occupant depending on the risk assessment conducted.

The Campus Facilities Manager and the Security and Traffic Manager will conduct the risk assessment.

Where the loss of a key presents a high risk to the University a re-key of the area or building will be occur. The cost of the re-key will be borne by the school/element to which the key belongs.

If an Access Card is lost or stolen, and after a 24 hour period are still not found, it is to be reported to the respective Gallagher operator.

4.1.6 Automated Access Card Expiry

To assist in managing the unauthorised use of Access Cards the following expirations are programmed in Gallagher:

- Fixed Term appointments – card use expires at the end of the contract
- Continuing appointments – card use expires every two years
- Students – card use expires at the end of their enrolment
- All card use expires after 180 days of inactivity

4.1.7 Key Audits

Each year the Security and Traffic section conducts a full Master key audit and spot checks of service level keys.

5. ORDERING OF LOCKS

New locks or padlocks should be submitted on a Campus Life Work Request form on the Griffith Portal.

6. RESPONSIBILITIES

6.1 Associate Director Facilities Management is responsible for:

- Approving the Key and Access Card Control Plan.

6.2 Security and Traffic is responsible for:

- Design and management of the University's physical and electronic access control systems
- Reviewing and updating the Key and Access Control Plan
- Maintenance of a central Key Register (GGMK, GMK, GSMK and MK)
- Maintenance of a central Access Card Register
- Auditing the access control system
- Annual auditing of all Master Keys
- Spot audits of Service level keys
- Supplying the University's locksmith with an up to date register of authorised Key Control Officers
- Maintain an accurate register of Access Card Operators

6.3 Campus Facilities Operations Coordinators are responsible for:

- Initial issue of keys to Schools/Elements on occupation of an area
- Retrieval of keys when a School/Element vacates a space
- Recording and destruction of all redundant keys
- Undertaking the role of Key Control Officer for keys issued to the Campus for maintenance, cleaning and security

6.4 Deans, Heads of School/Department or Director of Element is responsible for:

- Appointing a Key Control Officer to order, store, manage and account for all keys issued to the School/Element. Where the responsibility is not delegated the relevant Deans, Heads of School/Department or Director of Element will be held responsible.

- Appointing an Access Card Operator to order, store and program Access Cards issued within the School/Element. Where the responsibility is not delegated the relevant Deans, Heads of School/Department or Director of Element will be held responsible.

6.5 Key Control Officer is responsible for:

- Ensuring all keys issued to the School/Element are secured in an approved key cabinet and documented appropriately
- Managing all keys under their control in accordance with the Key Control Guidelines (ordering, issuing, recording and auditing of keys)
- Ensuring keys are retrieved from staff and students when they cease employment, studies or go on extended leave. For the purpose of this document extended leave means 120 days or more.

6.6 Access Card Operator is responsible for:

- Ordering, storing, programming and issuing Access Cards within their Element/School
- Ensuring Access cards are retrieved from staff, students and visitors when they cease employment studies or go on extended leave. For the purpose of this document extended leave means 120 days or more
- Withdrawing access from Gallagher where staff, students or visitors do not return access cards on leaving the University, or when access cards are reported lost.

6.7 All persons issued with a University key/access card are responsible for:

- Safe-keeping of the key/access card including not lending the key/access card to any other person
- Reporting any loss or theft of, or damage to, the key/access card to their respective Key Control Officer upon discovery of the loss, theft or damage
- Handing back keys at cessation of employment, studies or when on extended leave. For the purpose of this document extended leave means 120 days or more.

7. TENANTS AND CONTRACTORS IN UNIVERSITY OWNED BUILDINGS

Commercial businesses and other tenants using University buildings are required to use the same key systems as the University and are required to adhere to this Policy. Tenant keys are issued by the School/Element Key Control Officer responsible for the space in which the tenant resides.

Tenant and Contractor organisations that lose or cannot produce a key on demand will be liable for the total cost associated with re-keying the locks to the area/s compromised and providing replacement keys.

DEFINITIONS

Key and Access Control Plan – A document that sets out how the university uses electronic and mechanical keying to secure its buildings and rooms. Identifies the initial issue of keys to Schools and Elements, the method by which keys are to be stored when not in use, the process to be followed when keys are lost and audit process for ensuring effective key management.

Key Cabinet – A secure key press/cabinet used for the storage of keys when not in use. The cabinet may be either mechanical or electronic in its operation.

Key Control Officer – A person designated by the School/Element to be responsible for the management and administration of all physical keys under their control.

General Services Master Key – A key that opens all switchboards and service risers.

Access Card Operator - A person designated by the School/Element to be responsible for the management and administration of all Proximity Cards.

Great Grand Master Key – A *campus* specific Master Key that opens all doors in all buildings on campus. The great grand master key designed to fit a number of different master-keyed systems of locks.

Grand Master Key – A *building* specific Master Key that opens all doors within a designated building.

Master Key – A Master Key that opens all door within a school/element or floor area for a specific building.

Room Key/Service level key – An individual room key for a specific building.

Maison Keying - A Maison key system is a keying system that permits a lock to be opened with a number of unique, individual keys. Unlike a master key system, where each individual lock has one individual operating key and one common master key, a Maison lock is designed to be operated by every key within the system.

Redundant Key – A key that is no longer issued due to damage and/or the lock being replaced.

Proximity (Access) Card – An electronic card used for access to buildings, electronically locked rooms, limited and undercover carparks.