

# Security guidelines

Queensland Health 2022

QH-GDL-502:2022



# Contents

---

<b>Terminology</b>	<b>3</b>
<b>Version Control</b>	<b>4</b>
<b>Background</b>	<b>5</b>
<b>Purpose</b>	<b>6</b>
1. Principles	6
<b>Scope</b>	<b>6</b>
<b>Objective</b>	<b>8</b>
<b>Part A: Security Risk Management and Planning</b>	<b>9</b>
1. Introduction	9
2. A guide for assessing security risks	10
3. Developing a security plan	19
<b>Part B: Controlling risks through physical security</b>	<b>23</b>
1. Introduction	23
2. Physical security controls in the healthcare environment	24
3. Physical security controls, equipment, and concepts	26
<b>Part C: Standard operating procedures for healthcare environments</b>	<b>42</b>
1. Introduction	42
2. Healthcare Security Models	44
3. Local standard operating procedures (SOPs)	46
<b>References</b>	<b>74</b>
<b>Appendices</b>	<b>75</b>

# Terminology

Term	Definition
<b>Threat</b>	Risk occurrence that would have a negative impact, AS4485.1:2021.
<b>Hazard</b>	Potential source of harm, HB188:2021.
<b>Security risk</b>	Factors or events, or combination of factors or events, which may impact on the security and welfare of patients, workers and others, and property (including information) for which the facility has a duty of care, AS4485.1:2021.
<b>Security risk assessment</b>	Methodical process of identifying, analysing, and evaluating security risks and of determining appropriate controls, AS4485.1:2021.
<b>Risk acceptance</b>	The informed decision to take a particular risk, noting that risk acceptance can occur without risk treatment or during the process or risk treatment, and that accepted risks are subject to monitoring and review, ISO Guide 73:2009, HB188:2021.
<b>Risk tolerance</b>	The organisation or stakeholders' readiness to bear the risk after risk treatment to achieve its objectives, ISO Guide 73:2009, HB188:2021.
<b>Risk avoidance</b>	The informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk, HB188:2021.
<b>Risk profile</b>	Description of any set of risks, HB188:2021.

# Document approval details

## Document custodian

Queensland Occupational Violence Strategy Unit (QOVSU)

## Approval officer

Joanna Griffiths, Manager QOVSU

## Approval date:

09.12.2022

## Effective from:

09.12.2022

## Review

This Guideline is due for review: 9 December 2025

## Supersedes:

Security Guideline for Queensland Health – Health Care Facilities 2001.

# Version Control

Version	Date	Comments
V. 1	07.06.2022	<i>This document supersedes the 'Security Guideline for Queensland Health – Health Care Facilities' released in 2001, following changes to Australian Standards</i>

# Background

The Security Guidelines, Queensland Health ('the guidelines') have been updated by the Queensland Occupational Violence Strategy Unit (QOVSU) in consultation with the Queensland Security Managers Network (QSMN) to ensure state-wide collaboration across Hospital and Health Services (HHS). These guidelines supersede the previous document 'Security Guideline for Queensland Health – Health Care Facilities' released in 2001.

The guidelines have been developed with strong guidance taken from the updated Australian Standards AS 4485.1 and 2:2021 Security for Healthcare Facilities, which supersedes AS 4485.1 and 2:1997. This standard outlines principles, standards, and common practices for the development of effective security systems throughout healthcare facilities.

Separated into three specific sections, the guidelines expand on the previous content and aligns content with updated standards and Department of Health strategic direction to promote systematic and contemporary best practice for security arrangements within Queensland Health.

The content within the guidelines contributes to the [Department of Health Strategic Plan 2021–2025](#) objective to 'support and advance our workforce' through strategies that ensure the workplace is safe, rewarding, enhances wellbeing and adequately equips the workforce to perform at the highest level.

Recommendation with the guidelines supports the approach towards person-centered care and aligns with the National Safety and Quality Health Service Standards, Comprehensive Care Standard criteria through minimising patient harm and reducing restrictive practices.

The implementation of the guidelines contributes to Recommendation 14 of the Occupational Violence Prevention in Queensland Health's Hospital and Health Services Taskforce Report 2016 (section 8.3.3. Security Service Arrangements), regarding functions and roles.

The requirement to provide updated security guidelines to guide the development of local arrangements with a degree of consistency, was identified at the inaugural Healthcare Security Managers Network – Leadership Forum 2021. The forum provided an opportunity to connect HHSs security leaders with peers. Security leaders identified the absence of formal security governance across Queensland Health HHSs.

The guidelines will promote consistency in procedural development by providing reference to relevant Australian Standards, recommendations for minimum security arrangements, information regarding security models, and role clarity regarding functions of the Healthcare Security Officer (HSO).

For information about how the guidelines support the Onboarding & Upskilling Security Managers Toolkit, please see the Queensland Health Security Framework [Queensland Health Security Framework | QOVSU | MNHHS](#).

# Purpose

The QSMN identifies the below vision and purpose relevant for security services in healthcare.

**Our Vision:** To provide a professional service that maintains a safe healthcare environment.

**Our Purpose:** To contribute to the delivery of innovative and coordinated security services and to promote a safe environment through collaboration, effective use of resources, technology, and best practices.

## 1. Principles

This guideline contributes to the [Department of Health Strategic Plan 2021–2025](#) objective to ‘support and advance our workforce’ through strategies which ensure the workplace is safe, rewarding, enhances wellbeing and adequately equips the workforce to perform at the highest level.

The fundamental principles that underpin the guidelines are:

- Everyone has the right to a healthy, safe, and secure workplace
- Everyone has a right to access safe healthcare
- Security and safety are everyone’s responsibilities
- Patient safety and worker safety should be addressed conjunction with one another
- Personal and private information held about patients and employees must be protected, as must other forms of information, and valuable and attractive property
- Security management strategies, supporting processes, and practices are:
  - Designed to protect assets, people, property, information, activities, and reputation
  - Designed to support least restrictive practices, person-centred care, and cultural safety
  - Subject to the principles of continual improvement
- Standard operating procedures (SOPs) are to be designed by each HHS to (in a manner that suits the HHS), to:
  - Mitigate risk through clear and concise instructions
  - Enable prioritisation of tasks and duties
  - Promote role clarity
  - Promote contingencies and escalation pathways where appropriate to maintain safety
  - Encourage informal dynamic risk assessments (completed in real-time) to maintain safety whilst completing activities (answering questions i.e.: what are the risks? what are our resources? how are we going to respond safely?)

