SESLHD PROCEDURE COVER SHEET

NAME OF DOCUMENT	Security Management within SESLHD Facilities
TYPE OF DOCUMENT	Procedure
DOCUMENT NUMBER	SESLHDPR/639
DATE OF PUBLICATION	July 2023
RISK RATING	High
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standards: Standard 1 – Clinical Governance Security Improvement Audit Tool
REVIEW DATE	July 2025
FORMER REFERENCE(S)	Nil
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	General Manager, Corporate Services
AUTHOR	Manager Health Safety and Wellbeing/Close Associate, Master Security Licence Rosanna.Martinelli@health.nsw.gov.au
POSITION RESPONSIBLE FOR THE DOCUMENT	SESLHD Head of Security Services/Close Associate, Master Security Licence diane.odonaghoe@health.nsw.gov.au
FUNCTIONAL GROUP(S)	Workplace Health and Safety
KEY TERMS	Security, risk management, access, property, safety
SUMMARY	An operational overview of how SESLHD manages the security of its assets, people and patients and an overview of the obligations of SESLHD staff in ensuring the standards of the NSW Health Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in NSW Health Facilities manual are met.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

Feedback about this document can be sent to SESLHD-Policy@health.nsw.gov.au

Contents

1. POLICY STATEMENT

The purpose of this procedure is to provide an operational framework for SESLHD Facilities and Services to implement the salient requirements of the NSW Health Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in NSW Health Facilities manual.

SESLHD is committed to providing an effective security risk management program across the District.

2. BACKGROUND

The NSW Health Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in NSW Health Facilities manual (Protecting People and Property manual) outlines the security standards for NSW Health Agencies to maintain an effective security risk management program.

The standards outlined in the Protecting People and Property manual must be implemented within SESLHD, unless a risk assessment determines that an alternative or additional control is required. This procedure documents the local implementation processes within SESLHD to ensure the standards are met.

This procedure should be read in conjunction with the Protecting People and Property manual.

2.1 Definitions

Keys: refers to metal keys, electronic keys, swipe, electronic access cards and keypad codes.

Multidisciplinary response/team means a group of sufficient numbers of clinical, security and other staff, with a delegated clinical leader, who are skilled and trained in Category 3 of the NSW Health Prevention and Management of Violence Training Framework.

Non-capacity patient: means a patient assessed by a medical practitioner as incapable (either temporarily or permanently) of giving consent to urgent and necessary medical treatment to save the life of the patient or to prevent serious damage to the patient (see Section 4.5.6).

Other duty holder: means another person (or organisation) who concurrently has a duty for the same health and safety matter as the NSW Health Agency e.g. Labour Hire Companies, building /service contractors, retail stores, lessors (referred to in the Work Health and Safety Act 2011, Section 16). Each duty holder must comply with that duty to the standard required by WHS Act, even if another duty holder has the same duty.

Restraint: means the interference with, or the restriction of, an individual's freedom of movement and / or behaviour through the use physical means, including manual restraint, use of a mechanical device or removal of a mobility aid.

Security: is the protection of a person from violence, threats and/or intentional harm; the protection of information from unauthorised disclosure, and the protection of property from intentional damage and from theft.

Staff: anyone who carries out work for a NSW Health Agency including:

- employees
- contractors, including visiting practitioners
- sub-contractors
- employees of contractors and subcontractors
- an employee of a labour hire company e.g., agency staff
- volunteers
- an apprentice or trainee
- work experience students

Anyone who carries out work for NSW Health Agency is given the legal status of 'worker' under the Work Health and Safety Act 2011, Section 7.

Violence: is any incident or behaviour in which staff feel abused, are threatened or assaulted in circumstances arising out of, or during, their employment including verbal, physical, psychological or emotional abuse, threats or other intimidating behaviours, intentional physical attacks, aggravated assault, threats with an offensive weapon, sexual harassment and sexual assault.

3. RESPONSIBILITIES

3.1 Employees will:

- Wear their staff identification at all times while at work
- Adhere to local security procedures and processes for security and access control
- Participate in consultation regarding security matters
- Report security-related matters and incidences to their line manager
- Attend security-related training
- Where assigned to a Code Black team, respond to all incidences as per their designated role.

3.2 Line Managers will:

- Ensure compliance with local security procedures and processes
- Consult on security matters with staff, security staff, Health Safety and Wellbeing Advisors and other duty holders
- Keep staff informed of personal and property security policy and procedures and management action in response to hazard and incident reports
- Identify areas where personal and property security can be improved in consultation with staff
- Respond to incident and hazard reports
- Implement risk control strategies to improve security within the Department/Service.
- Implement the measures for key control in their department as outlined in Section 4.10

- Identify staff training needs in relation to security
- Report security related incidents to the General Manager/Service Director.

3.3 Security staff and Health and Security Assistants (HASAs) will:

- Take personal responsibility to maintain currency of their security licence and First Aid Certificate
- Maintain knowledge of relevant legislation and security-related policies and procedures (e.g., patient restraint)
- Respond to security-related requests in a timely manner
- Record all security-related incidences on the security incident report (for example, *Handidata*) and in the Incident Information Management System (IIMS+)
- Prepare reports and recommendations on security matters for the facility/service
- Undertake security audits and inspections
- In addition, senior security staff will attend and advise on committees and workgroups to consult on security matters related to the construction or refurbishment of premises, changes to equipment, and changes to systems of work.

3.4 Head of Security/Facility Security Managers will:

Ensure the ongoing implementation of an effective security program at their facility or sites, including:

- The appointment of suitable numbers of qualified and licenced security personnel (as deemed from ongoing risk assessments of security incidences and risks)
- Effective operational Code Black procedures involving a multi-disciplinary response of appropriately trained personnel.
- The ongoing maintenance of installed systems to support the site security, including but not limited to CCTV, access control, alarms, general lighting
- Appropriate consultation, reporting and escalation of incidents to:
  - the Chief Executive
  - General Managers
  - Emergency Services
  - any relevant external agencies such as SafeWork NSW and the Environmental Protection Authority

3.5 Clinical staff will:

- Attend to all responsibilities as a staff member as outlined in Section 3.1 of this procedure.

4. PROCEDURE

4.1 Security Risk Management

All reasonably foreseeable security related hazards in clinical and non-clinical environments within SESLHD are identified, assessed, managed and monitored as per SESLHDPR/212 – Health, Safety and Wellbeing Risk Management procedure.

The WHS & Security Risk Assessment form (**Appendix A**) is utilised to document specific security-related risks, and the associated controls, and form part of the relevant Departmental Risk Register.

Security-related risks, incidences and trends are tabled at the facility and service health and safety committees. Security related risks that cannot be effectively mitigated at the department or facility level are escalated via the SESLHD Enterprise Risk Management System (ERMS).

All facilities and larger services undergo the NSW Health Security Improvement Assessment Tool audit on a biannual cycle.

The SESLHD Security Risk and Governance Committee is the peak committee within the District for collaborating and sharing information between clinical, work health and safety and security personnel on security matters. The Committee also considers District-wide strategies to address emerging concerns and trends.

The SESLHD Security Risk and Governance Committee reports through to the SESLHD Executive Council, including the outcomes and progress with action plans arising from the Security Improvement Assessment Tool audits.

4.2 Security Risk Management responsibility

The Audit and Risk Sub-committee of the SESLHD Board receives periodic reports on the security risk management within SESLHD. Where deemed necessary, the Audit and Risk Sub-committee will provide high-level recommendations to the District.

The SESLHD Chief Executive is responsible for ensuring an effective security risk management system that meets the NSW Health security risk management standards outlined in the Protecting People and Property manual. To this end, the Chief Executive has appointed the Director, Corporate and Legal Services to hold the Master Security Licence, and delegated the responsibilities for implementing the security risk management system to the Director, Corporate and Legal services and the Head of Security Services.

The Head of Security Services is responsible for ensuring the ongoing implementation of an effective security program, as outlined in Section 3.4 of this procedure.

Security staff and Health and Security Assistants responsibilities are outlined in Section 3.3 of this procedure.

4.3 Ongoing review and continuous improvement of Security Risk Management

Opportunities for continuous improvement in security risk management is formally supported by the biannual implementation of the Security Improvement Assessment Tool (SIAT).

Health Safety and Wellbeing coordinate the program of SIAT audits across SESLHD. Trained auditors include Security personnel and Health Safety and Wellbeing Advisors.

The SIAT audit identifies areas of non-compliance with the security standards in the Protecting People and Property manual and includes recommendations to improve performance.

Following the audit completion, the Head of Security Services is required to support the facility/service to address the non-compliance areas through the development of a Security Improvement Plan with defined targets and outcomes, using the risk levels of each non-compliance as a guide to the prioritising of the remediation.

Progress of the facility/service in addressing the Security Improvement Plan will be reported to the facility/service executive and the Audit and Risk Committee

Informal continuous improvement opportunities are identified at the Facility/Service through the normal work health and safety risk management process as outlined SESLHDPR/212 – Health, Safety and Wellbeing Risk Management procedure.

4.4 Security Education and Training

The Security Workforce and Development Manager will coordinate a Training Needs Analysis for staff in high-risk areas, specialist roles and Security staff on a biannual basis, in accordance with the NSW Ministry of Health Policy Directive PD2017_043 - Violence Prevention and Management Training Framework for the NSW Health Organisations.

Managers within these high-risk areas will assist with the training needs to ensure the staff in the workgroups are appropriately targeted based on roles and locations.

