INTERNAL ONLY

ISLHD PROCEDURE COVER SHEET

NAME OF DOCUMENT	Security of ISLHD Property and Assets
TYPE OF DOCUMENT	Procedure
DOCUMENT NUMBER	ISLHD CORP PROC 63
DATE OF PUBLICATION	August 2021
RISK RATING	High
REVIEW DATE	August 2023
FORMER REFERENCE(S)	ISLHD OPS PROC 63
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Executive Director Strategic Improvement Programs
AUTHOR	ISLHD Security and Fire Safety Manager
KEY TERMS/DEFINITIONS	Property, assets, security, documentation, risk minimisation, theft **Assets-** an item of property owned by a person or company, regarded as having value **Attractive Assets**- Assets of high value and easily accessed **CPTED-** Crime Prevention Through Environmental Design **MRN-** Medical Record Number **ICAC**- Independent Commission Against Corruption
FUNCTIONAL GROUP OR HUB	District Wide
NSQHS STANDARD	Standard 1
SUMMARY	Protecting People and Property: MoH Policy and Standards for Security Risk Management in NSW Health Agencies establishes standards for Security Risk Management in NSW Health Agencies. This procedure details steps for all managers and supervisors to follow to minimise the potential for theft and / or wilful damage of ISLHD assets / property. All staff should embed security into their normal daily work practice.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

Feedback about this document can be sent to ISLHD-CorporateGovernance@health.nsw.gov.au

Security of ISLHD Property and Assets — ISLHD CORP PROC 63

1. POLICY STATEMENT

This procedure relates to Protecting People and Property: MoH Policy and Standards for Security Risk Management in NSW Health Agencies IB2013_024.

ISLHD is required to ensure that all potential for theft and wilful damage is identified, assessed, eliminated where reasonably practicable or at least effectively minimised where elimination is not possible.

2. BACKGROUND

The Protecting People and Property manual outlines standards which must be implemented. The Chief Executive and Executive have the overall responsibility of ensuring the protection of ISLHD's assets – people, property, information – from theft or wilful damage, however all employees have a responsibility for security at all times.

3. RESPONSIBILITIES

3.1 Employees will:

- Be security aware at all times and report any suspicious activity.
- Conduct 'out of office' or 'close of business checks' i.e. make sure desk / work area is cleared of all items such as portable expensive equipment or 'attractive' assets, and lock away.
- Check doors to offices / work areas are locked.

3.2 Line Managers will:

- Co-ordinate risk assessments in their areas of responsibility to identify 'attractive' assets.
- Ensure systems are in place to eliminate or minimise the risk of theft / wilful damage for 'attractive' assets.
- Ensure their employees receive sufficient information to understand their role in protecting ISLHD assets and property, and
- Report any loss immediately to their senior manager and investigate all thefts.

3.3 Network Managers/ Service Managers will:

- Ensure risk assessments are regularly carried out to identify areas where property and assets may be at risk of theft and or damage, and as a result, implement processes to eliminate or mitigate that risk.
- Report any theft to the relevant Tier 2 who will follow the documented process for these circumstances. All thefts will be investigated and Reported to NSW Police.

4. PROCEDURE

4.1 Asset and Property Registers

- District Fixed Asset Registers must be kept up to date providing full descriptions of each item, including serial numbers.
- Donated items or equipment of historical value is to be recorded in the relevant site or services assets register.

4.2 'Attractive' portable asset Registers

An 'attractive' asset as per the NSW Health Accounting Manual for Public Health Organisations includes such items as laptops, mobile phones, expensive trade equipment, safes, copiers, dictating machines, works of art and technical equipment.

