Justice Health & Forensic Mental Health Network
PO BOX 150 Matraville NSW 2036
Tel (02) 9700 3000
http://www.justicehealth.nsw.gov.au

JH&FMHN Key Administration

Policy Number 2.050

Policy Function Leadership and Management

Issue Date 5 May 2015

Summary This policy ensures that effective key control procedures are implemented across the Justice Health & Forensic Mental Health Network.

Responsible Officer Executive Director Governance and Commercial Services

Applicable Sites

- ☒ Administration Centres
- ☒ Community Sites (e.g. Court Liaison Service, Community Integration Team, etc.)
- ☒ Health Centres (Adult and Juvenile Correctional Centres or Police Cells)
- ☒ Health Centres (Juvenile Justice Centres)
- ☒ Long Bay Hospital
- ☐ The Forensic Hospital

Previous Issue(s) Policy 2.050 (May 2009)

Change Summary

- Minor terminology changes
- Clarification of roles and responsibilities in the Health Centres, Long Bay Hospital, Forensic Hospital and the Justice Health Administration Centre

TRIM Reference POLJH/2050

Authorised by Chief Executive, Justice Health & Forensic Mental Health Network

1. Preface

An established key management system ensures that the organisation has a comprehensive system for managing all keys, which outlines security related accountabilities to protect people and property and minimise the likelihood of thefts or assaults.

Staff working in a partner agency environment must follow their policies and procedures when allocated keys at the site they are working in.

2. Policy Content

2.1 Mandatory Requirements

It is the responsibility of each health centre and administration facility to develop an ongoing system of managing the distribution and allocation of keys. Staff must ensure that all reasonably foreseeable security risks associated with key control are identified, assessed and eliminated through effective control of keys.

2.2 Definition of Keys

2.2.1 Security Keys

Security keys generally control access to people or assets and can include the following:

- Grand master keys, master keys, sub-master and individual room keys.
- Restricted keys.
- Custodial keys.
- Pharmacy, drug safe and cabinets containing valuable or confidential materials.
- Safe keys or other security container keys.
- Key safes.
- Keys or proximity cards to specialist areas where for clinical/legal reasons patient movement around the facility or area is restricted.
- Keys to access high valued assets or sensitive assets.

2.2.2 General Administration Keys

General administration keys give access to support services and domestic assets that are not considered high value.

2.2.3 Proximity Cards

Proximity cards are smart cards which can be read without inserting it into a reader device, as required by earlier magnetic stripe cards such as credit cards.

2.3 Implementation - Roles & Responsibilities

Staff are responsible for:

- Managing the keys issued to them and making sure that keys are not lying around in view. The staff member issued with a key and proximity card is solely responsible for its use. Individual keys and proximity cards must be securely attached to staff clothing at all times to ensure its safe keeping. A staff member must never give their allocated keys or proximity cards to any other staff member at any time.

- If keys are discovered as lost, staff members must contact the relevant Manager as soon as possible to report the loss. Any staff member that becomes aware that they do not have their key or proximity card must inform their line manager or the Nursing Unit Manager (NUM) immediately.
- Incident must be logged by the employee (or their line manager) at *Property Security Hazard* form in Incident Information Management System (IIMS).

At any time for whatever reason a staff member is absent from their work area and such area is lockable by any means, the staff member must ensure that the door is locked during their absence, particularly the areas accessible by patients and visitors.

Managers (*refers to all managers and supervisors who have direct responsibility for staff*) are responsible for:

- Ensuring correct procedures are being followed in their work areas (e.g. keys securely attached to staff clothing at all times).
- Undertaking routine security risk self-assessments and taking appropriate action/s where necessary (e.g. Key control management).
- Identifying and assessing areas where personal and property security can be improved in consultation with staff.
- Reporting security related incidents, so that a risk assessment can be undertaken.
- Notifying the Records Management Unit (RMU) when staff resign from their positions.
- Ensuring local orientation for S4 and S8 drug safe keys to approved staff.