Reviews will be conducted and include an evaluation of the effectiveness of security-related education and training by reviewing the number and outcome of security-related incidents; staff participation and competency in Code Black responses; the identification and mitigation of security hazards; and staff awareness of security-related procedures and protocols.

Identified high risk areas within SESLHD include:

- Cashiers and Pharmacies at all sites
- Emergency Departments at Prince of Wales Hospital, Sydney, Children's Hospital (Randwick), St George Hospital and Sutherland Hospital
- Inpatient Mental Health facilities
- Outpatient and Community Mental Health facilities
- Neurological/brain injury wards at Prince of Wales Hospital
- Dementia wards at Prince of Wales Hospital, St George Hospital, Sutherland Hospital and the Garrawarra Centre
- Adolescent Mental Health Unit and Child Protection Unit at Sydney Children's Hospital (Randwick)
- Newborn Intensive Care Unit and Assumption of Care Unit at the Royal Hospital for Women
- Outpatient and Community Drug and Alcohol Services

Specialist roles identified for security training include:

- Supervisors and managers of high-risk areas (as listed above)
- Code Black team personnel (clinical and non-clinical staff)
- Security staff and Health and Security Assistants

- Security managers
- Health Safety and Wellbeing Advisors
- Fire Wardens
- Health and Safety representatives

A training matrix for staff in specialist roles, high risk areas and Security personnel is located at Appendix B. Training for these staff will be provided prior to commencement or as soon as possible after commencement, of duties appropriate to their role and consistent with NSW Ministry of Health Policy Directive PD2017_043 - Violence Prevention and Management Training Framework for the NSW Health Organisations.

4.4.1 Code Black training

Staff identified as Code Black or duress responders to a clinical or corporate/security incident are provided with specific training by the site.

The Code Black training includes:

- the process for duress response
- assessing a scene
- verbal de-escalation and negotiation skills and evasive self-defence
- physical restraint techniques
- use of mechanical and other restraints where appropriate and approved for use
- associated legal implications

Code Black training (excluding physical restraint training) is coordinated at the site level.

Refresher training for Code Black or duress responders is conducted on at least an annual basis.

4.4.2 Emergency Department Violence Prevention Management training

The Emergency Department Violence Prevention Management (EDVPM) training program is coordinated through Organisational Development and Learning. Training is held at Sydney/Sydney Eye Hospital, Prince of Wales Hospital, St George Hospital and The Sutherland Hospital.

New staff to the Emergency Departments are required to be enrolled within three months of their commencement of duty. Enrolment is via *My Health Learning - Emergency Department Violence Prevention Management (EDVPM) Learning Pathway.*

Refresher training in EDVPM is available to staff of the Emergency Departments, via one-hour in-service modules, coordinated through Organisational Development and Learning.

4.5 Role of Security staff in SESLHD

Each SESLHD facility will periodically review the level of security staffing through a documented risk assessment. The review shall consider the identified risk of security/violence occurring, the size of the facility, the services being provided and the local demographic.

Refurbishment or redevelopment of SESLHD facilities, particularly a planned increase in the size or number of buildings and services on site, will trigger a review.

Consultation with staff and other duty holders at the premises is required as part of the review. IIMS and the security incident report information may inform the review.

4.5.1 Position Description

SESLHD Security Officers and Senior Security Officers work to a standardised position description, consistent with the scope outlined in NSW Health Protecting People and Property – Chapter 14 (**Appendices C and D**).

Health and Security Assistants also work to a position description that reflects aspects of Chapter 14 of NSW Health Protecting People and Property.

4.5.2 Contract security staff

Use of contract security staff is kept to a minimum through effective rostering and recruitment processes.

Contract security staff are only utilised for “specialling” patients in specific circumstances and units as authorised by treating teams and relevant service managers.

Where contract security staff are used, the authorising SESLHD manager will be responsible for ensuring the company is current in the contractor management database.

The contract security company must provide a current copy of their Master Security Licence in line with the services being provided and either a copy of company’s security officer’s licence register or a copy of the security licences for the individual security officer who will be working on SESLHD premises.

Where contract security staff are required, the following is implemented to reduce the specific risks associated with their use:

- Contractors are provided with training on the role of security staff in Health prior to commencement
- Their details are added to the site security sign-on register
- Standard Safe Operating Procedures are explained to contract staff
- Contractors are provided with written flyer of duties
- Handover conducted with nursing staff

4.5.3 Security licences and registers

Every manager of Security and Health and Safety Assistants (HASAs) in SESLHD is to obtain current copies for security licences and first aid certificates, along with maintaining a register of the full name, licence number, expiry of licence, and subclass of each class 1 or class 2 licensee employed or contracted to the department. The manager will check licences at least monthly for currency.

A daily sign-on register is also maintained as per the Security Industry Regulation 2016 Clause 35.

Every SESLHD Security Officer will wear his or her licence on his or her person so as to be clearly visible while on duty, as per the Security Industry Act 1997 Clause 36

Every SESLHD Security Officer is responsible to ensure they maintain a current security licence with the appropriate class for the work they are employed along with a current First Aid certificate HLTAID003 (Provide first aid) or HLTFA311A (Apply First Aid).

SESLHD Security Officers must immediately report to their manager if at any stage that licence or first aid certificate becomes suspended or revoked during the licence term (length of licence).

4.5.4 Escalation processes for security incidents

All security-related incidents are recorded in the security incident report (for example, *Handidata*) and on IIMS+. A review of the incident may inform improvement plans or changes in practice or procedure to mitigate a repeat of the incident.

Where the incident relates to a breach or failure in the site's security systems (including factors related to staff expertise, numbers and availability), the incident is to be reported via the Head of Security Services to the facility General Manager/Service Director.

Clinical incidents related to clinical management of a patient or client are escalated to the senior clinician where the incident occurred.

Where the incident involves external parties, such as the response of the NSW Police, a formal debriefing of the incident will occur at the next Police Liaison Committee or Emergency Management Committee of the facility.

There are a number of incidents that must be reported by the Head of Security or their representative (Manager of Security) as soon as practicably to the Master Security Licence which include:

- When a SESLHD licenced security officer has been recorded as having a criminal conviction or their licence suspended
- When a SESLHD licenced security officer fails to maintain a current security licence or first aid certificate.
- A contract security provider has an expired or suspended Master Licence.
- A contract security provider fails to provide a certificate of currency for Public Liability and Workers Compensation.
- A contract security provider supplies unlicensed class 1A security officers.
- Incidents involving firearms or prohibited weapons.
- Where Security Licencing Enforcement Directorate (SLED) contact or attend a site.
- Incidents involving security officers which are investigated by NSW Police or SafeWork NSW.
- Misconduct or alleged misconduct of Security Officers which breach the conditions of their Security Licence or Code of Conduct.
- Prosecution of Security Officers as a result of an incident at any SESLHD site.
- Complaints that have been made to SLED regarding a security officer's behaviour.

The master licence holder will notify the Head of Security Services of any incidents reported to them in relation to conduct, licencing issues of security officers or reports received from SLED. This will include outcomes of any compliance audits of licencing, incidents and sign on registers.

4.5.5 Arresting without a warrant

It is the SESLHD position that if a person is in the act of committing an offence or has been observed committing an offence, that the NSW Police should be called to attend. Security or any other SESLHD staff should not engage or be instructed to engage in a "citizen's arrest".

4.5.6 Absconding patients

Security staff must only assist in stopping a person from leaving a hospital where directed by a health professional, and where the person is lawfully detained as an involuntary mental health patient or a non-capacity patient, and unlawfully attempting to

The role of security personnel is limited to aiding in the prevention of a person's departure from a hospital. This assistance is authorised only when directed by a healthcare professional, and the individual in question is lawfully detained either as an involuntary mental health patient or a non-capacity patient. The situation warrants such action when the person is attempting to unlawfully escape or abscond.

Patients treated under the Mental Health Act who are attempting to abscond from a SESLHD Mental Health facility are managed in accordance with SESLHDGL/082 - Clinical Risk Assessment and Management – Mental Health.

Security staff must not prevent any other patient (not lawfully detained under the Mental Health Act or defined as a non-capacity patient) from leaving any SESLHD premises.

4.5.7 Use of Weapons by Security Staff

No Security staff in SESLHD are issued with weapons such as batons and handcuffs. Violence risk control strategies within SESLHD are cognisant that no weapons are available to or will be used by Security personnel.

4.6 Security Risk Management in the planning process

Security risks may be inherent in plans and proposals such as construction or refurbishment of premises, changes to equipment, and changes to systems of work such as models of care.

The leads or coordinators of plans and proposals within SESLHD (such as the Director of Capital Works and Redesign, General Managers, Clinical Managers and Department heads) must ensure Corporate and Security representatives are included as members of committees and workgroups to consult on security matters related to the construction or refurbishment of premises, changes to equipment, and changes to systems of work.

Where security risks are identified, the assessment of the security risks and strategies to eliminate or minimise the risks must be documented as part of the planning process (such as the service development plan, business plan, disaster/emergency planning, project definition planning and procurement processes).

4.7 Health Facility design

4.7.1 Security risk assessments

Security risk assessments must be completed and documented as part of facility planning, design, refurbishment and prior to engaging in any significant reorganisation of the physical working environment.

These risk assessments must form part of the formal business documents related to the facility planning, design, refurbishment or reorganisation.

Evidence of consultation with Health Safety and Wellbeing Advisors, Corporate and Security representatives and other duty holders where applicable (such as Ambulance Services) must be included in the risk assessment.