The following standards must be implemented unless a risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk):

- Keep assets and property registers up to date, providing full descriptions of each item, including serial numbers.
- Keep a separate register of donated items, equipment of historical value, antique furniture, or other items of historical, heritage or cultural significance.
- Keep a register of property theft and wilful damage to assist with identifying problem areas or patterns of behaviour.
- Investigate all theft.
- Identify all assets with a unique physical marking, such as bar code, micro dot systems, digital photography, Nano marking, invisible marking pens or chemical identification. This includes items of historical, heritage or cultural significance which should be invisibly coded.
- Store attractive portable items separately in a locked area. Only designated staff should have access.
- Enforce an effective key control program (for more information refer to Chapter 10 of Protecting People and Property Manual).
- Utilise CCTV monitoring of identified high risk areas.
- Install alarm systems (refer to Chapter 11 of Protecting People and Property Manual).
- Ensure effective perimeter and internal access control (refer to Chapter 9 of Protecting People and Property Manual).
- Ensure CPTED principles are applied when designing/refurbishing facilities (refer to Chapter 4 Protecting People and Property Manual).

- Reduce risk of theft by ensuring that obsolete equipment with no historical value is written off and disposed of correctly and promptly.
- Where items of historical, heritage or cultural significance are displayed, and where practicable, ensure that display cabinets are secure with shatterproof glass, secure locks and, where risk assessment indicates a need, alarms that respond to any breach of locks or glazing. The cabinets should be under camera surveillance and located in high traffic areas to reduce opportunities for unobserved theft.
  Install security screens in areas that are not continually staffed, e.g. reception areas, so that valuables such as telephones and computers are secure.

4.3 Engineering/Maintenance:

- Ensure controlled access to areas where tools or equipment are stored.
- Brand or stencil all tools or equipment to show ownership.
- Ensure that vehicles are parked away from storage areas to reduce opportunities to steal items.
- Maintenance Manager and Staff are to conduct regular checks of Maintenance Equipment.

4.4 Transport

- Only purchase vehicles with a locked petrol cap cover and inbuilt security devices (e.g. data dot technology, ignition locks).
- Regularly monitor vehicle running petrol sheets purchase details and comparing them to distance travelled.
- Where practicable ensure that vehicles are securely garaged or parked in compounds. Garages and compounds should be subject to security inspections on a regular basis.
- Ensure that any quiet sounding vehicles (Electric and Hybrid) are correctly turned off before exiting the vehicle.
- Ensure that all property transported in vehicles (e.g., laptops) is removed or secured when the vehicle is unattended.

4.5 Laundry

- Ensure deliveries are met and signed for.
- Check delivery weights (quantities) against delivery dockets.
- Check account delivery amounts and quantities against Linen Service records for correctness.
- Ensure linen is not left on open trolleys in areas where it can be stolen if left unobserved, for example on loading docks, infrequently used corridors or corners, or unsecure bays. Where practicable, linen should be stored in a lockable room or linen bay.

- Ensure that vehicles are parked in areas away from the linen supply area.
- Ensure that individuals do not take bags into the linen supply area.
- Undertake spot checks of facility areas which have been allocated linen to look for:
  - Excess stock, above the agreed impress levels.
  - Shortage of stock.
- Ensure that soiled linen bags are not left outside wards or in easily accessible positions.
- Ensure babies are not discharged in NSW Health Agency clothing or blankets.

4.6 Catering

- Regularly reviewing work areas and levels of stores held, querying large stocks.
- Check supplies ordered against menu cycle to determine if quantities ordered are comparative with the menu cycle.
- Check comparable deliveries for quantity, quality and delivery dockets signed. Deliveries should be immediately moved to secure storage areas.
- Ensure that fridges and store areas are locked at all times and only opened to take supplies necessary for the meal that is to be cooked. Ideally the store should then be locked. Consider installing time delay alarms to alert when a door is not secured or is opened without authority.
- Ensure that lockers are provided for staff personal bags and that these are not stored in kitchen areas.
- Restrict the amount of food retained in the kitchen to minimum quantities.
- Do not allow leftover food to be taken home. This can cause over-cooking to create a surplus and encourages taking more than just leftovers. Ensuring additional meals that may be diverted for non-patient consumption are not provided as part of the meal run.
- Prevent unauthorised access to the kitchen. Persons are not allowed in the kitchen area unless accompanied by a senior kitchen staff.
- Ensure that all stores and fridges are locked when maintenance work is being carried out.
- Regularly check trolleys used to transport food from the kitchen for food or other goods that should not be there.
- Ensure that stocks of food held in wards are kept to a minimum.
- Ensure vending machines are in high traffic/populated areas to create a passive surveillance situation.