### **This guideline recommends the following:**

- HHS security risk assessments be designed to inform HHS security plans
- HHS security plans articulate how risks are holistically managed within HHSs
- HHS SOPs are developed to provide local instruction on effective security practices

Physical security controls are implemented by HHSs to reduce risk, based on the specific needs of each HHS

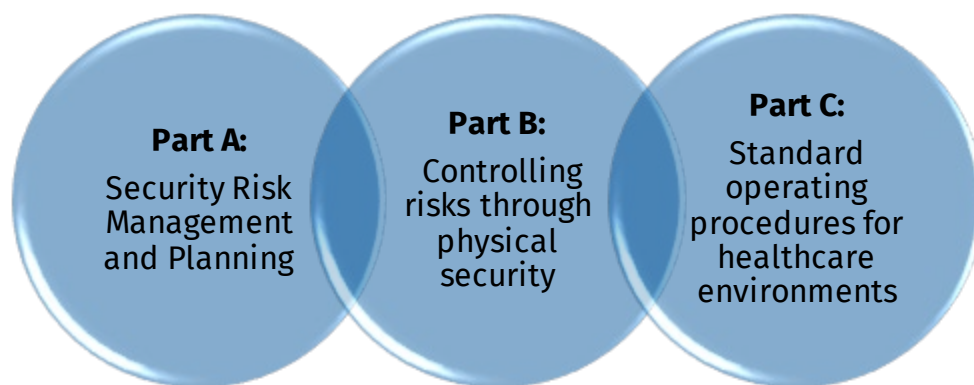
# Scope

The scope of this guideline is for Queensland HHS employees (permanent, temporary, and casual) and all organisations and individuals acting as its agents (including, but not limited to: Visiting Medical Officers and other partners, contractors, consultants, and volunteers).

The guidelines are designed primarily for those stakeholders with direct responsibility for management of security arrangements (in particular, those with line management of internal security services and personnel) and responsibility of security risks within their HHS.

The guidelines are scoped to be referenced as a foundation from which health services may build their own specific instructions for their specific needs based on local resourcing and risk assessments.

The guidelines are divided into three sections for ease of use:



**Part A:** Security Risk Management and Planning, is a foundation from which health services may build their own specific security risk assessments to develop local security plans designed for the specific needs of the HHS.

**Part B:** Controlling risks through physical security, has been established to support HHSs regarding physical security control arrangements. This encourages HHSs to implement and monitor physical security controls through local security risk management processes.

**Part C:** Standard operating procedures for healthcare environments, promotes the development of standard operating procedures aimed at ensuring a safe environment through layering control measures and providing clear instruction.

# Objective

To achieve the best outcomes, physical security controls, SOPs, and security plans must be appropriate, consider risk exposure, and aim to protect people, information, and property. It is the objective of the guidelines to promote comprehensive security risk assessments to ensure any proposed security controls are fit for purpose, developed, and implemented in consultation with stakeholders.

Each HHS is responsible for ensuring they have a risk management process to assess security risks and develop security plans that suit the needs of their facilities. An objective of the guidelines is to recommend best practice minimum security arrangements, physical security controls and security equipment for HHS consideration. To enhance safe and secure workplaces HHSs should consider:

- Promoting the application of security risk assessments to ensure all reasonably foreseeable security-related hazards are identified, assessed, and where reasonably practicable, risks are eliminated, or where risks cannot be eliminated appropriate control strategies are implemented to reduce risks
- Ensuring security plans and physical security controls contribute to the safety of facility occupants and the protection of property against the potential threat of criminal activity
- Supporting the provision of safe services through documented security specific processes to evaluate the effectiveness of existing controls
- Encouraging consultation with staff at all levels including facility stakeholders, relevant committees, workplace health and safety (WHS) professionals, healthcare security, clinical and operational staff
- Ensuring physical security controls are informed by security risk assessments
- Ensuring physical security controls contribute to the protection of property and people against the potential threat of criminal activity, occupational violence, and support provisions of safe services
- Ensuring SOPs are comprehensive and aligned with local security plans to reinforce the growth of a positive security culture

This guideline aims to highlight necessary considerations to improve local practices and promote safe and secure healthcare environments. Outlined within this guideline are key SOPs that each HHS should consider benchmarking with reference to existing procedural instructions or development of additional documents. The guidelines are not intended to supersede existing established local procedures, rather to further inform and align practices (of each HHS) to promote consistency across Queensland Health.



# Part A: Security Risk Management and Planning

## 1. Introduction

Security Risk Management and Planning has been developed to support HHSs in providing and maintaining a safe and secure environment through risk informed security planning and effective controls.

This guideline outlines requirements to be implemented in accordance with legislative obligations and accreditation recommendations in a manner consistent with Queensland Health objectives to ensure the safety and security of employees, patients, visitors, and assets.

This guideline aligns with the Queensland Health Safety Management System. Elements from relevant Australian Standards have been used to inform the risk management process of identifying hazards, assessing risks, controlling risks, and reviewing control measures. Guidance is also taken from the Australian Government's [Protective Security Policy Framework](#) for security planning and risk management.

**Australian Government's Protective Security Policy Framework:**

*“Security planning establishes the strategic direction and sets out the expectations for the efficient and effective security management practices in the entity. This includes ensuring security risks are managed effectively and consistently across the entity to adapt to change, minimise damage and disruption and build resilience”.*

Security risk assessments differ from other risk assessments as they focus primarily on external perimeters and crime prevention. Security risk assessments provide a method to assess criticality, vulnerability, threats, and physical security control measures. Security risk assessments provide an opportunity to engage security professionals within HHSs and the ability to draw from local knowledge. Consultation and leadership enable effective development of local security plans. Security plans increase risk mitigation capabilities and promote a positive safe security culture.

The security risk assessment process outlined in this document (aimed to support stakeholders responsible for managing security), predominantly focusses on the security of a facility, and its ability to avoid or protect against potential impacts of criminal activity with a focus on external environments including plant and equipment, main public spaces, and physical security controls.

The Occupational Violence Risk Assessment Tool (OVRAT) has a similar approach to identify risks, with a specific focus on occupational violence prevention within wards and departments. Dependant on local arrangements, both risk assessments may inform each other, compliment evaluations, and validate findings that emerge from the different approaches and strategic focus.