4.7.2 Implementation of Security standards

The standards outlined in the Australasian Health Facility Guidelines and the Protecting People and Property manual are referenced and compliance achieved during all stages of the facility planning, design or the refurbishment process.

Senior security personnel and Health Safety and Wellbeing Advisors must be consulted in ensuring the security standards are met, as well as the four *Crime Prevention through Environmental Design* (CPTED) principles of territorial reinforcement, surveillance, space management and access control, during all stages of the facility planning, design or the refurbishment process.

New development or refurbishment specifications in SESLHD buildings are to meet the standards as outlined in the Protecting People and Property manual:

- Doors and windows - Chapter 9
- Access and egress control – Chapter 9
- Duress alarm systems – Chapter 11
- External and internal lighting – Chapter 12
- Car parks – Chapter 19

In particular, new emergency departments being planned must comply as far as practicable with Parts B and C of the Australasian Health Facility Guidelines and with other NSW Health standards set out in the Protecting People and Property manual.

Signs (and floor markings where appropriate) must follow the requirements set out in NSW Health Information Bulletin IB2022_048 Wayfinding for Healthcare Facilities.

4.8 Health Service leasing of property to or from external parties

Before a premises is leased from an external organisation, a security risk assessment must be undertaken in consultation with staff and other duty holders. Any property leased by SESLHD must meet the security standards set out in the Protecting People and Property manual prior to occupation by SESLHD staff.

The risk assessment must document that staff who will occupy the premises have been adequately consulted with respect to security concerns.

The lease must specify the responsible parties for the security related items, such as the installation and maintenance of security grills, locks, alarms and lighting.

A Business Continuity Plan must be developed, detailing how any foreseeable issues arising with the occupation of the leased premises will be addressed.

4.9 Access and egress control

Access and egress controls in SESLHD premises are supported by a risk assessment (the WHS & Security Risk Assessment form – Appendix A) and developed in consultation with staff and other duty holders at the premises, and in accordance with the standards outlined in the Protecting People and Property manual (Chapter 9).

Each SESLHD facility and service has documented procedures or business rules, which include the identification and roles of key authorised staff for the following:

- Remote locking of the emergency department
- Personal identification of staff and access to Facility buildings and areas
- Facility lockdown
- Securing and control of building perimeters, including doors and windows
- Control of access to and egress from the land controlled by the facility or service
- Safe access and egress after hours and during emergencies
- Controlling access to vulnerable areas and securing vulnerable patients
- Applying the principles of Crime Prevention Through Environmental Design

Staff only areas have signage clearly identifying these areas as staff only, be access controlled and fitted with fixed duress alarms.

4.9.1 Identification Cards and Name Badges

All staff of SESLHD are provided with a photo identification card on commencement of employment. Staff are also provided with a NSW Health name badge that includes at least their first name, and position. The name badge is to be worn at chest height at all times while on duty.

Name badges are ordered through Minit Commercial (SESLHD-F027 Staff Identification Badge Order form).

Security staff and Health and Security Assistants will display their full licence while on duty in accordance with the Security Industry Act 1997, Section 36.

4.9.2 Photo Identity/Access Systems

In SESLHD facilities, the Security Department is responsible for maintaining the Photo Identity/Access system for staff and volunteers.

The facility executive determines the level of access to be granted to each staff member or volunteer as per their role and responsibilities. This includes locums and casual staff, and Code Black team members.

Each facility also determines the local process for verifying the identity of staff or volunteer, their level of access to the facility, and the period of access.

All volunteers are required to have a StaffLink number and are identified by their photo ID including a large V or the word Volunteer on their card.

Separation of staff and volunteers

As part of the separation procedure for volunteers or staff resigning from SESLHD or transferring to another facility, line managers are responsible for collecting and returning the photo identification card and access card for former volunteer/staff to the Security Department within a week of their resignation/transfer.

Review of Access

Security are responsible for updating the records in line with the movement of staff and volunteers to/from the facility.

Security will also review access records on a periodic (at least six-monthly) basis to determine where issued access cards are not being used, and follow-up with the Department manager as required.

4.10 Key control

Each facility will determine and document the authorised person to hold and control the issue of keys. In large facilities, this is usually the Security Department.

Departmental Managers are also responsible for managing the control of keys to their unit/department. A risk assessment conducted in consultation with staff will inform the Department in documenting the procedures to minimise risks associated with the issuing, returning and storage of keys.

4.10.1 Key Storage

Keys that are not issued are to be stored in locked container in an area out of sight of unauthorised persons.

4.10.2 Key Authority Record

All personnel authorised to draw and return keys must have their name printed and a specimen signature recorded.

4.10.3 Key and Security Log

A log of keys issued is kept and reviewed at least on an annual basis. The key log should also be updated as staff cease or commence employment in the facility and department.

4.10.4 Cutting of Additional or Replacement Keys

Staff are not permitted to cut keys to their office or work environment. The facility will engage an authorised locksmith to cut keys. Contact the Security Manager (or facility manager) to arrange for the cutting of additional keys.

4.10.5 Keypad Access Codes

Keypad access codes are only provided to those persons with a legitimate reason for access. Keypad access codes should be changed every six months (or sooner if needed) to prevent compromise of the facility or department.

4.11 Duress alarm systems

4.11.1 Risk assessment and review

Each SESLHD facility will ensure a documented risk assessment is undertaken at least biannually to review the alarm system. The risk assessment will be conducted in consultation with staff (including those working in high-risk areas for violence) and consider:

- Back-up in the event of system power failure
- Strategic locations for fixed alarms
- Mobile duress alarms for staff working in high risk or isolated positions within the facility
- Mobile duress systems for staff regularly working offsite i.e., community health staff
- Training and information requirements for staff.

Redevelopment or refurbishment of the facility must include a review of the risk assessment, to ensure the alarm system meets the additional requirements.

Mobile and fixed alarms used in SESLHD facilities will adhere to the feature requirements outlined in Chapter 11 of the NSW Health Protecting People and Property manual.

4.11.2 Mobile duress alarms

All staff working in an emergency department must wear a mobile duress alarm while on duty.

Mobile duress alarms are also provided to staff working in high risk or isolated positions, as determined by a risk assessment.

Training in the wearing, testing and use of the mobile duress alarm will occur during induction.

<u>Testing of mobile duress alarms</u>

Each department issuing mobile duress alarms must establish a procedure for staff that includes:

- Testing the mobile duress alarms at the beginning of each shift.
- Recording the tests on a testing log.
- Reporting faults, and notifying staff of faulty alarms

4.12 Lighting

Each SESLHD facility will ensure a documented risk assessment is undertaken at least biannually to review the internal and external lighting. The risk assessment will be conducted in consultation with staff, and ensure the standards documented in Chapter 12 of the NSW Health Protecting People and Property manual as follows:

- The minimum standards have been implemented for internal lighting
- Special lighting has been installed in areas such as entrance foyers, emergency departments, staff entry and exit points, pharmacies and car parks.
- External lighting is sufficient to eliminate dark areas and allow facial recognition to facilitate correct functioning of CCTV cameras.

4.13 Workplace camera surveillance

Refer to SESLHDPR/626 - Closed Circuit Television – management and operation of in SESLHD Facilities.
Security staff operating or monitoring the closed-circuit televisions in SESLHD are provided with local induction and training in responding to events and requests for information.

4.14 Physical and mechanical restraint

4.14.1 Patient physical restraint

SESLHDPR/483 - Restrictive practices with adult patients
SESLHDBR/014 - Prone Restraint Restriction for the Mental Health Service (MHS)
NSW Ministry of Health Policy Directive PD2020_004 - Seclusion and Restraint in NSW Health Settings
Except in certain specified emergency situations outlined in Section 4.14.3 below, a decision to use physical restraint on a patient must only be made by a medical practitioner, or for patients being cared for under the *Mental Health Act 2007*, a registered health practitioner.

Staff who are required to undertake physical restraint in SESLHD must be trained in Module 3 of the Violence Prevention Management program, or the Emergency Department Violence Prevention Management program or the Mental Health Safety for All program.

Physical/manual restraint should be used for the briefest period required, with the least force required, to allow the consumer to safely regain control of their behaviour.

Departments/wards must document each event involving a restraint in IIMS, the patient/consumer health care record, the Restraint Register and the Patient Restraint Chart (MR137).

Additionally, Security staff involved in a physical restraint must record the incident in the security incident report (for example, *Handidata*), as per their security licence obligations.

Following any physical restraint, the department involved in the incident will conduct a debriefing with involved staff.

Sites may develop Clinical Business Rules around local restraint concerns or practices.

4.14.2 Mechanical restraints

Mechanical restraints are used on patients as a last resort, and for the minimum amount of time only. The decision to apply mechanical restraints can only be made by a senior clinician caring for the patient.

Following any mechanical restraint, the department involved in the incident will conduct a debriefing with involved staff.

4.14.3 Security staff role in physical restraint of patients

Physical restraint of patients is led by clinical staff. Security staff may be requested to assist as part of the team involved in the physical restraint of a patient but may not lead the restraint.

Security staff are not to assist in a restraint of a patient where the intended purpose of the restraint is to administer medical treatment, and the patient is legally capable of giving consent to treatment, but who chooses not to have treatment.

Specific emergency situations – only when there are no clinical staff in the immediate vicinity, or clinical staff are unable to issue instructions (e.g., they are themselves injured), may Security staff determine that the use of restraint on a patient is needed to defend themselves or others, and lead the restraint.