4.7 Facility Register to record all thefts / property damage

- All thefts will be reported to the onsite Site Security where a Security HandiData Report will be kept as a permanent register of all instances of theft. This is to enable identification of any patterns associated with these thefts e.g. date / time, location.
  Theft also to be reported to the Manager

4.8 Stores

- Educate relevant staff to ensure they are aware of stock control procedures for incoming and outgoing goods.
- Conduct stock takes of consumable stores and check all items listed in the assets register - both quarterly and when there is a change of management.
- Keep stock levels to workable minimums.
- Check invoices against the stock card to ensure goods received are marked on records, and requisitions for store goods against stock cards.
- Conduct physical checks to look for broken packages or seals, and to ensure that bottom packages of large stocks have not been tampered with.
- Prohibit bags being taken into the store area.
- Lock away items such as batteries.
- Ensure that stocks held in areas are securely stored and not easily accessible to patients and unauthorised staff. Where possible, ward stores need to be locked and accessible only to the nurse or unit manager or their delegate.
- Regularly review impress system to ensure stock levels are appropriate.
- Ensure stores returned dockets are used and signed by the ward area if goods are returned from areas to the store.
- Ensure that goods being delivered to facility areas are not left in accessible places and vehicles are not left unattended. Goods received should be immediately located in a secure area.
- Ensure that goods to be delivered to facility areas are receipted/signed for with copies of signed paperwork kept with facility and stores area.
- Ensure that only authorised persons are allowed in store areas.
- Ensure that stocks held in areas are securely stored and not easily accessible to patients and unauthorised staff.

4.9 Administration

- Secure administration areas to prevent access to unauthorised persons.
- Ensure that the administration area is not left unoccupied during work hours or secure the area if it is to be left unoccupied.
- Keep records containing sensitive information secured at all times. They should only be made available to authorised persons.
- Ensure laptop computers are password protected and securely stored when offices are left unattended.

4.10 Mail Deliveries

- Ensure receptacles for mail are clearly labelled and cannot be accessed or opened by unauthorised persons.
- Ensure deliveries of mail are made in a restricted, defined area with appropriate access control.
- Ensure staff pigeon holes are in secure areas accessible only by staff.
- Keep registered mail/couriered packages separate from other incoming mail and establishing procedures for receiving and promptly securing registered mail/couriered packages.
- Ensure that incoming mail (including registered mail/courier packages) is kept in a secure location to prevent loss and unauthorised access until it can be delivered to the addressee.
- Limit the access to the mail areas or use a sign-in access card system.

4.11 Patient Property

- In general, patients should be encouraged / advised not to bring money or valuables with them when being admitted to an ISLHD facility.
  Where ISLHD is requested to provide safe custody for any money or valuables of a patient, please refer to the Patient Valuables Policy (ISLHD CORP PD 44).

4.12 Staff Property

- Discourage staff from bringing large sums of money, personal documents or belongings into the workplace.
- Ensure that staff are provided with a lockable storage area (e.g., individual locker or cupboard) for safe keeping of their property.
- Ensure car parks have good lighting and camera surveillance to deter theft and vandalism.
- Signpost areas such as locker rooms and cafeterias to warn staff to keep their valuables secure.

5. REFERENCES

- Protecting People and Property: MoH Policy and Standards for Security Risk Management in NSW Health Agencies IB2013_024

6. REVISION & APPROVAL HISTORY

Date	Revision No.	Author and Approval
February 2014	0	Manager Corporate Compliance Approved for publishing by ISLHD Director Finance
July 2017	1	District Manager Security & Fire Safety
August 2018	1	Approved by Executive Director Corporate Services, Assets and Chief Financial Officer
September 2021	2	**Author:** District Fire & Security Manager **Approval/Date:** Corporate Policy Recommendation committee/ August 2021 **Approval/Date:** Executive Director Strategic Improvement Programs / September 2021