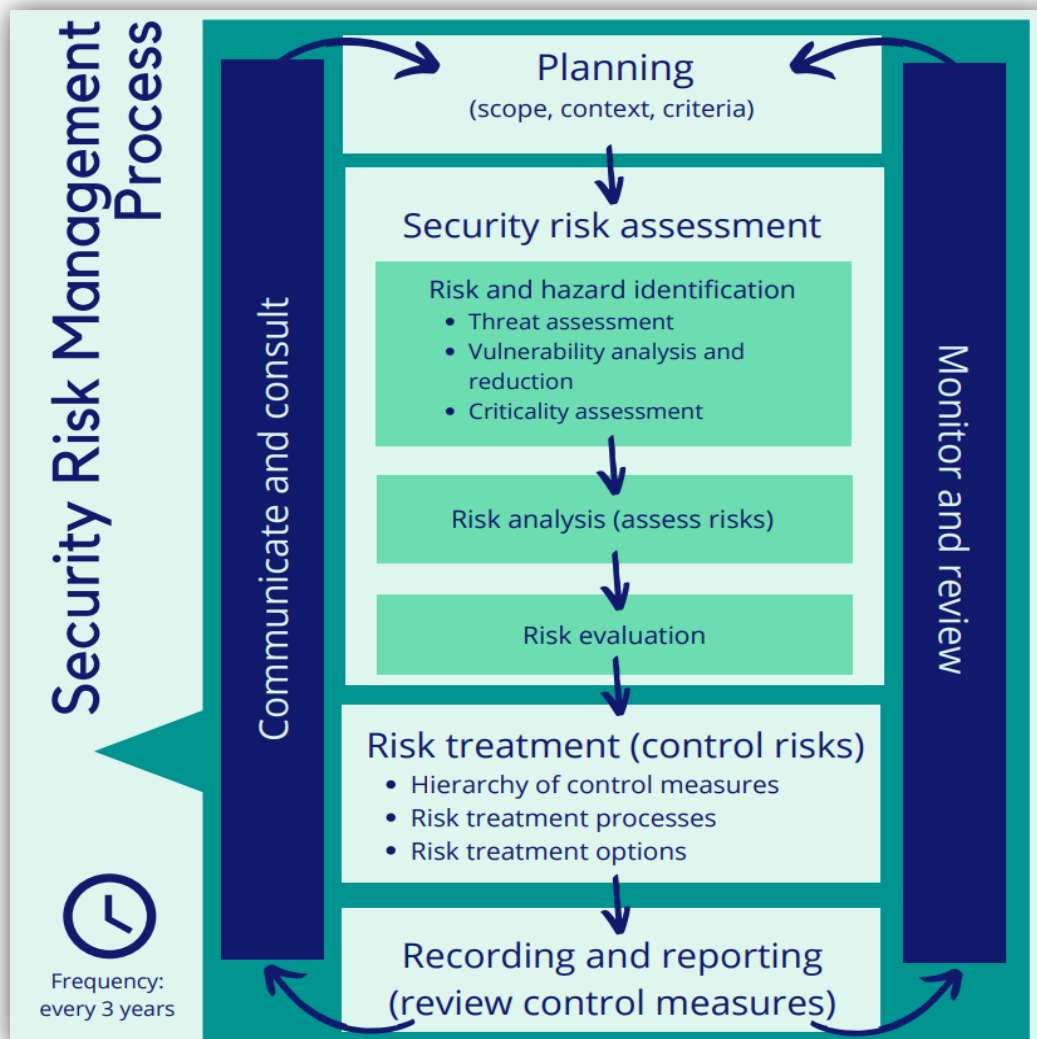
## 2. A guide for assessing security risks

Security risk assessments provide methods for HHSs to identify threats, vulnerabilities, and risks, as well as a method to measure the effectiveness of existing controls. Security risk assessment outcomes should inform decision-making regarding HHS priorities. Security risk assessments should be conducted by qualified and experienced personnel and require thorough consultation to ensure physical security controls are implemented appropriately. Assessing security risks should involve a systematic, and collaborative approach, drawing on the knowledge of local stakeholders.

Engagement with stakeholders during the assessment improves understanding, increases information sharing, develops resilience, and promotes benefits post assessment.

When HHSs are conducting security risk assessments, they should consider seeking specialist advice, communicating with stakeholders (internal and external), and requirements for planning and completing a security risk assessment.

HHS security management may consider using the provided templates found through the appendices or create their own reports. Please see the below Security Risk Management Process adapted from Handbooks HB167, HB188, HB327 and [QH-GDL-401-3-1:2021](#).



**Figure 1:** Security Risk Management Process

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

## 2.1 Seeking specialist advice for security risk assessments

Australian Standards recommend that security risk assessments are to be conducted by qualified and experienced personnel in consultation with relevant stakeholders. HHSs may consider consulting:

- The Queensland Police Service (QPS): QPS may provide advice about community policing initiatives, criminal activity, and appropriate measures to minimise the possibility of acts resulting in loss or harm. The online crime map may provide relevant data [Maps and statistics | QPS \(police.qld.gov.au\)](#).
- External consultants and security firms (preferably with knowledge and experience in healthcare security management, and the health industry).
- Internal professionals, such as security managers, security advisors (or equivalent), and Queensland Health employees with appropriate qualifications or experience.

To comply **AS 4485.2:2021**, states that a Security administrator or equivalent position hold the below:

- a) "Provide executive management with expert advice on security matters*
- b) Identify, assess, manage, and monitor security threats, vulnerabilities, and consequences to the facility's workers, property and information,*
- c) Develop a security risk management plan to address the identified risks outlined in section 3 and incorporating the requirements of the facility's security governance mechanism,*
- d) Implement and manage the security function throughout the facility,*
- e) Develop and review security measures to control the risks to acceptable levels,*
- f) Monitor security arrangements to ensure that they are being applied properly and are proving effective,*
- g) Liaise effectively with other agencies concerned with security matters,*
- h) Raise the awareness of workers and other about security matters and*
- i) Provide advice to planning groups on refurbishment and new construction projects."*

## 2.2 Communicating and consulting with stakeholders for security risk assessments

HHS security management conducting security risk assessments should consider how information is to be communicated and perceived. HHS security management should consider how the security risk assessment is to be shared with the HHS, received by stakeholders, and how feedback is to be collected. Please see below figure.



**Figure 2:** Factors influencing success of communication HB327.

**HB 327:2010 Communicating and consulting about risk, consultation as a process** states:

*“... for communication to be effective the following aspects must be considered.*

- *Where the purpose of the consultation is to obtain the views of others (usually stakeholders) those being consulted should as far as practicable be equally informed about the relevant issues and context as are those seeking the views*
- *Where the purpose of the consultation is to obtain factual knowledge, the enquiry must be framed in a way that avoids ambiguity about meaning and provides those being consulted with insight about the context in which the enquiry is being made*
- *Reasonable time must be provided to allow all parties to the consultation to form considered responses*
- *Sensitive issues should be approached carefully to ensure a balance between legitimate expectations of privacy and the overall veracity of the consultation.”*

**HB 327:2010 Communicating and consulting about risk, benefits from communication and consultation** states:

*“The main benefit from involving stakeholders is a shared and better understanding of the risk faced and the range of treatment options. The following secondary benefits are derived from this understanding:*

- *Reassurance to each stakeholder that all views are taken into account*
- *Bringing together different areas of expertise*
- *Endorsement or acceptance of subsequent decisions by people who may not benefit as much as other*
- *Enhancement of the decision-making process and change management*
- *Improved transparency and assignment of a fair share of responsibility to manage risks to those who are most likely to be affected by the consequence.”*

Perceptions about the identified risks and how they are evaluated will always be present. An individual's perceptions often influence stakeholder willingness to adopt treatments or consider information, for many reasons. Developing consistent and easily understood definitions, that are evidence based, can aid in communicating recommendations, risk treatments, and proposed security improvements.

Planning security risk assessments is crucial to identifying mechanisms for communication with stakeholders, and ensuring all interested parties are appropriately involved.