4.14.4 Non-patient (visitor, relative) restraint

Where a non-patient is threatening to or actually assaulting a person or damaging SESLHD property, security may determine that physical restraint is required to defend themselves or others and call a Code Black.

Only if there are sufficient numbers of trained Code Black staff available (minimum of four) will a restraint be attempted.

If there are not sufficient numbers of staff available, security will call the Police, and make all attempts to isolate the area, and remove other visitors and staff.

Security departments have Safe Work Practices or Business Rules in place for conducting physical restraints specific to their local arrangements and resources.

4.15 Searching patients and their property

Refer to: SESLHDPR/597 - Client and Patient Safety and Security Searching, SESLHDBR/080 - Search to maintain safety in the SESLHD Mental Health Inpatient Facilities.
When required and authorised, the Client and Patient Safety & Security Search is conducted according to Ministry of Health Policy and NSW legislative requirements.

Appropriately trained and competent clinical and security workers will provide for a safe and healthy work environment during client safety & security searches by removing articles from persons that may cause harm.

Training in client and patient searching is found at My Health Learning.

4.15.1 Suspected illicit or unidentified substances

Where the client has been identified as having possession of, or using, suspected illicit or unidentified substances, local processes should be followed. Refer to:

- Mental Health - SESLHDBR/031 - Illicit substances and/or alcohol and other drugs use within inpatient Mental Health Services
- Prince of Wales/Sydney-Sydney Eye Hospital Clinical Business Rule – Suspected illicit substances and implements associated with their use

4.15.2 Potential or suspected weapons

Where the client has been identified as having possession of a suspected weapon, Security staff are to follow local processes. This may include calling for a Code Black response.

4.16 Escorting individuals (non-patients) from SESLHD premises

If an individual who is not a patient is acting in a manner that is offensive to a reasonable person, or creating a risk for others, then they can be directed to leave the hospital premises.

If they refuse to leave the hospital premises, they should be advised they are in breach of lawful direction and the NSW Police will be called.

If their conduct is deemed unacceptable, and cannot wait until the Police arrive, only persons authorised by the SESLHD Chief Executive, and the facility General Manager/Service Director may escort the individual from the premises.

4.17 Security arrangements for patients in custody

Where the Police or Corrective Services bring patients in custody to SESLHD facilities, the custodial agency is responsible for the secure management of the patient. It is the responsibility of the Police or Corrective Services to have conducted a risk assessment to determine the numbers of their staff required, and their procedures for managing that patient in a manner that does not risk SESLHD staff or property.

The primary role of security when a patient in custody is admitted is to protect SESLHD staff and assets from potential harm, not to guard the patient in custody.

Each SESLHD facility is required to develop local Clinical Business Rules or protocols to address the risks associated with patients in custody. Documented risk assessments should inform and provide the basis of these Clinical Business Rules or protocols. The Clinical Business Rules or protocols must document the following:

- The roles of SESLHD staff and that of the other external agencies
- Providing information to the external agency about the facility WHS arrangements, relevant clinical protocols and evacuation plans
- The process for advising the appropriate staff (e.g., facility manager and security staff) when a patient arrives or is admitted, and potential risks associated with their admission
- Transferring a patient in custody if they cannot be safely managed at that facility
- Identifying when custodial patients are to be placed away from other patients and staff, (e.g., use of a self-assessment room)
- Managing public and media inquiries
- Managing clinical inquiries from Justice Health medical staff

- The process for SESLHD to obtain information about the patient in order that a risk assessment of the individual patient can be made.

SESLHD clinical staff involved with the management of patients in custody must be trained and competent in violence prevention management, restraint techniques, and the use of mechanical restraints.

4.17.1 Patients in the custody of Police

SESLHD facilities must ensure a specific Clinical Business Rule or protocol is established in consultation with security and the Police to outline the transfer of patients in custody to the facility.

The Clinical Business Rule or protocol must ensure the transfer of the patient in custody includes information on potential risks associated with their admission; and that adequate numbers of facility security personnel are available to support the handover to clinical staff while the admission process is taking place.

The SESLHD facility must establish a regular interagency meeting with the Police Local Area Command/s, to develop and communicate the relevant protocols, review incidences and improve the security management of the patients in custody.

4.17.2 Corrective Services patients in custody

Where Corrective Services patients are treated or admitted, the SESLHD facility must make all reasonable attempts to establish a regular interagency meeting with Corrective Services, to develop and communicate the relevant protocols, review incidences and improve the security management of the patients in custody.

The SESLHD facility is to ensure staff are appropriately informed and where required, trained in the requirements for managing patients in custody.

4.17.3 Juvenile detainee patients

Where Juvenile Detainee patients are treated or admitted, the SESLHD facility is to ensure staff are appropriately informed and where required, trained in the requirements for managing this patient group.

If appropriate (as per a risk assessment), an interagency meeting may be established with Corrective Services for this particular group.

4.17.4 Forensic patients transferred from a Mental Health Service

Refer to: NSW Ministry of Health Policy Directive PD2012_050 - Forensic Mental Health Services specifically Guidelines for forensic and correctional patient ground access, leave, handover, transfer and release - Section 9.

SESLHD Mental Health Services will inform security of the impending transfer of the forensic mental health patient prior to the admission occurring. The transfer will include information on the potential risks associated with their admission, and the staffing level required.

Where a forensic mental health patient is being transferred into a SESLHD facility from another local health district or other agency, the SESLHD facility will ensure security is informed of the impending transfer, and that the transferring local health district or other agency provides adequate information on the potential risks associated with their admission, and the staffing level required.

4.18 Security in the clinical environment – Emergency Departments

Emergency Departments (EDs) are to ensure there is a current documented risk assessment, developed in consultation with staff, which identifies, assesses and minimises, or eliminates risks within the ED environment.

EDs are to ensure that where the identified security risks are managed through procedures, the staff are aware of and trained in their roles and responsibilities to manage those risks.

ED staff are responsible for communicating to their colleagues the risks presented by a patient, particularly at handover, and through the patient medical record and alerts.

Protocols for caring for patients identified as being under the National Disability Insurance Scheme includes the completion of a Transfer of Care Risk Assessment where a person with disabilities is a non-planned admission to a ward or department through the Emergency Department.

4.18.1 Main public entry doors to the Emergency Department

The main public entry access doors or each SESLHD ED can be locked/unlocked remotely and are fitted with closed circuit TV monitoring.

ED staff are trained in local protocols for activating the remote locking of the public entry access doors.

4.18.2 Closed Circuit Television in the Emergency Department

CCTV cameras which both record and provide live view, and provide a clear visual image of individuals, are placed in waiting rooms and are positioned to prevent unauthorised access to treatment areas such as tailgating.

CCTV live feeds are available at ED staff stations. The positioning of the CCTV takes into consideration the privacy issues for patients and staff.

4.18.3 Communication with patients (and carers) awaiting care in the Emergency Department

Each ED has processes to provide patients (and carers) awaiting care with regular information on expected waiting times. ED staff are trained in the local processes and their role in communicating this information.

4.18.4 Safe Assessment Rooms

Each ED has at least one Safe Assessment Room, and manages patients with Acute Severe Behavioural Disturbance in accordance with NSW Ministry of Health Guideline GL2015_007 - Management of Patients with Acute Severe Behavioural Disturbance in Emergency Departments.

4.18.5 Clinical protocols for preventing and managing violence

All ED staff are required to be trained in the ED Violence Prevention Management training pathway as soon as possible after commencement.

Each ED has documented local protocols, developed in consultation with staff, for preventing and managing violence.

SESLHDPR/341 - Violence Prevention and Management

4.19 Security in the clinical environment – other clinical areas

Clinical departments and wards are to ensure there is a current documented risk assessment, developed in consultation with staff and other duty holders, which identifies, assesses and minimises, or eliminates risks with in the clinical environment.

Clinical protocols to manage potential, or actual, violence arising from a patient's medical or mental health condition are communicated to staff. The protocols outline the roles and responsibilities of staff and are appropriate to the level of risk.

Clinical department and ward staff are responsible for communicating to their colleagues the risks presented by a patient, particularly at handover, and through the patient medical record and alerts.

Patients identified as being under the National Disability Insurance Scheme are to be managed as per the NSW Ministry of Health Policy Directive PD2017_001 - Responding to the Needs of People with Disability during Hospitalisation.

Patients with Acute Severe Behavioural Disturbance are managed in accordance with NSW Ministry of Health Guideline GL2015_007 - Management of Patients with Acute Severe Behavioural Disturbance in Emergency Departments.

Clinical departments and wards are to ensure that where the identified security risks are managed through procedures, the staff are aware of and trained in their roles and responsibilities to manage those risks. The Training Needs Analysis tool for determining the level of Violence Prevention Management training required for staff is at **Appendix E**.

Clinical departments and wards are also to ensure that staffing levels and skill mix support prompt clinical care, early recognition of potential violence and adequate response to incidents of violence.

4.20 Security in the clinical environment – working in the community

Community-based services and teams are to ensure there is a current documented risk assessment, developed in consultation with staff and other duty holders, which identifies, assesses and minimises, or eliminates, risks of staff working in the community.

4.20.1 Code Black procedures for community-based services and teams

All community-based sites must develop appropriate local Code Black procedures which consider their resourcing, availability of a skilled multi-disciplinary team response and the likely response times of the local Police. Chapter 29 of NSW Health Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in NSW Health Facilities provides information to assist Managers and staff in developing a local Code Black procedure.

The Code Black procedure must also consider the layout and location of the site, ensure safe areas are clearly identified, duress systems and lock down protocols are available, and staff roles and responsibilities are clearly identified and understood.

