Estate Management

Key Management Procedure

Security & Traffic Management

Authorised by:	Tara Murphy, Security & Traffic Management Manager, 5th August 2015
Effective date:	5th August 2015
Superseded documents:	N/A
Contact officer/s:	Tara Murphy (Manager) tara.murphy@unsw.edu.au 9385 6781 Natalie Glanville (Systems Officer) n.glanville@unsw.edu.au 9385 7978 Melissa Fenech (Operations Manager, Systems) m.fenech@unsw.edu.au 9385 1358
Related documents:	Key Approval Form, Authorized Restricted Key Holder List.

1. Purpose

The purpose of the Key Management Procedure is to assist with the control, usage and possession of keys within the University of New South Wales to ensure an appropriate level of accessibility and security is supplied to all personnel and facilities.

2. Scope

The Key Management procedure applies to all Faculty/Divisions, Contractors, Cleaners and Security within The University of New South Wales who are issued any restricted keys such as Great Grand Master, Grand Master, Master, Switchboard, Bollard and E-Keys. The Key Management procedure relates to Kensington, Randwick, Tarben Creek, David Phillips Field, Cliffbrook, Paddington and Manly Vale campuses.

3. Definitions

Great Grand Master Key (GGMK) – A master key which opens all the locks in a large master key system divided into two or more groups of locks, each group operated by a different grand master key and further subdivided into other groups operated by different master keys.

Grand Master Key (GMK) – A master key opening all the locks in a master key system or in a sub-system, which is divided into two or more groups of locks, each group operated by a different master key.

Master Key (MK) – A key which operates every lock in a group, whether keyed different or keyed alike.

Sub-Master Key (SMK) – A key designed for control of a limited number of a series of lock operating mechanisms and subordinate to a master key.

E-Key – A selective master key designed into a master key system and set to open locks also controlled by various other master keys, without cross-keying, thereby permitting maintenance people to enter areas they must enter without giving them the use of the high level master keys.

Keying Levels – The division of a master key system, each higher level operating more groups of locks than the next lower level.

Key Manager – ProMaster Key Manager is a database designed to track and control key issue and return, providing an effective level of security and protection.

4. Roles and responsibilities

1. The Security Systems Officer will manage and control restricted keys being issued and collected, as well as associated paperwork and database maintenance.

2. All restricted key requests must be logged via ARCHIBUS with authorization from the appropriate level of authority that will then be submitted to the Systems Officer for approval.

3. Upon notification of key collection, a signature is required from the key holder and approver which must be personally picked up from the Systems Office.

4. Keys shall be stored in a Keywatcher or secure location left on Campus. Key holders shall take measures to protect and safeguard any keys issued to them or in their name.

5. Key holders must not transfer or loan keys to non-authorized individuals.

6. Key holders will not attempt in any manner to duplicate or modify keys in their possession.

7. Individuals will only be issued with only one copy of each key. There may be an exception for approved multiple keys for operational purposes that will be managed on a case by case basis.

8. Keys shall be issued for a required period of time, not by term of employment.

9. All keys must be returned to Security & Traffic Management when no longer required. In the situation of an individual changing position within the University, the individual must return the keys issued for their specific position and will be issued the appropriate new keys for their new position if required and/or approved.

10. It is the responsibility of the Faculty/Division Managers to ensure keys are returned to the Security Systems Office when staff leave or move elsewhere.

11. Broken, damaged, or worn keys must be returned to the Security Systems Office with a Key Request form for replacement key/s.

12. Found keys should be returned to the Security Systems Office as soon as possible.

4.1 Lost Keys

1. Key holders must immediately report any lost, damaged, missing or stolen keys to Security Systems. If a key is lost, a Lost Key Form shall be completed and signed by the person whose key was lost or stolen. The key's status shall be changed to "Lost" in the Key Manager database and the appropriate steps followed for issuing a new key.

2. The Security Manager or Security Systems Officer will assess the risk associated with the missing key(s). This may lead to Security & Traffic Management seeking re-imbursement of the cost of re-issuing the key after it has been lost or stolen from the corresponding department, individual or contractor. If the loss or theft of a key creates the need to re-key a part of the campus then the cost may be passed to the department, individual or contractor.

3. Re-keying of a building or a group of rooms may result in personnel being required to exchange an old key for a new one. Head of Departments are responsible for ensuring the collection of old keys and disposing of them appropriately before new keys are issued.

4. If any individual has two or more separate incidents of lost, stolen, or non-returned key violations within a one-year period, key privileges will be reviewed and may be revoked.

4.2 Key Audits

An initial Key Audit will be performed to ensure an accurate starting point. Subsequently, the Security Systems Officer will conduct random audits.