## 2.3 Planning a security risk assessment

Providing context around the security risk assessment during the planning phase ensures the scope of the security risk assessment is understood and promotes consistency when communicating criteria. This reinforces treatments with a structure that is aimed at eliminating risks, or where practical, reducing risks to a tolerable or acceptable level.

### 2.3.1 Frequency

In accordance with AS4485, after a HHS completes an initial security risk assessment, a review of security arrangements should be undertaken by HHSs at a minimum of **every three years**, or more frequently if the facility undergoes one or more of the following:

- Significant changes to its environments (internal and external)
- Changes to its property and buildings
- Refurbishment
- Experiences a significant increase in volume or severity of security incidents.

A security risk assessment should also be conducted in association with any decommissioning and planning processes for new and redeveloped facilities or to reflect changes in the security risk environment and national threat levels. For more detailed information about threat levels, refer to [Appendix 1](#).

### 2.3.2 Scheduling

HHSs should establish a schedule or program to plan when, where, and by whom, security risk assessments are conducted. This ensures evidence exists of past and planned assessments, and aids in monitoring and reviewing progress. Scheduling should include consulting relevant stakeholders and governance processes for committees responsible for addressing security risks and improving safe work environments.

### 2.3.3 Scope

HHSs should determine the scope of the security risk assessment. The scope may include the below:

- Specific inclusions, and exclusions
- Objectives and expected outcomes
- Responsibilities and relevant information
- Risk assessment tools and techniques or methodology
- Related processes and activities

### 2.3.4 Context

HHSs should determine the context of the security risk assessment. Context considerations should include:

- List of stakeholders, oversight bodies and commitments
- The purpose for the risk assessment
- Reinforce risk management integration with culture of the facility and into core business activities and decision-making (security is everyone's responsibility, all staff have the responsibility to promote a positive security culture)
- Reporting requirements within the HHS

### 2.3.5 Criteria

In accordance with HB167, HHSs should determine the criteria of the security risk assessment. Criteria is a term of reference by which the significance of a risk is assessed and should consider the following:

- Definitions of consequences and likelihood
- Consistency in the use of measurements
- Demonstrate how risk is to be determined

### 2.3.6 Retention

Security risk assessments are to be **retained for a period of 7 years** in accordance with AS 4485.2:2021, s 3.5 “performing risk assessments”.

This retention period aligns with [Corporate Records Management Policy Framework, Business Classification Scheme section v5 \(2021\) \(BCS\)](#): Governance, Risk Management, Assessment and Mitigation, which outlines the requirement to retain records relating to the identification, assessment and monitoring of risks, including the implementation of risk reduction practices and procedures for a period of 7 years after business action completed (disposal authorisation 1051, BSC).

When establishing local arrangements regarding restriction and classification guidance may be taken from the PSPF, however, this is not a mandatory requirement.

Please see [Appendix 2](#) Assessing sensitive and security classified information.

## 2.4 Completing a security risk assessment

Security risk assessments measure the likelihood of a threat to the HHS. [QH-GDL-401-3-1:2021](#) outlines that risk is usually expressed as a measure of the likelihood and consequence to provide a risk rating. Asset identification and assessment of vulnerabilities, existing controls, and threats are optional strategies that inform the risk assessment process.

Likelihood ↓	← Consequence →				
	Negligible	Minor	Moderate	Major	Extreme
Almost certain	Medium (7)	Medium (11)	High (17)	Very high (23)	Very high (25)
Likely	Medium (6)	Medium (10)	High (16)	High (20)	Very high (24)
Possible	Low (3)	Medium (9)	High (15)	High (18)	High (22)
Unlikely	Low (2)	Medium (8)	Medium (12)	Medium (14)	High (21)
Rare	Low (1)	Low (4)	Low (5)	Medium (13)	High (19)

**Figure 3:** Risk matrix QH-GDL-401-3-1:2021.

Please refer to [Appendix 3](#) Consequence assessment and [Appendix 4](#) Likelihood (probability) assessment, for further information.

In accordance with HB167, the **‘R2 D3’ model** can be utilised to measure a controls capability to:

- Deter an attack

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

- Detect an attack
- Delay an attack
- Respond to an attack
- Recover from an attack

Note: An 'attack' in this context may include:

- Trespassing
- Wilful damage (vandalism)
- Stealing (theft)
- Stalking
- Arson
- Assault

Please see [Appendix 5](#) Security control rating, and [Appendix 6](#) Security in depth factors R2D3.

### 2.4.1 Risk and hazard identification

Security advisors (or equivalent positions undertaking the security risk assessments) and HHS stakeholders may identify risks and hazards through facilitated workshops, interviews, questionnaires, research, and physical inspections. Hazard identification includes consideration of all things and situations that could potentially cause harm. Risk identification determines what, where, when, why, and how, something could happen. The following factors should be considered:

- Tangible and intangible sources of risk or cause of risk and indicators of emerging hazards
- Threats and opportunities
- Vulnerabilities and capabilities
- Consequences and impacts
- Previous criminal activity or events

#### **Asset Identification**

In accordance with AS4485, asset identification is the documentation and description of the primary property or service (including critical assets / infrastructure), that may be exposed to, or harmed by a threat. Dependent on the scope of the security risk assessment, the following information may be entered in the provided templates:

- Services provided by the facility
- Facility location, size, positioning, boundaries, surroundings, major geographic features, land use and impacts
- Critical infrastructure, important assets, plant, machinery, and hazardous materials
- Information, systems, resources, and controls
- Utilities, power, water, sewerage, gas, and telecommunications
- Networks which, if destroyed, degraded, or rendered unavailable for an extended period, would have significant impact





- intent refers to the expressed or implicit aims, desires, motivational factors, or objectives associated with the threat
- capability considers attributes of a prospective threat that make it a credible source of threat

### **Vulnerability analysis and reduction**

Conducting a vulnerability analysis identifies weaknesses, the degree of susceptibility, and areas that may require consideration if to build resilience against potential threats and become a less attractive target. Factors that influence the vulnerability of a facility, include (but are not limited to):

- Attractiveness of assets (regarding theft, property damage, vandalism)
- Effectiveness of existing controls (regarding the ability defend against potential threats)
- Ability to treat and recover from a security incident
- Culture and application of security arrangements

Please see [Appendix 8](#) Vulnerability matrix.

### **Criticality Assessment**

Criticality assessment recognises and allocates importance to all resources. Potential impacts derived from the criticality assessment are used to determine the overall risk consequence through defining how critical an asset is and the impacts of losing such asset. The criticality matrix may inform the risk tolerance of an organisation regarding the importance of assets and may influence the perceptions towards suggested risk treatments and proposed controls through providing the scale of the resources' importance.

Please see [Appendix 9](#) Criticality matrix.

## **2.4.2 Risk analysis (assess risks)**

HHSs should undertake a risk analysis that involves detailed consideration to investigate the identified risks with the purpose of comprehending the nature and characteristics of the risk. This provides a rating that categorises the level of risk based on its likelihood and consequences.