4.20.2 Home visiting and working off-site

Workers conducting visits in the community face several potential risks to health and safety. Worker's safety is paramount and must always take priority over the need or desire to conduct, or complete, a particular visit or service in the community.

Guidelines for developing and implementing safe work procedures, determining appropriate equipment and communication devices and managing home visiting for staff working off-site are contained in:
SESLHDPR/323 - Working in Isolation Risk Management.

4.21 Remote or isolated work locations

Workers that work alone anywhere onsite within a premises or campus under control of SESLHD, and who are unable to get immediate assistance from colleagues or other people may face a number of additional risks to their health and safety. This includes working in isolated areas onsite either during or outside their usual rostered working hours.

SESLHDPR/323 - Working in Isolation Risk Management assists department managers, in consultation with workers, to implement a range of controls to minimise the risk to those required to work alone.

4.22 Security in Pharmacies

All SESLHD pharmacies are required to maintain a current risk assessment, developed in consultation with staff and other duty holders, which identifies, assesses and minimises, or eliminates, their specific security risks within the pharmacy environment.

Each pharmacy has documented processes for managing security incidences and potential violence.

Pharmacy staff must undertake training in Protection against Armed Hold-up and Robbery (externally sourced course).

4.23 Security of on-site car parking

SESLHD facilities which include on-site car parking are to ensure there is a current documented risk assessment, developed in consultation with staff and other duty holders, which identifies, assesses and minimises, or eliminates, risks with the car parking facilities.

Appropriate lighting levels, access control, CCTV surveillance, signage and after-hours access are to be maintained for all SESLHD car parks. Responsibility for the maintenance of these items are clearly documented. Where the operation of a SESLHD car park is managed or licenced to a third party, the contract must detail the responsibilities for the security arrangements.

Where reasonably practicable, car spaces are allocated for afternoon and night shift staff. Security will provide escorts to afternoon and night shift staff between the Facility and the car park as operational requirements allow – i.e., the staff member may be asked to wait until security personnel are available.

4.24 Security of property

SESLHD endeavours to ensure there is a current documented risk assessment, developed in consultation with staff and other duty holders, which identifies, assesses and minimises, or eliminates, risks of damage or theft of SESLHD assets and property. The following systems are in place to monitor and manage SESLHD property:

- An up-to-date asset register, maintained by the Finance Department
- An up-to-date property register, maintained by Capital Works

Every case of theft, break and entry, motor vehicle impact and malicious damage to SESLHD assets or property must be entered in IIMS and reported to the Police.

4.24.1 Engineering/Maintenance

All SESLHD Engineering and Maintenance Departments ensure the security of tools and equipment through:

- Ensuring staff are aware of their responsibilities for tools and equipment assigned to them
- Controlling access to the department, and keeping an inventory of tools and equipment
- Branding or stencilling all SESLHD tools to show ownership

4.24.2 Motor Vehicle Fleet

SESLHD Fleet Management coordinates the purchase and replacement of vehicles and ensures specifications of each vehicle is appropriate for operational use. This includes regular auditing of vehicle usage and fuel purchases.

SESLHD Facilities and Services are responsible for the secure garaging or parking of fleet vehicles and reporting any loss or malicious damage to vehicles to SESLHD Fleet Management. Fleet parking areas are to be included in regular security inspections.

SESLHD staff are to ensure all property transported in vehicles (e.g., laptops, documentation, clinical kits) is removed or secured out of sight (e.g. in the boot) when the vehicle is unattended.

Refer to: SESLHDPD/285 - Motor Vehicle Policy.

4.24.3 Linen, Catering and Stores

SESLHD facilities and services are responsible for local stock control processes for ensuring all linen, catering and stock deliveries are met and signed for, and stored in secure areas.

Any unaccounted anomalies in linen, catering and stock supply/levels will be investigated. Spot checks of linen and food supplies will assist in checking for unaccounted anomalies.

SESLHD facilities and services shall also ensure patients are not discharged with NSW Health linen or clothing.

Any knives fitting the description of Cleaver, Chef's knife, Paring Knife Carving Knife Utility Knife or Boning Knife must be stored in a dedicated lockable drawer to secure these items when not in use.

Vending machines are located in high traffic areas to deter break-ins and tampering.

4.24.4 Administration, Mail Deliveries and Cash Handling

Administration areas in SESLHD facilities and services are to be always secured when unoccupied, to prevent theft of equipment and security of sensitive information.

SESLHD facilities and services ensure mail is delivered to a secure staff only area with appropriate access control and supervision.

SESLHD facilities and services ensure cash handling, receipting and banking practices are consistent with the NSW Health Accounting Manual for Public Health Organisations

4.24.5 Patient Property

SESLHD provides patients with information before admission on the risk of bringing their own personal property into SESLHD Facilities and Services (Before You Arrive, Staying Safe).

Inpatients are provided with a lockable bedside drawer or closet for storing essential items brought into hospital with them. Routine checking of food trays and linen, for patient property such as hearing aids/dentures occurs at the ward level.

Where SESLHD accepts a patient's property or valuables for safekeeping (such as an emergency admission), the hospital or facility ensures the items are clearly and accurately labelled, and securely stored. Any discrepancies or reports of such valuables or money going missing are fully investigated by the facility, and where required, notifications made to the NSW Police and/or ICAC.

Also see: SESLHDPR/597 - Client and Patient Safety and Security Searching.

4.24.6 Staff Property

Staff are discouraged from bringing large sums of money, personal documents or valuables onto the workplace. Managers are required to ensure each staff member has access to a suitable locker or lockable cupboard for storing their personal belongings (such as a handbag or backpack).

4.25 Security of information

SESLHD has in place procedures and processes to ensure the security of clinical and corporate information.

SESLHDPD/196 - Records Management – describes how all records (paper based and electronic), including administrative, personnel, accounting and health records are to be managed within SESLHD.

SESLHDPR/510 - Managing Secure Organisation Access within Cerner EMR - describes the management of secure organisation access (including approval process for secure organisations) within the Cerner Electronic Medical Record (eMR) suite of applications.

SESLHDPD/288 - Service Continuity Policy for Health ICT Services – describes the governance framework for ICT service continuity management for critical clinical and non-clinical functions.

SESLHDPD/192 - Health Records (paper based) Disaster Management – describes the framework of a Health Records Disaster Plan for paper-based health records.

SESLHDPD/203 - Records Management – Retention Periods – describes how all records produced by SESLHD meet the minimum statutory requirements of the NSW State Records Act 1998.

SESLHDPR/220 - Records Management – destruction of – describes the process within SESLHD to gain authorisation to dispose of records.

4.26 Security of medical gases

Storage and security of bulk and cylindered medical gases are the responsibility of Engineering Services and the loading dock at each site. Access to any storage and gas plant areas is restricted by use of doors, barriers and signs, and secured against unauthorised removal, tampering, vandalism and misuse.

Any theft, tampering or damage to medical gases is reported immediately to the facility General Manager.

Relevant procedures are as follows:

SESLHDPR/431 - Fire Safety Risk Management – includes the emergency response procedures where the fire may involve sites with medical gas storage

SESLHDPR/229 - Transporting of Patients - Risk Management – describes the safe transportation of a patient with medical gas.

SESLHDPR/240 - Decommissioning a Workplace – assists personnel involved in vacating a workplace to ensure all hazards are safely managed or disposed of, including gases.

4.27 Security of radioactive substances

SESLHD has a comprehensive Radiation Safety Plan, found under R on the Policies and Publications intranet page, that addresses all reasonably foreseeable security risks associated with radioactive substances.

4.28 Security risk controls in unplanned events

SESLHD Facilities and Services will maintain local emergency procedures for unplanned events in line with relevant Australian Standards and NSW Health policies.

SESLHDPD/265 - Emergency Management

These procedures must include consideration of the specific security issues around managing and unplanned event, including accounting for staff, patients and other occupants, isolating the scene of the unplanned event, operating the emergency warning system as appropriate, securing against theft, looting or malicious property damage during the event, and managing crowds and traffic until the police can assist.

Each SESLHD facility has a local Emergency Management Committee to oversight the development and review of the local procedures and responsibilities through consultation with staff and other stakeholders in consideration of the relevant Australian Standards and NSW Health policy. Site specific emergency procedures are as follows:

Sydney/Sydney Eye Hospital Emergency Response Manual

Randwick Hospitals Campus Emergency Plan

St George Hospital Emergency Response Plan

The Sutherland Hospital & Community Health Services Emergency Response Plan

5. DOCUMENTATION

Form F384 WHS and Security Risk Assessment Tool

6. AUDIT

Security Improvement Audit Tool – conducted every two years
NSW Ministry of Health Policy Directive PD2021_037 - Security Improvement Audits

7. REFERENCES

Legislation:
Work Health and Safety Act 2011
NSW Security Industry Act 1997
Security Industry Regulation 2016
Australasian Health Facilities Guidelines
Crime Prevention through Environmental Design

NSW Ministry of Health
NSW Health Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in NSW Health Facilities

NSW Health Accounting Manual for Public Health Organisations

NSW Ministry of Health Policy Directive PD2017_043 - Violence Prevention & Management Training Framework for the NSW Health Organisations

NSW Ministry of Health Policy Directive PD2020_004 - Seclusion and Restraint in Mental Health Facilities