2.3.1 Health Centres

The NUM or Nurse in Charge (NiC) of a health centre is responsible for all aspects of key management including:

- Grand master keys, master keys, sub-master and individual room keys.
- Local orientation on policies and procedures for the management of JH&FMHN keys, including S4 or S8 drug safe keys. CSNSW / JJNSW will provide local orientation to JH&FMHN staff on procedures for the management of access keys used in Correctional Centres.
- Management of spare keys.
- Management of key watchers.

2.3.2 Long Bay Hospital

All staff working in Long Bay Hospital are allocated keys once they are biometrically registered. Key bunches are to be attached to a CSNSW issued lanyard at all times.

The name and workplace of new or relieving staff must be forwarded to CSNSW at least one week in advance to allow for CSNSW to allocate keys.

In the event of a key being damaged, broken or mislaid, Public Private Partnerships (PPP) Helpdesk and CSNSW, Manager of Security (MoS) must be informed immediately.

Drug safe keys must be carried by nursing staff at all times. S4 keys are to be kept on a blue lanyard and can be carried by enrolled nurses with endorsement. S8 keys are to be kept on a red lanyard and can only be carried by a registered nurse. If keys are mislaid, the nurse must report immediately to the NUM/NiC, CS NSW and the After Hours Nurse Manager (AHNM) and a Property Security Hazard form in IIMS must be completed. In the event of a key being damaged, the nurse must inform the NUM/NiC or the AHNM.

2.3.3 The Forensic Hospital

This section must be read in conjunction with JH&FMHN policies 5.002 *Access to the Forensic Hospital* and 5.005 *Alarm, Pager & Two-Way Radio Use and Management, Forensic Hospital*.

Keys and proximity cards at The Forensic Hospital are classified as security keys. For reasons of safety and security, the Emergency Response Team and clinical staff must maintain access to all clinical and patient areas. Therefore, it is essential that these areas remain on the master key system. Any changes to the master key system must be approved by the Manager Security and Fire Safety, Forensic Hospital.

The individual security key bunch normally consists of a master key, proximity card and personal duress alarm device. Staff can only be issued with individually allocated keys and proximity cards after approval by the JH&FMHN Manger Security and Fire Safety, Forensic Hospital. This process includes:

- Confirmation of identity including bio-metric registration
- Prevention & Management of Violence and Aggression (PMVA) training; and
- The Forensic Hospital Fire Safety Training.

Staff who have not been approved by the Manager Security and Fire Safety, Forensic Hospital for an individually allocated key bunch will be required to be escorted and supervised inside the Forensic Hospital site.

Manager Security and Fire Safety, Forensic Hospital is responsible for:

- Identifying, assessing and managing security risks for the facility.
- Monitoring the registration process and for resolving identified security issues.
- Allocating appropriate keys.
- Providing PPP with the Forensic Hospital key safe schedule and staff master list for programming and issuing restricted security keys.
- Initiating a hospital-wide search upon discovery of missing or stolen keys.
- Maintaining Forensic Hospital spare keys.
- Ordering security keys or cylinders when required.
- Initiating hospital-wide search upon discovery of missing or stolen keys.

PPP is responsible for:

- Maintaining the integrity of the key/proximity card system (e.g. key watcher safe).
- Maintaining security of custodial keys.
- Processing authorised staff to ensure that all persons seeking access to The Forensic Hospital undergo and meet the authentication requirements.
- Administer the issue and return of security keys and proximity cards.
- Auditing the keys and completing the key check log at approximately 1100, 1700, 1830 and 2130 hours.
- Completing the key reconciliation list at approximately 22:30 hours.
- Notifying the AHNM, Deputy Director of Nursing and Manager Security and Fire Safety, Forensic Hospital of any lost or stolen security keys or proximity cards in accordance with G4S Emergency Order No.6, Key Bunch compromise.

- Programming and issuing of security keys and proximity cards in conjunction with the notification given by the JH&FMHN Manager Security and Fire Safety, Forensic Hospital or delegate, through the Help Desk.
- Ordering security keys or cylinders for the Forensic Hospital in conjunction with authorisation from the JH & FMHN Manager Security and Fire Safety, Forensic Hospital.
- Producing reports on proximity cards from the system.
- Conducting annual asset key audit of custodial and security keys.