## **2.4.3 Risk evaluation**

HHSs should carry out a risk evaluation that supports decision-making processes and determines the required actions. Risk evaluation can lead to a decision to:

- Take no further action
- Consider risk treatment options
- Undertake further analysis to better understand the risk
- Maintain existing controls
- Reconsider objectives

## **2.4.4 Risk treatment (control risks)**

HHSs should consider the hierarchy of control measures when identifying risk treatment processes and options. The hierarchy of control measures promote elimination as the most effective way to control risk, where this is not reasonably practicable, reduces the risk.

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

The hierarchy of control measures includes:

- Elimination
- Substitution
- Isolation
- Engineering controls
- Administrative controls
- Personal protective equipment (PPE)

Risk treatment processes include:

- Formulating and selecting risk treatment options
- Planning and implementing risk treatment
- Assessing the effectiveness of that treatment
- Deciding whether the remaining risk is acceptable
- If not acceptable, taking further treatment

Risk treatment options include:

- Avoiding the risk by deciding not to start or continue with activity that gives rise to the risk
- Increasing the risk to pursue an opportunity
- Removing the risk source
- Changing the likelihood (mitigating risk)
- Changing the consequences (mitigating risk)
- Transferring or sharing the risk
- Retaining the risk by informed decision

Individual risks may include compressive treatment through controls applied holistically.

#### 2.4.5 Recording and reporting (review control measures)

Identified risks and control measures should be accurately recorded and reported. HHSs should:

- Record findings, ratings, and protective security treatments and administrative controls (such as governance, personnel, response procedures and the layering of physical controls)
- Communicate risk management activities and outcomes to stakeholders
- Provide information for decision-making
- Improve risk management activities

Controlling risks is an ongoing process. Controls must be reviewed regularly to maintain their effectiveness. For information regarding the WHS risk register and WHS risk profile please see [QH-GDL-401-3-1:2021](#).

**Protective Security Policy Framework, Security planning and risk management**, states:

*“A security plan specifies the approach, responsibilities and resources applied to managing protective security risks. The security plan allows entities to review the degree of security risk that exists in different areas of operations and take action to mitigate identified risks.”*

### Example Security Risk Assessment Template

Please see [Appendix 10](#) Example Security Risk Assessment templates as a method to record the security risk assessment process. Please copy, paste, and add lines where required.

## 3. Developing a security plan

HHS security management should develop a security plan to articulate how security risks are controlled within all facilities in consultation with Security Manager/Security Administrator (or equivalent position/position assuming this function) and relevant stakeholders. HHS security plans should summarise the security measures applied to protect key functions and assets against identified security risks. Where a single security plan is not practical due to the size or complexity of the HHS and its facilities, consider developing an overarching HHS security plan supported by more detailed facility level security plans.

### 3.1 Frequency and retention

HHS security plans should be informed by security risk assessments and reviewed at least **every two years** or where changes to the risk environment are identified. Each HHS or facility should determine how the security plan will be reviewed. The review should be facilitated by the personnel responsible for security management and include input from local stakeholders. The security plan is to be retained in accordance with the [Corporate records management policy framework](#).

**Whilst not mandatory, guidance maybe taken from the Protective Security Policy Framework: Supporting Requirements | Requirement 1 - Security Plan Review**, which states:

*“The security plan (and supporting security plans) must be reviewed at least every two years. The review process must include how the entity will:*

- a. Determine the adequacy of existing measures and mitigation controls, and*
- b. Respond to and manage significant shifts in the entity’s risk, threat, and operating environment”*

## 3.2 Contents

HHS security plans should include specific security requirements and mitigation strategies such as physical security controls and SOPs appropriate to threat levels and risk tolerances. Procedures may include how security personnel are used, emergency response, and the organisations response to emerging threats including increased criminal activity and change in the risk environment or business impact levels.

Please see [Appendix 11](#) 'Business impact levels for consequence of threat'.

The HHS security plan may detail:

- The security goals and strategic objectives of the HHS, including the fundamental principles and how security risk management intersects with and supports broader business objectives (including links to business continuity planning and disaster management)
- The security risk environment including threats levels that may potentially impact the protection of people, information, property, and assets
- The **risk tolerance** of the HHS (the level of acceptable risk after risk treatment and managing the residual risk at a level that is as low as reasonably practicable)
- The **risk appetite** of the HHS (the amount of risk that is accepted or retained to achieve objectives and includes risk appetite and tolerance statements that describe approach adopted towards risk taking).

Please see [Appendix 12](#) Risk appetite and risk tolerance levels



**Figure 5:** Security planning and risk management example of risk tolerance regions

- The maturity or progress in achieving a positive security capability to:
  - Minimise harm
  - Manage security risks
  - Maintain a positive security culture
  - Respond and learn from incidents
  - Achieve security outcomes while delivering business objectives
  - Identify areas for improvement

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

- Other considerations may include:
  - Governance arrangements
  - Information security (ICT)
  - Personnel security
  - Physical security

HHS security plans should also consider how to manage, avoid, or minimise risks that may jeopardise the safety and security of people.

**AS 4485.2:2021, s 6.3 Nature of risks,** states:

*“Risks to people within healthcare facilities rise from a number of factors including:*

- a) *The nature of the facility*
- b) *Location and design of the facility*
- c) *The prominence of the facility*
- d) *The facility’s workers profile*
- e) *Access to the facility*
- f) *The facilities emergency department*
- g) *The facilities holdings of drugs and pharmaceuticals*
- h) *The inclusion of mental health services, drug rehabilitation, maternity, nuclear medicine, and newborn services or other high-risk services on the facilities premisses or in close proximity; and*
- i) *Workers working alone”*

**AS4485.2:2021, s 6.3 Risks to people,** states:

*“Risks encountered by people in healthcare facilities could include:*

- a) *Aggression towards patients by other patients, workers, visitors, or intruders*
- b) *Aggression towards workers, by patients, other workers, visitors, or intruders*
- c) *Aggression towards visitors by patients, workers, other visitors, or intruders*
- d) *Abduction of patients (including infants), visitors or workers*
- e) *Loss or damage to property belonging to workers, patients, or visitors and*
- f) *Acts of terror”*

Please see [Appendix 13](#) ‘Special security considerations’ for more information.

### 3.3 Physical security controls

HHSs should use physical security controls to protect assets, people, property, information, activities, and reputation. HHS security management should implement physical security controls that are

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

informed, implemented, and monitored through local security risk management processes. Please see Part B: [Controlling risks through physical security](#).

## 3.4 Procedures

HHS security risk assessments should also inform SOPs (or equivalent documents). The SOPs should support the overarching security plan and be aimed at reducing or eliminating threats, strengthening existing controls, and ensuring a safe environment. This is achieved through layering of control measures and clear instruction. SOPs may be implemented to address the specific needs of individual facilities and services regarding physical security controls, local practices for security personnel, or functions of the Healthcare Security Officer (HSO) role. Part C: [Standard operating procedures for healthcare environments](#) may assist local security management in reviewing or establishing SOPs.