NSW Health Information Bulletin IB2022_048 - Wayfinding for Healthcare Facilities
NSW Ministry of Health Policy Directive PD2021_037 - Security Improvement Audits
NSW Ministry of Health Policy Directive PD2017_001 - Responding to the Needs of People with Disability during Hospitalisation
NSW Ministry of Health Policy Directive PD2012_050 - Forensic Mental Health Services
NSW Ministry of Health Guideline GL2015_007 Management of Patients with Acute Severe Behavioural Disturbance in Emergency Departments

SESLHD:
SESLHDPD/265 - Emergency Management
SESLHDPR/229 - WHS – Transporting of Patients – Risk Management
SESLHDPR/240 - Decommissioning a Workplace
SESLHDPR/431 - WHS – Fire Safety Risk Management
SESLHDPR/341 - Violence Prevention and Management
SESLHDPR/212 - Health, Safety and Wellbeing Risk Management
SESLHDPD/196 - Records Management
SESLHDPR/510 - Managing Secure Organisation Access within Cerner EMR
SESLHDPD/288 - Service Continuity Policy for Health ICT Services
SESLHDPD/192 - Health Records (paper based) Disaster Management
SESLHDPD/203 - Records Management – Retention Periods
SESLHDPR/220 - Records Management – destruction of
SESLHDPR/597 - Client and Patient Safety and Security Searching
SESLHDPD/285 - Motor Vehicle Policy
SESLHDPR/483 - Restraint Use with Adult Patients
SESLHDGL/082 - Clinical Risk Assessment & Management - Mental Health
SESLHDPR/323 - Working in Isolation Risk Management
SESLHDPR/626 - Closed Circuit Television – management and operation of in SESLHD Facilities
SESLHDBR/031 - Illicit substance and/or alcohol and other drug use within inpatient Mental Health Service
SESLHDBR/014 - Prone Restraint Restriction for the Mental Health Service
SESLHDBR/080 - Search to maintain safety in the SESLHD Mental Health Inpatient Facilities
POWH/SSEH Clinical Business Rule - Suspected illicit substances and implements associated with their use

8. VERSION AND APPROVAL HISTORY

Date	Version No.	Version and approval notes
27 November 2018	Draft 1	P Pollock, Manager, Health Safety and Wellbeing in consultation with the Implementation Working Party – Security Action Plan
21 January 2019	Draft 2	Feedback comments and recommendations included P Pollock, Manager, Health Safety and Wellbeing
29 January 2019	Draft 2	Processed by Executive Services prior to submission to Executive Council

March 2019	1	Approved by Executive Council.
May 2019	1	Minor review to include Outpatient and Community Drug and Alcohol Services.
May 2019	1	Formatted by Executive Services and published.
June 2021	2	Minor review. Changes relating to hyperlinks, reference documents, titles, grammatical corrections, ownership and forms. Approved by Executive Sponsor.
13 July 2023	2.1	Minor review approved by A/Director, Corporate and Legal Services. Changes relating to hyperlinks, reference documents, titles, grammatical corrections, ownership and forms. Updated Executive Sponsor to General Manager, Corporate Services.

APPENDIX A WHS & Security Risk Assessment Tool

Risk location:	[Facility Location]
Risk Description:	[A description of the risk, possible causes and impacts.]
Background/context:	[How did the risk arise? What information was used to identify the risk e.g. incidents, issues raised by staff, complaints, planned review; What factors impact on the risk; reference chapter in MoH security manual/better practice procedures if relevant]
Consultation	[record staff consulted in relation to the risk assessment]

Current Controls

Hazards/Risk Factors (if a security hazard, include relevant factors from MoH Security Manual chapter/s)	**Current Risk Controls (Follow Hierarchy of Controls)**	**Current Risk Rating (see appendix 1)**	**Are current controls effective?** Yes/No

Additional Controls

List Risk Factors that require additional Controls	Additional Risk Controls Required (follow appendix 2 Hierarchy of Hazard Controls)	Who will do it?	By when ?	Date completed	Planned review date	Are new controls effective?	Residual Risk Rating
1.						□ Working well □ Need review □ Need a new Risk Assessment	
2.						□ Working well □ Need review □ Need a new Risk Assessment	
3.						□ Working well □ Need review □ Need a new Risk Assessment	

Responsible manager: **Date:**	**Reviewed By:** **Date:**

Example risk matrix, use the tool currently endorsed for WHS risk assessments by your health entity

NSW Health Risk Matrix

Risk rating	Action required
Red = Extreme (A – E)	**Escalate to CE or Head of Health Service and Director-General** A detailed action plan must be implemented to reduce risk rating with at least monthly monitoring and reporting.
Orange = High (F – K)	**Escalate to Senior Management** A detailed action plan must be implemented to reduce risk rating.
Yellow = Medium (L – T)	**Specify Management Accountability and Responsibility** Monitor trends and put in place improvement plans.
Green = Low (U – Y)	**Manage by routine procedures** Monitor trends.

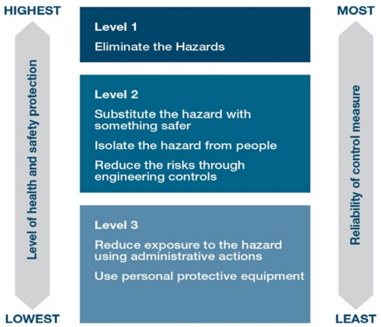
CONSEQUENCE EXAMPLES

NSW HEALTH RISK CATEGORIES	Catastrophic	Major	Moderate	Minor	Minimal
Clinical Care & Patient Safety	Unexpected multiple patient deaths unrelated to the natural course of the illness.	Unexpected patient death or permanent loss/reduction of bodily function unrelated to the natural course of the illness.	Unexpected temporary reduction of patient's bodily function unrelated to the natural course of the illness which differs from the expected outcome.	Patient's care level has increased unrelated to the natural course of the illness.	First Aid provided to patient unrelated to the natural course of the illness.
Health of the Population	An increase in the prevalence of known conditions contributing to chronic diseases across the state-wide population health KPI categories currently measured by NSW Health and or an increase of more than 10% in one or more category.	Failure to materially reduce the prevalence of known conditions contributing to chronic disease across the majority of the state-wide population health KPI categories measured by NSW Health and or an increase of more than 5% up to 10% in one or more category.	Failure to materially reduce the prevalence of more than one of the known conditions contributing to chronic disease from the state-wide population KPI categories measured by NSW Health and or an increase of more than 2% and up to 5% in one or more category.	Failure to reduce the prevalence of one of the known conditions contributing to chronic disease from the state-wide population health KPI categories measured by NSW Health or an increase of up to 2% in one or more category.	A preventative Health program has not demonstrably met planned objectives but the prevalence of known condition is continuing to decrease in line with KPI targets.
Workforce	Unplanned cessation of a critical state-wide program or service or multiple programs and services.	Unplanned cessation of a service or program availability within a Health Service with possible flow on to other locations.	Unplanned restrictions to services and programs in multiple locations or a whole hospital or community service.	Unplanned service delivery or program delays localised to department or community service.	Minimal effect on service delivery.
Communication & Information Facilities & Assets Management	Loss or permanent damage of major utilities, records, IT data systems and communications resulting in prolonged suspension of service delivery.	Restriction or damage of or prolonged service disruption to some utilities, records, IT data systems & communication.	Temporary suspension of work due to damage to property, assets, records or access to IT or communication systems.	Localised damage to property, assets or records and restricted access to IT systems or communication.	Minimal effect on infrastructure, records, IT systems or communication and minimal or no disruption to service delivery or work.
Emergency & Disaster Response	State-wide system dysfunction resulting in total shutdown of service delivery.	Health Service is compromised as service providers are unable to provide effective support and other areas of NSW Health are known to be affected.	Disruption of a number of services within a location with possible flow on to other locations in the area.	Some disruption within a location but manageable by altering operational routine.	No interruption to services.
Finance & Legal	More than 5% over budget NOT recoverable within the current or following financial year. Unable to pay staff or finance critical services. Legal judgement, claim, non compliance with legislation resulting in indeterminate or prolonged suspension of service delivery. Fraud impacts on service delivery.	Up to 5% over budget or a material overrun NOT recoverable within the current financial year. Unable to pay creditors within DOH benchmark. Legal judgement, claim, non compliance with legislation resulting in medium term suspension of service delivery. A fraud impacts on service delivery.	Up to 5% over budget but recoverable within current financial year. Legal judgement, claim, non-compliance with legislation resulting in medium term but temporary suspension to services.	Up to 1% temporarily over budget and recoverable within current financial year. Legal judgement, claim, non-compliance with legislation resulting in short term disruption to services.	Less than 1% temporarily over budget. Temporary loss of or unplanned expenditure related to individual program or project but no net impact on budget. Legal judgement, claim or legislative change but no impact on service delivery.
Safety & Security	Multiple deaths or life threatening injuries to non-patients.	Death or life threatening injury/ illness causing hospitalisation of non-patients.	Serious harm / injury or illness causing hospitalisation or multiple medical treatment cases for non-patients.	Minor harm or injury to a non-patient where treatment or First Aid is required.	Harm, injuries or ailments not requiring immediate medical treatment.
Leadership & Management Community Expectations	Failure to meet critical priority KPI's included in the service's performance agreement. Sustained adverse national publicity. Significant loss of public confidence, loss of reputation and/or media interest across NSW in services.	Failure to meet a significant number of priority KPI's included in the service's performance agreement. Sustained adverse publicity at a state-wide level leading to the requirement for external intervention. Systemic and sustained loss of public support/opinion across a service.	Failure to meet a number of priority KPI's included in the services' performance agreement. Increasing and broadening adverse publicity at a local level, loss of consumer confidence, escalating patient/consumer complaints. Extended loss of public support/opinion for a Facility/Service.	Failure to meet one or more of the KPI's (excluding priority KPI's) included in the service's performance agreement. Periodic loss of public support.	Occasional adverse local publicity.