2.3.4 Justice Health & Forensic Mental Health Network Administration Centre

Manager Facilities & Logistics (MF&L) is responsible for:

- Considering who in the Justice Health Administration Centre (JHAC) will have the authority to hold and control keys in the JHAC.
- Maintaining a JHAC key register to list key cutting codes and track the inventory and issuance of keys. Keys issued on a daily or temporary basis should be tracked in detail and documentation must be retained for a minimum of twelve months after last action completed.
- Physically checking the keys on hand for the JHAC once every six months against the key register to ensure that all keys are accounted for and report any unaccounted keys to the Manager Corporate Services.
- Managing all forms relating to the issuance, transfer or return of keys in the JHAC.
- Taking immediate action to replace compromised locks in the JHAC.
- Destroying keys in the JHAC that are no longer required.
- Reconcile monthly proximity card list for the JHAC and the JHAC car park provided by PPP and advise PPP of any changes.
- Provide three monthly access reports to Pharmacy and the Executive unit.
- Issue proximity cards only to staff based at the JHAC and to staff with direct reporting to Executive Directors at the JHAC.
- Issue unrestricted (24/7) boom gate cards to the JHAC car park only to permanent JHAC staff and restricted (After hours) boom gate cards to the Forensic Hospital staff.

Access to the JHAC Key Safe

Key safes are located in the JHAC for the storage of JH&FMHN owned keys. Keys to the key safe are held by the MF&L and the Manager Administrative Services. The register is located in the key safe. People with authorised access to the key safe include the:

- Chief Executive
- Executive Director Governance & Commercial Services
- Manager Corporate Services
- MF&L
- Manager Administrative Services

Return of Keys or Surplus Keys in the JHAC

Should staff find that a JH&FMHN key issued to them is no longer required, the key must be returned to the MF&L. The key register will be noted with any key return.

When staff resign they must return all keys issued to them. The final personnel and pay clearance will depend on the staff member returning the keys issued to them. Replacement costs for keys not returned upon

resignation may be deducted from final pay. Staff resigning must return the keys to the MF&L and must not hand any keys to replacement staff.

Loss of Security Keys

The loss of a security key must always be regarded as a security risk. If a security key is missing or found, staff must contact their line manager in the Health Centre or PPP Helpdesk at the JHAC, Forensic Hospital and Long Bay Hospital. A security risk that has arisen from a found or missing security key in a health centre must be logged in IIMS.

Keys Issued Temporarily

Temporary access to a JH&FMHN facility, property or vehicle may be arranged through the relevant line Manager or the MF&L. Staff will be required to sign for the key, which must be returned as soon as possible after it is no longer needed. All relevant forms must be forwarded to the MF&L for retention.

Staff should not be using other staff's proximity cards as every entry is captured on an activity report provided by PPP. This report captures the proximity card number, the name of the staff the card is assigned to, the entry point and the date and time of entry.

Duplicated Keys

Staff should note that the duplication of any JH&FMHN keys is prohibited without prior authorisation from the MF&L and JH&FMHN Manager Security and Fire Safety, Forensic Hospital. Duplication of any non-JH&FMHN owned key is prohibited without prior written authorisation from the owner of the key.

2.3.5 Administration Centres

Office Managers are responsible for:

- Maintaining a key register
- Managing issuance, transfer and return of keys and proximity cards
- Updating security key pads where applicable

3. Definitions

Must
Indicates a mandatory action required that must be complied with.

Should
Indicates a recommended action that should be followed unless there are sound reasons for taking a different course of action.

4. Legislation and Related Documents

JH&FMHN Policies and Guidelines	1.364 *Sydney Sobering Up Centre Service Provision* 5.002 *Access to the Forensic Hospital* and JH&FMHN policy 5.005 *Alarm, Pager & Two-Way Radio Use and Management, Forensic Hospital.* 5.135 *Security Risk Management* *JH&FMHN Medication Guidelines*, April 2015
NSW MoH Policy Manuals	Protecting People and Property - NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies, June 2013
PPP Partners	G4S Security *Emergency Orders* manual, Emergency Order No.6 Key Bunch Compromise