Key Control Procedure

1. Guiding Principles

As part of the WA Country Health Service (WACHS) Security Risk Management Policy, this procedure addresses key control issues, including:

- issuing keys and cards
- key management
- key audits
- key registers and
- lost or stolen keys.

The responsible person, in consultation with stakeholders is to ensure that appropriate controls are implementing to assure the integrity of the key management system.

2. Procedure

The aim of this procedure is to protect people and assets and minimise the likelihood of security events related to theft and violence. All WACHS facilities are to be locked down at a time determined by the responsible person, as outlined in the WACHS Access Control Procedure.

Employees who have been issued with keys or access cards accept responsibility and are authorised to use these items to gain access to those areas necessary for the performance of their routine duties and responsibilities. The keeping of spare keys and activated access cards and the duplication of keys other than through engineering services is prohibited.

The responsible person, following risk assessment, is to determine the following:

2.1 Issue of Keys and Cards

- Where practicable, all external doors are keyed alike as this increases the security of the building as all after-hours access to the building is through the designated after hours single point of entry.
- Areas can be either be keyed alike or keyed differently. No maison keying is to occur within WACHS.
- Common use areas are to be keyed alike to limit the number of keys that need to be issued.
- Re-keys are to be kept at the lowest level (service level) of keying possible. Areas are not to be re-keyed to a system where people are reliant on Master keys to obtain access to several areas; these areas are to be keyed alike or where practicable and cost effective, fitted with an Access Control Card System (ACCS).
- All keys that are not issued are to be stored in approved “secure key cabinets”. The maintenance officer is to determine the type and size of key cabinets in consultation with the responsible person.

- The total cost involved in cutting of new or replacement keys and locks, once approved by the responsible person, is to be at the expense of the cost centre making the request, unless the work is a new building, or replacement due to normal wear and tear. Maintenance due to wear and tear of locks and keys, as determined by the maintenance officer, is to be paid for and carried out by engineering.

The Normal Scale of Key Issue is to be:

- one service level room key to each occupant of a separate room in the building interior. If, at the discretion of the responsible person, a decision is made to permanently issue a master or higher-level key, then full details pertaining to the issue of these keys need to be reported to the maintenance officer (or delegate).
- keys to common use areas (general office spaces, resource rooms, photocopy areas, store rooms and so on) are to be issued to those people who are required to access to these common use areas before anyone else on a daily basis. Another key to these areas are to be kept in the key cabinet for short-term sign out and issue as required.
- one access card or external door key for the single point of entry to the building for those persons provided with a room key as above, upon establishment that after-hours access is required on a frequent basis.
- switchboard and/or electrical service riser keys are not to be issued to any person other than the responsible person. Exceptions may be considered by the responsible person in consultation with the maintenance officer, subject to a specific recommendation outlining the need for such access (accompanied by a risk assessment) is made to the responsible person.

2.2 Establish and Maintain Key Management Systems

- Control of keys is normally to be determined by the responsible person in consultation with the maintenance officer.
- Where keying is controlled centrally through engineering, the maintenance officer is accountable for the maintenance and management of the key management system (i.e. cutting, issuing, recording and auditing of keys). The maintenance officer is to ensure returned or non-issued keys are secured and documented appropriately.
- Where keying is de-centralised, the responsible person (or delegate) for the facility is accountable for the maintenance and management of the key management system (cutting, issuing, recording and auditing of keys). The responsible person is to ensure returned or non-issued keys are secured and documented appropriately.
- Master keys are not to be issued unless specifically authorised by the responsible person or maintenance officer. Master keys that are not issued are to be kept in a secure area in a key cabinet for emergency use only.
- Master keys are only to be taken off site when authorised in writing by the responsible person. Disciplinary action is to follow if keys are taken off-site without authorisation.

- All key cupboards are to be kept locked at all times and keys for their operation are to be held only by the responsible person for key management and one other delegated officer authorised to operate the key cupboard for urgent requirements in case of absence.
- The responsible person is to ensure that keys are retrieved from staff and others (i.e. a visiting medical practitioner) when they cease employment, contract work or go on extended leave.
- Each employee and other issued a key is responsible for its safekeeping. If an employee or other ceases employment or work at the site or goes on extended leave, they are required to return all keys issued to the person responsible for key management for that site.
- Keys are only to be issued to staff with authority to draw them. This process is to be appropriately documented for audit purposes.
- Cleaning and maintenance staff are not to have uncontrolled access to departmental keys.