CONSEQUENCE RATINGS

Probability	Frequency	LIKELIHOOD	Catastrophic	Major	Moderate	Minor	Minimal
> 95% to 100%	Several times a week	Almost certain	A	D	J	P	S
> 70% to 95 %	Monthly or several times a year	Likely	B	E	K	Q	T
> 30% to 70%	Once every 1 -2 years	Possible	C	H	M	R	W
> 5% to 30%	Once every 2 – 5 years	Unlikely	F	I	N	U	X
< 5%	Greater than once every 5 years	Rare	G	L	O	V	Y

Hierarchy of Controls


HIGHEST
LOWEST
Level of health and safety protection
Level 1
Eliminate the Hazards
Level 2
Substitute the hazard with something safer
Isolate the hazard from people
Reduce the risks through engineering controls
Level 3
Reduce exposure to the hazard using administrative actions
Use personal protective equipment
MOST
LEAST
Reliability of control measure

Level 1 examples Workplace design to eliminate hazards and develop a calming environment Removing objects that could be used as potential weapons Removing asbestos
Level 2 examples Barriers and screens Access control Changes to client contact arrangements Video intercoms for night entrances Dual entry points to eliminate potential entrapment Secure retreat areas Credit card facilities instead of cash Security lighting Alarm systems Changing chemical to less hazardous Contracting out high risk tasks to suitably qualified staff
Level 3 examples Task rotation Policies Safe work practices / safe operating procedures Personal protective equipment – duress alarms, gloves, goggles, masks, plastic gowns, safety shoes Signage Training

You must always aim to eliminate the risk, which is the most effective control. If this is not reasonably practicable, you must minimise the risk by working through the other alternatives in the hierarchy.
The lower levels in the hierarchy are less effective because controls that change the hazard or minimise exposure to the hazard can only minimise the risk. You cannot eliminate the risk without eliminating the hazard.
Administrative controls and personal protective equipment (PPE) are the least effective at minimising risk because they do not control the hazard at the source and rely on human behaviour and supervision.
These control measures should only be used:

- to supplement higher level control measures (as a back-up)
- as a short-term interim measure until a more effective way of controlling the risk can be used, or
- when there are no other practical control measures available (as a last resort)

APPENDIX B Security training matrix for SESLHD staff

COURSE (inc HETI code)➔ **GENERAL STAFF** 🡣	**Customer Service** 121026761	**Security Awareness – all staff** 194502198	**VPM Module 1** 144148304	**VPM Module 2** 39964595 189851344	**VPM Module 3** 144264294	**VPM Module 4** 39990453	**Code Black***	**EDVPM** 135736176	**Armed Holdup****
Code Black team members	✓	✓	✓	✓	✓		✓		
Staff & Managers Emergency Department	✓	✓						✓	
Managers - High Risk clinical units or teams	✓	✓	✓	✓		✓			
Staff - High Risk clinical units or teams	✓	✓	✓	✓					
Staff – High Risk required to participate in team restraint	✓	✓	✓	✓	✓				
Staff & Managers of low risk units & teams	✓	✓	✓						
Cashiers	✓	✓	✓						✓
Pharmacy staff & managers	✓	✓	✓						✓

COURSE ➔ **SECURITY STAFF** 🡣	**Customer Service** 121026761	**Security Awareness – Security staff** 197081007	**VPM Module 1** 144148304	**VPM Module 2** 39964595 189851344	**VPM Module 3** 144264294	**VPM Module 4** 39990453	**Code Black***	**EDVPM** 135736176	**Security in the Health Environment** 132300956
Manager Security	✓	✓	✓	✓	✓	✓	✓		✓
Senior Security	✓	✓	✓	✓	✓		✓	✓	✓
Security Officer	✓	✓	✓	✓	✓		✓	✓	✓
Health and Security Assistants	✓	✓	✓	✓	✓		✓	✓	✓

* Local course designed and run at the site

** External course sourced through external training providers, e.g. Courtnell Armed Robbery Safety Awareness Online Course

APPENDIX C - SESLHD Security Officer Position Description

Position Details			
Position Number:			
Position Title:	Security Officer		
Cost Centre:		**(Cost) Percentage:**	100%
Organisation:	South Eastern Sydney Local Health District		
Location:			
Facility:			
Are multiple Awards relevant to this position?	No		
Award:	Health Employees (State) Award	**Classification:**	Security Officer
Registration and Licence requirements:	Security Licence 1A NSW Drivers Licence "C"		
Specialty Code:	N/A		
Vaccination Category:	Category A		
Responsible to:	Security Manager, Senior Security Officer Deputy Manager, Operations Manager, Shift Supervisor		
Responsible for (staff):	Nil		
Position Description Approved/Reviewed :	October 2017		

Primary Purpose of the Position

South Eastern Sydney Local Health District (SESLHD) is committed to improving the care provided to our patients in line with our vision of ***Working together to improve the health and wellbeing of our community.***

Security Officers are required to respond to requests for assistance from staff, patients and visitors on the hospital campus whilst promoting a cohesive and inclusive team environment.

Security Officers are required to promptly respond and provide a security response for all emergencies ensuring all security patrols, tasks and activities are completed in accordance with instructions and training.

Security Officers will have a genuine desire to understand and help others, and view interaction with all patients, staff, and visitors as a significant proportion of their role.

Key Accountabilities

- Provide protection to staff, patients and visitors at site where rostered, including; escorting staff and visitors and other duties as directed.
- Support and assist in the development of relevant policies and procedures to ensure that correct practice is maintained consistent with the requirements of Ministry of Health, SESLHD, the relevant hospital (s) and applicable legislation including Security Licencing and Enforcement Directorate.

- Provide regular foot and mobile patrols of all areas of the hospital grounds including; access control to restricted areas as per the security policy and procedures to ensure crime prevention against person, property or equipment within area of responsibility.
- Assist in managing aggressive and violent patients/other persons in line with SESLHD policy and procedures, at the direction of the clinical staff/ Department Managers.
- Patrol hospital premises to identify security risks and ensure buildings, and unoccupied premises are safe and secured and where appropriate make recommendations for improvements.
- Act as part of the emergency disaster team, including following the briefing on the disaster, assist as directed and carry out instructions as per the Emergency Plan or as directed by Security management.
- Investigate and compile reports of all thefts of personal and hospital property and incidents, including; completing follow up reports and maintain a register for the collection of lost and found articles.
- Maintain the traffic management plan, including monitoring and actioning infringement notices for illegally parked vehicles.
- Undertake ID, access control, key management and CCTV duties within level of authority and access privileges.
- Assist with the transportation of confidential material
- Attend to all response alarms, emergencies, fires and other similar matters, evacuating premises and contacting appropriate emergency services as required within area of responsibility and maintain a clear and accurate log of all events, jobs performed during shift.
- Participate in meetings to maintain standards, procedures, service levels, operations and support of the Unit's activities.
- Ability to create a positive presence and act as an appropriate and effective role model whilst promoting a positive culture and supporting practices that reflect the organisational values through demonstrated behaviours and interactions with patients/clients/employees.
- Maintain responsibilities for personal and professional development by participating in training/education activities and performance reviews in order to continuously improve the level and quality of service.
- All staff are expected to take reasonable care that their actions do not adversely affect the health and safety of others. All staff are also expected to comply with any reasonable instruction that is given to them and with any reasonable policies/procedures relating to health or safety in the workplace, as well as notifying any hazards/risks or incidents to their managers.

Key Challenges and Influences

Challenges/Problem Solving:

- Maintaining current knowledge of the frequently changing security policies and procedures.
- Managing competing priorities and high volumes of work, given often limited resources.
- Attending to the wide variety of day-to-day security tasks, resolving them on behalf of the Security Manager and Senior Security Officer of the unit/department.
- Ability to work across a 24 hour roster over a seven day service and provide a dynamic security environment across multiple sites.
- Ability to have personal resilience and remain calm under pressure when managing challenging behaviours and using conflict resolution skills.

Communication:

- Internally, the Security Officer is required to communicate regularly with the Security Manager, Deputy Manager, Shift Supervisors and Senior Officers as well as internal stakeholders and other health team members.
- Externally, the Security Officer will develop and maintain effective relationships with external stakeholders to ensure effective delivery of service.

Decision Making/Influence:

- Work independently under limited direction and within constraints set by senior management.
- Escalate more complex issues outside the scope of their position description to the Senior Security Officer or Security Manager.

Selection Criteria

1. Must hold NSW Security licence 1A: NSW Drivers licence "C" and a current relevant first aid certificate.
2. Demonstrated knowledge and experience providing security and customer service in a large client base environment.
3. Demonstrated ability to work under minimal supervision and complete all patrols and any other security work during the shift.
4. Demonstrated experience with a sound understanding of alarm systems, access control system, CCTV and Fire Indication panels.
5. Proven experience in communicating and responding to challenging and aggressive situations such as distressed persons, demonstrating empathy, integrity and resilience under various circumstances.
6. Excellent written communication skills particularly in the area of report writing, maintaining shift logs and entering information into databases.
7. Demonstrated ability to develop and maintain effective working relationships with senior management and other key stakeholders including ability to work co-operatively as a member of a team.