## 3.5 Protection of information

In accordance with [Information security policy QH-POL-468:2019](#), HHSs should comply with applicable legislative and regulatory security requirements, manage information security risks effectively, reasonably establish an effective information security culture and regularly review and improve information security performance and capability.

HHSs should ensure that security risk assessments, plans, and supporting documents are developed in compliance with relevant legislation, information security standards and policies. Information that may require protection might include, but not be limited to, management documents relating to sensitive plans, policies, finances, and other matters associated with running the healthcare facilities, and patients' and staffs' personal records.

The *Hospital and Health Boards Act 2011* (Qld) deals with confidentiality and the responsibilities of the health service and workers to protect information.

Specifically, section 142 of the *Hospital and Health Boards Act 2011* (Qld) prescribes:

“Confidential information must not be disclosed by designated persons

*(1) A designated person must not disclose, directly or indirectly, confidential information to another person unless the disclosure is required or permitted under this Act...*”

The *Information Privacy Act 2009* (Qld) deals with information privacy as it relates to the fair collection and handling in the public sector environment of personal information.

HHSs should seek advice where they are uncertain as to the nature or status of information.

### 3.5.1 Documentation planning (information security)

HHSs and workers should comply with the [Information security user responsibilities standard QH-IMP-066-2:201](#). This standard identifies responsibilities for users regarding information security. A security risk assessment may also identify additional controls necessary to address risks:

- **Security risk assessments, security plans, SOPs (or equivalent documents)** should include responsibilities for information security management where appropriate. This may include:

- Risk rating or business impact levels
- Publishing considerations or protections
- Sponsors, delegations, and author / custodian responsibilities
- Consultation strategies and dissemination approval
- Document control and coordination
- Plan for retention, review, and frequency (including arrangements for storage and storage of duplications for business continuity)
- **Security of personal health information** must have appropriate protections to avoid unauthorised practice, disclosure, loss, or other misuse and to promote secure storage of this information with appropriate access restrictions
- **Disclosure and information management** may take guidance from the Office of the Information Commissioner Queensland in relation to privacy legislation in Queensland (Office of the Information Commissioner Queensland)

For operational guidance regarding video surveillance system information (VSS) and security-controlled information access, storage, disposal and other reporting and documentation, please see Parts B and C, [Controlling risks through physical security](#) and [Standard operating procedures for healthcare environments](#).

## Part B: Controlling risks through physical security

### 1. Introduction

Physical security refers to the combination of physical and procedural measures used to prevent or mitigate threats or attacks against physical assets, information, and people.

This section outlines physical security controls that can be implemented by HHSs. These controls equip facilities with resources to maintain a safe and secure environment for all occupants and to protect property and assets.

This section considers risk-informed physical security controls and security equipment that deter, detect, and delay security incidents within HHSs. These controls also enable an informed response and recovery from security incidents.

Minimum requirements should be implemented in accordance with legislative obligations and accreditation recommendations in a manner consistent with [Department of Health Strategic Plan 2021–2025](#) objectives to ensure the safety and security of workers, patients, visitors, members of the public, property, and assets, are also outlined in this section.

This section aligns with Queensland [Health, safety and wellbeing management system](#) and utilises elements from relevant Australian Standards to inform recommended physical security controls.

**Australasian Health Facility Guidelines** defines ‘physical security’ as:

*“That part of security concerned with physical measures designed to safeguard people, to prevent unauthorised access to equipment, facilities, material, and documents, and to safeguard against damage and loss.”*

## 2. Physical security controls in the healthcare environment

HHSs should consider physical security controls that contribute to a healthcare environment consistent with a ‘person-centred care’ approach. This approach aims to support various services in providing safe, quality health care experiences that respects a person’s individual preferences, needs, and values.

The following is taken from Australian Commission on Safety and Quality in Health Care. Person-centred care:

*“...Key dimensions of person-centred care include respect, emotional support, physical comfort, information and communication, continuity and transition, care coordination, involvement of carers and family, and access to care.*

*... There is good evidence that person-centred approaches to care can lead to improvements in safety, quality, and cost effectiveness, as well as improvements in patient and staff satisfaction.”*

To effectively implement controls which enable the delivery of ‘safe’ person-centred care, HHSs should consider promoting:

- The safety of staff delivering care
- A safe environment in which care can be delivered, and
- The safety of those receiving or accessing care and visitors



HHSs should consider the use and placement of physical security controls as well as the impact of controls or how controls may be perceived by consumers in the healthcare environment.

**See Think Act** 2<sup>nd</sup> Edition is a handbook for people who work in secure mental health services. Published by the Royal College of Psychiatrists Quality Network for Forensic Mental Health Services, the handbook states:

*“Security provides the framework within which care, and treatment can be safely provided. Neither patients nor staff can participate positively in the activities of the service unless they feel safe first. There are three distinct but inter-related elements of security in a secure mental health setting. They are:*

- *Relational security*
- *Procedural security (the policies and procedures in place to maintain safety and security)*
- *Physical security (the fences, locks, personal alarms and so on that keep people safe)”*

**AS 4485.2:2021, s 6.3: Risks to people** states:

*“Risks encountered by people in healthcare facilities could include:*

- *Aggression towards patients by other patients, workers, visitors, or intruders*
- *Aggression towards workers, by patients, other workers, visitors, or intruders*
- *Aggression towards visitors by patients, workers, other visitors, or intruders*
- *Aggression towards patients by other patients, workers, visitors, or intruders*
- *Abduction of patients (including infants), visitors or workers*
- *Loss or damage to property belonging to workers, patients, or visitors and acts of terror”*

HHSs should consider the use of physical security controls including but not limited to:

- Controls applied to reduce triggers for conflict and vulnerabilities and improving perceptions of safety through the design of areas (e.g., incorporating the use of barriers, lighting, and signage in waiting and reception areas)
- Controls applied to minimise the risk of unauthorised access and the illegal removal of babies and children from maternity and paediatric units (e.g., secure areas with proximity swipe card access)
- Controls applied to aid in providing safe care to patients with mental health, cognitive impairment or patients who may be at risk from wandering or absconding (e.g. workplace design factors inclusive of the layering of security controls with crime prevention through environmental design concepts)

- Controls applied to aid in providing safe care to patients with behavioural disturbances or patients in custody who may require increased observation (e.g., the ability to increase security presence (security specials) and video surveillance systems)
- Controls applied to mitigate risks associated with the safe and secure storage of pharmaceuticals, currency (cash), weapons, and illicit substances (e.g., secure containers, safes, or drug storage cabinets)
- Controls applied to contribute to the safety and security of high-risk areas such as Emergency Departments and acute mental health units and inpatient settings (e.g., use of barriers, airlocks, and duress systems)