2.3 Key Audits

- Every year a full master key audit and 50% service key audit (via a sampling methodology) is to be conducted by each area that has responsibility for key management to ascertain that key security is maintained. The responsible person (or delegate) is to nominate audit dates and compliance periods and the means of reporting the outcome through the safety committee.

2.4 Key Register

- The responsible person is to ensure that a key register (see example below) is maintained. Keys, including access cards, may be issued to an employee or others as outlined below. A site procedure is to exist that makes it clear to a person signing for a key that they:
  - are accountable for the security and safety of the key which remains WACHS property
  - must surrender a key on demand of the responsible person
  - are required to produce the key on demand for audit purposes
  - are not permitted to wear a key around the neck
  - must not leave the key in an insecure place or loan it to another person.
- Keys subject to alternative arrangements, for example a set of orderly or shift supervisor's keys, must be signed for in a handover book and are subject to normal key audit requirements.
- Where service continuity dictates, after an initial sign out from the site key register by the responsible person or their delegate, an alternative means of verifying key possession may be implemented.

2.5 Lost or Stolen Keys

- Keys lost or stolen and unable to be found after a 24 hour period are to be reported to the responsible person and a WACHS Safety Risk Report Form is to be completed with an attached detailed statement outlining the events which occurred resulting in the keys becoming lost or stolen. Risk controls may result in either a re-key of the area that the key opens or new keys being cut for the occupant depending on the risk assessment conducted.

3. Example of Key Register

KEY REGISTER

SITE NAME: _____ **Office Use Only**

				Keys Issued			Keys Returned		
Date Issued	**Name (print)**	**Signature**	**Telephone Number**	**Series Number**	**Filing Cabinet (tick)**	**Other (List)**	**Date Returned**	**Name of Receiving Officer**	**Initial**

4. Definitions

Responsible person in the context of this procedure	- the line manager - the person in control of the workplace where this is not the line manager.
Security risk management	refers to the systematic application of WACHS policies, procedures and systems of work to the tasks of establishing the context and identifying, controlling, monitoring and communicating risk. It encompasses the assessment of all aspects of the clinical and non-clinical environment, including consideration of internal and external risks or threats
Key management	is the establishment of an original and duplicate key control system for keys to various departments and area within the facility
Key registers	are a record of signed out and returned keys for members of staff
Delegated Authority	means the person within the facility authorised to manage the Key Management system

5. Roles and Responsibilities

The responsible person is to conduct an annual audit of all master keys and 50% of service keys to ensure that key registers are accurate. The results and any necessary corrective actions is to be reported to the safety committee.

6. Evaluation

Nil key management infringements in restricted areas.
Key audits account for 100% of keys.

7. References

Australasian Health Facilities Guidelines, part C – design for access, mobility, OHS and security, (2010). HCAMC and UNSW, Sydney, NSW.

Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in Health Facilities (2003). NSW Department of Health, Sydney, NSW.

Standards Australia, (1997). AS/NZ 4485.1:1997 - Security for Health Care Facilities (General requirements), Homebush, NSW.

Standards Australia, (1997) AS/NZ 4485.2:1997 - Security for Health Care Facilities (Procedures guide), Homebush, NSW.

Standards Australia, AS/NZS ISO 31000:2009 - Risk Management, Homebush, NSW.

8. Related Policy Documents

WACHS Access Control Procedure

WACHS Security Risk Management Policy

9. Related WA Health Policies

WA Health Risk Management Policy

10. WA Health Policy Framework

Risk, Compliance and Audit Policy Framework

This document can be made available in alternative formats on request for a person with a disability

Contact:	WACHS Work Health and Safety Manager (K.McClean)		
Directorate:	Workforce	**TRIM Record #**	ED-CO-15-2128
Version:	2.00	**Date Published:**	1 May 2017