Employment Screening Checks

X National Criminal Record Check

☐ National Criminal Record Check (Aged Care)

☐ Working with Children Check

APPENDIX D - SESLHD Senior Security Officer Position Description

Position Details			
Position Number:			
Position Title:	Senior Security Officer		
Cost Centre:		**(Cost) Percentage:**	100%
Organisation:	South Eastern Sydney Local Health District		
Location:			
Facility:			
Are multiple Awards relevant to this position?	No		
Award:	Health Employees (State) Award	**Classification:**	Senior Security Officer
Registration and Licence requirements:	Security Licence 1A NSW Drivers Licence “C”		
Specialty Code:	N/A		
Vaccination Category:	Category A		
Responsible to:	Security Manager		
Responsible for (staff):	Security Officers		
Position Description Approved/Reviewed :	October 2017		

Primary Purpose of the Position

South Eastern Sydney Local Health District (SESLHD) is committed to improving the care provided to our patients in line with our vision of ***Working together to improve the health and wellbeing of our community***.

The Senior Security Officer will supervise and lead hospital Security Officers in the delivery of security services across the hospital.

The Senior Security Officer will provide support to the Security Manager in the administrative and operational management of the Security Department.

Key Accountabilities

- Promptly provide a security response for all emergencies ensuring all security patrols, tasks and activities are completed in accordance with instructions and training.
- Provide protection to staff, patients and visitors at a SESLHD site where rostered including escorting staff and visitors and delegating duties such as assisting hospital staff to locate missing patients and returning them to the appropriate departments.
- Develop and review relevant policies and procedures to ensure that correct practice is maintained consistent with the requirements of Ministry of Health, SESLHD, the relevant hospital (s) and applicable legislation including Security Licencing Enforcement Directorate.
- Provide afterhours relief for the Fire and Safety Officer in accordance within agreed scope for organisational requirements.

- Ensure accurate records are maintained including but not limited to; lost and found property in the register, hospital key register and shift log reports.
- Provide and delegate regular foot and mobile patrols of all areas of the hospital grounds including; access control to restricted areas as per the Security policy and procedures to ensure crime prevention against person, property or equipment within area of responsibility.
- Manage and provide direction to Security Officers in handling of aggressive and violent patients and other persons as per organisational policy and procedures, at the direction of the clinical staff/ Department Managers.
- Patrol hospital premises to identify and mitigate security risks. Ensure buildings, and unoccupied premises are safe and secured and where appropriate make recommendations for improvements and implementation of risk controls.
- Investigating incidents of theft or property damage and provide accurate reports to the Security Manager and police as required. Undertake and manage any follow-up action as required.
- Be a key part of the emergency disaster team, including following the briefing on the disaster, assist and direct other Security staff to carry out instructions as per the Emergency Plan.
- Attend all response alarms, emergencies, fires and other similar matters, evacuating premises and contacting appropriate emergency services as required within area of responsibility.
- Maintain and assist in the development of traffic management plans, including monitoring and actioning infringement notices for illegally parked vehicles.
- Manage ID access control, key management and CCTV duties as required within level of authority and access privileges.
- Assist with the transportation of confidential material.
- Ensure control room is manned at all times and make certain that control room duties such as CCTV cameras and the recording of evidence is undertaken. Monitor the performance of Security Officers in providing these functions in line with current policies and procedures.
- Ability to create a positive presence and act as an appropriate and effective role model whilst promoting a positive culture and supporting practices that reflect the organisational values through demonstrated behaviours and interactions with patients/clients/employees.
- Recruit, coach, mentor, train and performance develop Security staff, to develop the capabilities of the team to undertake changing roles, responsibilities and to provide for succession within the unit.
- Comply with and implement the NSW Health Work Health and Safety Better Practice Procedures by identifying, assessing, eliminating/controlling and monitoring hazards and risks within the workplace, to the extent of delegated authority for the role and assist Security management with the development of WHS Objectives.
- Maintain responsibilities for personal and professional development by participating in training/education activities and performance reviews in order to continuously improve the level and quality of service.
- All staff are expected to take reasonable care that their actions do not adversely affect the health and safety of others. All staff are also expected to comply with any reasonable instruction that is given to them and with any reasonable policies/procedures relating to health or safety in the workplace, as well as notifying any hazards/risks or incidents to their managers.

Key Challenges and Influences

Challenges/Problem Solving:

- Maintaining current knowledge of the frequently changing policies and procedures.
- Managing competing priorities and high volumes of work, given often limited resources.
- Attending to the wide variety of day-to-day security tasks and resolving them on behalf of the Security Manager of the department.
- Ability to work across a 24 hour roster over a seven day service and provide a dynamic security environment across multiple sites.
- Ability to have personal resilience and remain calm under pressure when managing challenging behaviours and using conflict resolution skills.

Communication:

- Internally, the Senior Security Officer is required to communicate regularly with all hospital staff to ensure effective delivery of service.
- Externally, the Senior Security Officer will develop and maintain effective relationships with external support services such as Police, Fire, Ambulance and Private Hospitals.

Decision Making:

- Work independently under limited direction and within constraints set by senior management
- Escalate more complex issues outside the scope of their position description to the Security Manager.

Selection Criteria

1. Must hold NSW Security licence 1A: NSW Drivers licence "C" and a current relevant first aid certificate.
2. Demonstrated experience managing a team of security officers in a large complex work environment.
3. Proven experience providing security and customer service in a large client base environment.
4. Demonstrated ability to coordinate and complete all patrols and any other security work during the shift.
5. Demonstrated knowledge and experience with a sound understanding of alarm systems, access control system, CCTV and Fire & Safety procedures including Fire Indication panels.
6. Proven experience in communicating and responding to challenging and aggressive situations such as distressed persons, demonstrating empathy, integrity and resilience under various circumstances.
7. Strong written communication skills particularly in the area of report writing, maintaining shift logs and entering information into databases.
8. Demonstrated ability to develop and maintain effective working relationships with senior management and other key stakeholders including ability to work independently and co-operatively as a member of a team.

Employment Screening Checks

X National Criminal Record Check

☐ National Criminal Record Check (Aged Care)

☐ Working with Children Check

APPENDIX E - Violence Prevention Management Training Needs Analysis

Overview

As set out in NSW Health PD2017_043 Violence Prevention & Management Training Framework for the NSW Health Organisations

A training needs analysis is to be undertaken to Identify and assess education and training needs of staff in regard to violence prevention and management. This needs to be based on the various operational groups/roles and work environments of the workers.

This tool has been developed to document experiences of exposure to client and visitor initiated aggression and violence in departments.

All staff working in Emergency Departments as a minimum must complete the Emergency Department Violence Prevention management learning pathway

How to use

Using this risk matrix, departments and wards will be able to determine the level of risk to each group of workers within the department. This is to be based on both documented incidents in IIMS and direct input of the workers.

1. Department manager to determine the groups of workers they manage within their department and record this on the tool. *I.e. on a ward this may consist of nurses, administration staff, educators*
2. In consultation with the individual worker groups use the matrix below to determine the highest actual risk level and record this on the tool. *It is important to consult with workers as using IIMS data alone may indicate under reporting.*
3. Once completed return the tool to District VPM Coordinator, Organisational Development and Learning

For workgroups that work across multiple locations or departments such as security, wards persons, hospital assistants and physio's, the manager may seek input from other departments to verify information about incidents but the risk level is to be based on the highest risk identified.

All staff must complete Violence Prevention and Management – Promoting Acceptable Behaviour in the Workplace and Violence Prevention and Management Awareness

Actions

The results of the compiled data will be reviewed in conjunction with incident data from IIMS and other sources to help identify the specific training requirements across the facility and organisation.

In addition to identifying the level of training required, consultation with workers may also reveal some systemic issues within the department or facility that the manager will need to follow up on.

For example, it might identify:

- A workforce skilled in defusing/de-escalating situations before they become violent.
- A limited understanding of what constitutes an aggressive incident.
- Issues associated with incident reporting and communication of risks.
- Under-reporting of incidents.
- Work practice issues within a work area that require further investigation (e.g. staff skill mix).

Note – the exposure to aggression risk calculator has been based on the T1tool which was developed in conjunction with WorkSafe Victoria and a number of Victorian Health groups Prevention and management of aggression in health services - A handbook for workplaces

Facility:_______________ Department: _________________________________ Manager: ________________________ Date: ______________

Matrix

Exposure type → **Frequency ↓**	**Aggression incident resulting in serious injury** Severe physical attack, including repeated kicking, punching etc.	**Aggression incident possibly resulting in serious injury** Physical attack including, kicking, punching etc. **Or specific threat to harm**	**Aggression incident resulting in minor injury (i.e. First Aid only)** Pushing, grabbing, and scratching.	**Specific threat to harm** Overtly physically aggressive (hitting furnishing etc).	**Verbal aggression** Abuse, swearing directed at specific staff **Non-specific threats**	**Elevated emotional state** Heated disagreement, raised voices
Weekly	H	H	M	M	L	L
Monthly	H	H	M	L	L	L
Bi-annually	H	M	M	L	L	L
Annually	M	M	L	L	L	L
5 yearly	M	M	L	L	L	L

L = All staff	M = Category 2 and 3 staff	H = Category 3 staff
• Violence Prevention and Management – Promoting Acceptable Behaviour in the Workplace • Violence Prevention and Management Awareness	Additional Violence Prevention and Management modules • An introduction to Legal and Ethical Issues • Personal Safety	Additional Violence Prevention and Management module • Team Restraint Techniques

Worker Group	Risk Rating	Workers consulted (document names)

Other identified issues –