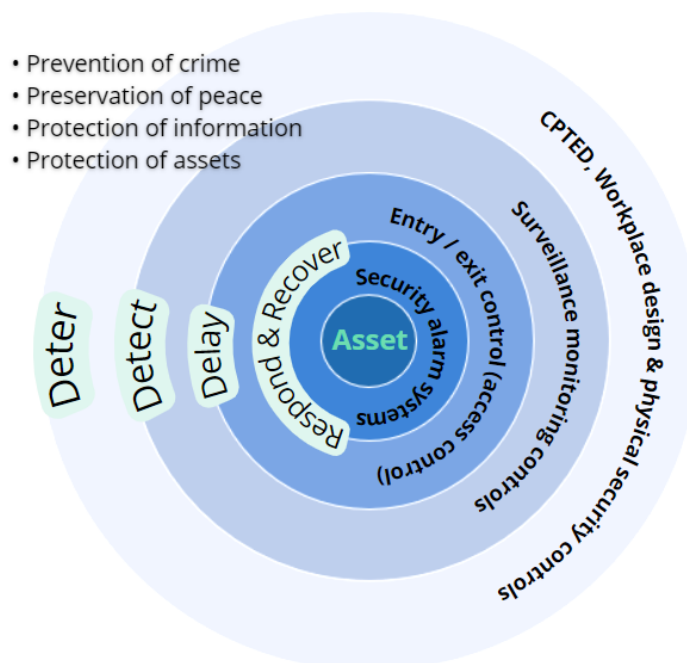
### 3. Physical security controls, equipment, and concepts

HHSs should use physical security controls to protect assets, people, property, information, activities, and reputation. Security management within the HHS should be consulted in developing, implementing, and monitoring informed security controls, as well as associated security risk management processes.

Physical security controls may include restricting movement of people; influence over healthcare environment activities, and the use of physical security.

HHSs should consider:

- **Crime Prevention Through Environmental Design (CPTED)** concepts that inform the placement of physical security controls and environment
- Workplace design to deter, delay and minimise potential criminal and antisocial activity
- Monitoring and response controls designed to detect security issues and enable an adequate response to emergency events, and to recover evidence (post event)
- Entry/exit control (access control) designed to deter, detect, and minimise the potential for unauthorised access, thus minimising potential exposure to crime
- Security alarm systems inclusive of duress and intruder alarm systems enable appropriate responses to security incidents

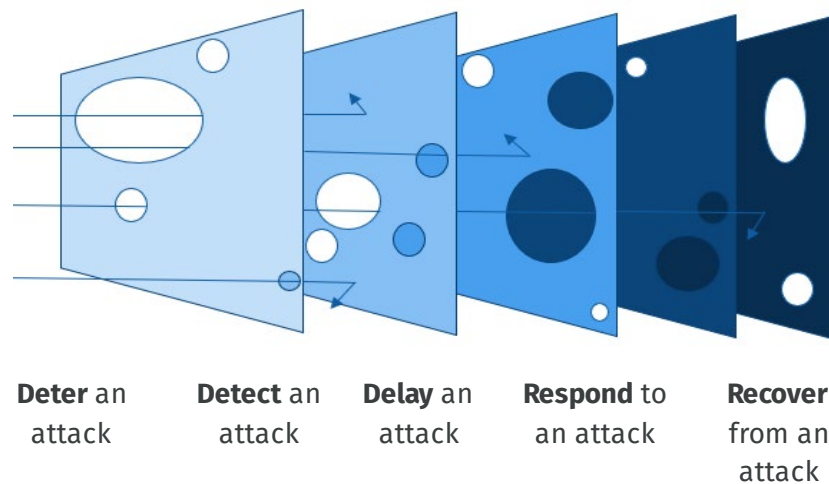


**Figure 6:** Layering concepts and controls

**HB 167, s 4.5: Conducting the vulnerability analysis** states:

*“No matter how many layers are in place or how well constructed they are, they cannot be one hundred percent effective for one hundred percent of the time. Borrowing a safety model developed by James Reason (Human error, Cambridge CUP, 1990) each layer of security controls (or counter measures) will resemble a slice of swiss cheese, with holes of varying size through it. Under normal circumstances the holes are covered subsequent layers of controls. However, under certain circumstances the holes in all layers will line up and all defences can be penetrated...”*

A well-informed vulnerability analysis identifies weakness or gaps within existing controls and offers the opportunity to address short falls.



**Figure 7:** Determining vulnerability HB167

Consultation with healthcare security services is crucial when making changes to the workplace or undertaking works that impact existing security controls. Consultation with local security professionals ensures all reasonably foreseeable risks are minimised and controls are considered in the initial planning for new buildings or redevelopment and refurbishment of existing buildings. This ensures risks are controlled effectively and that new risks are not introduced.

Workers who work in the subject area environment or discipline should be consulted as often these workers best placed (i.e., security professionals) to offer insight into identifiable risks, as well as relevant and solutions. Collaboration and information sharing across workplace health and safety (WHS) professionals, clinical, and operational staff optimises the effectiveness of risk control measures.

**Queensland Health – Capital Infrastructure Requirements: Volume 1 – Overview** states:

*“s 2.7.4 Undiminished safety, Redevelopments including new additions shall not diminish the safety level that existed prior to the start of the work”.*

*“s 5.3 Work health and safety, project managers, design managers, architects, engineers and others involved in the design process, have an important role to play in identifying health and safety risks that could arise throughout the life cycle of the building or structure and, where practicable, eliminating risks through design.”*

### 3.1 Crime Prevention Through Environmental Design (CPTED)

CPTED (pronounced “sep-ted”) is a multi-disciplinary approach to address potential criminal behaviour utilising design strategies that focus on influencing a potential offender’s decisions that precede potential criminal activities and creating an environment that minimizes occurrences. CPTED aims to reduce the likelihood of threats such as: trespass, wilful damage (vandalism), stealing (theft), stalking, arson, and/or assault.

**Australasian Health Facility Guidelines 2018** states:

*“...incorporating CPTED can significantly reduce real or perceived fear and risk of crime as well as the considerable costs associated with adding security equipment and personnel after an incident has occurred or in response to changing standards”.*

**AS 4485.2:2021 s 4.2.2 Crime prevention through environmental design, 4.2.2.1 Overview** states:

*“The location of some departments will warrant special consideration in the furniture design and access / exit requirements. Placement of windows, doors, furniture, and fittings can influence the level of security within a site. Likewise, the facility’s grounds design and vegetation can impact on both personal and property security”.*

#### 3.1.1 CPTED Concepts

CPTED concepts maximise the risk to offenders by increasing the likelihood of detection, and effort required to commit crime through:

- Territoriality and ownership
- Natural surveillance and lighting
- Natural access control
- Image, management, and maintenance

Combining CPTED concepts can reduce a facility's vulnerability by eliminating spaces that are isolated, devoid of people, reducing areas of potential concealment or entrapment and addressing areas that provide opportunities for unforeseen crime to take place or make it difficult for others to respond or provide help.

### **Territoriality and ownership**

Territoriality and ownership can be increased by establishing clear barriers and distinction between public and staff only areas. This encourages staff adopted ownership and control of their work areas, which translates into:

- Staff occupying an area taking responsibility for their safety and security
- Easy identification of intruders
- Challenging of unauthorised access and discouraging trespass

### **Natural surveillance (passive surveillance)**

Natural surveillance encourages people to feel safe in public areas where they can be seen and interact safely with others. This is achieved through the following considerations:

- Maintaining open view or line of sight through discouraging the use of large obstructive plants and the like which block the view of observers from buildings, CCTV, and lighting. The ideal view is one that is well light and free from obstacles
- Avoid establishing isolated or hidden spaces which create a risk of concealment. This may include recessed doorways, corners and voids in building hidden from view
- Promote trimmed or well-maintained plants, both existing and planned. Flora should be selected and planted so not to obstruct view
- Eliminate isolated routes particularly paths that are predictable or do not offer alternative pedestrian routes
- Promote effective lighting to prevent undesirable activity and increase the potential for activities to be observed by staff



**Figure 8:** Surveillance principle (buildings and public areas are positioned to maximise passive surveillance) (Crime Prevention Through Environmental Design Guidelines for Queensland)

### Natural access control

Natural access focuses the movement of people by strategically directing them towards areas of natural surveillance. This may include physical elements such as doors, fences, strategically placed shrubs and hedges, walls (ideally transparent), and barriers to guide movement.

Natural access is supported through:

- Effective use of sensor lighting, landscaping, and furniture
- Limiting the number of access and egress points to discreetly direct both foot and vehicular traffic in ways that decrease the potential for opportunistic crime
- The removal of natural ladders (objects that may be climbed or used to climb)

### Image and management / maintenance

Promoting a positive image and the appearance of routine maintenance to ensure operationally functional and to transmit a positive perception of the area serves as an expression of ownership and encourages the above points to be adopted more easily by more people. Examples of this may be removing graffiti and repairing broken windows and features.

**HB 188:2021 s 4.3 Controls in building design** states:

*“For building owners, the primary goal of CPTED is to deter offenders from attempting attacks. CPTED will not stop a determined attacker as the sole solution. It is part of the broader security design to enhance security features.”*

## 3.2 Workplace design

HHS facilities should consider several options to achieve an optimal combination of security arrangements. Design should be based on the principle that the management of security risks is not achieved by technology or staffing alone, but rather a combination of factors and with adequate consultation.

**Australasian Health Facility Guidelines 2018**, states:

*“...this element refers to the physical security that is afforded by the way in which buildings are planned and constructed, providing access paths both vertically and horizontally through openings for both pedestrian and vehicles, and including considerations of service’s penetrations and the use of clear lines of sight to reinforce natural surveillance”.*

HHS environments have different functional areas that will have unique requirements or considerations for security services and secure design features.

Factors which HHSs should consider at the design/concept stage or in response to security risk assessments may include, but are not limited to:

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022



### 3.2.2 Lighting

HHS facilities should establish and maintain external lighting systems as follows:

- Illumination to all areas of access/egress, parking and any other service or activities provided by facilities
- Lighting that is effective at deterring potential intruders and enhances the possibility of detection
- Lighting that is sufficient for safety and security whilst having low energy consumption and - where practical - connected to an UPS.
- Ensure lighting supports surveillance and does not jeopardise visibility.

#### Lighting:

- Example of overlapped lighting for consistent illumination for pedestrians



**Figure 10:** Example lighting (Crime Prevention Through Environmental Design Guidelines for Queensland)

Further information can be found in [Appendix 16](#) AS4485.1 Security lighting levels standards relating to lighting:

- **AS/NZS 1680.1:2006: Interior and workplace lighting** Part 1 – General principles and recommendations, sets out general principles and recommendations for the lighting of interiors of buildings for performance and comfort
- **AS/NZS 1158.12.2-2012: Lighting for roads and public spaces** – Vehicular traffic (Category V) lighting – Guide to design, installation, operation, and maintenance

### 3.2.3 Barriers

Purposely designed barrier protection may include fences, walls, gates, boom gates, permanent bollards, guard, and handrails. HHSs should consider establishing appropriate barriers to guide traffic and control risks related to pedestrian safety, accidental vehicle collision or hostile vehicle mitigation.

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022



Establishing barriers can increase the protection of access points, critical assets, and infrastructure such as fuel and gas tanks, water mains, fire suppression systems, and other vulnerable areas such as reception, waiting rooms and cash and drug holding areas. There are various forms of barriers available for HHS consideration.

**Passive barriers:** such as trees, benches, sculpture features and statues, walls, bus shelters and light or sign poles and so on may be effective at protecting assets if reinforced, however static.

**Active barriers:** such as retractable bollards, drop arm barriers, sliding gates provide the dynamic use capabilities.

### 3.2.4 Signage

Signage can be used to inform or direct staff, visitors and others or warn of restrictions or potential danger. HHSs should use signage with printed display characters or fonts of sufficient size to allow the message to be read at 10 metres by a person with normal sight and placed at a height of 1.5 metres.

The colours used for signage should be in accordance with the Queensland Health conventions and in all cases the message text shall contrast sufficiently with the background to be clearly legible to the observer. Colour combinations that present a challenge for people with visual impairments or an inability to perceive certain colours should be avoided. Signage can be one method to regulate and control safety related behaviour, to warn of hazards and to provide emergency information.

**AS 4485.2:2021 s4.2.2.5 Signage**, states, *signage is critical for CPTED principles of territorial definition, access control and activity support.*

For further information regarding [wayfinding](#), please see [Queensland Health Wayfinding Design Guideline](#). Wayfinding design incorporates coordinated design elements that assist wayfinding including the built environment, signage, type of signage, terminology, and location.

## 3.3 Monitoring and response controls

### 3.3.1 Video surveillance systems (VSS) / Closed circuit television (CCTV)

HHS should consider establishing VSS or and CCTV as necessary to enable surveillance of at-risk areas. In Health Services, such areas may include:

- Entrances and foyers
- Mental health facilities
- Reception areas and waiting rooms
- Car parks, passageways thoroughfares
- Pharmacy department counter
- Emergency department
- Paediatric areas
- Other high-risk areas (as informed by security risk assessments)

CCTV may also be used in conjunction with alarm systems and access control systems enabling a response assessment to alarm activation or identification regarding entry/exit activities. It is best practice to display appropriate signage advising people that cameras are in use.

Access to footage should be restricted to authorised persons only and may be provided to the Queensland Police Service (QPS) or other regulatory bodies or law enforcement agencies as required by law (such as Crime and Corruption Commission (CCC) and other government departments).

**AS 4485.2:2021 s4.3.9 Video surveillance**, states: *“For the safety of workers and for maximum effectiveness, a VSS should be monitored by a competent person able to respond to incidents or report the incident to someone who can respond”.*

Installation, management, and use of video surveillance must be in accordance with the *Hospital and Health Boards Act 2011 (Qld)*, *Crime and Corruption Act 2001 (Qld)*, *Right to Information Act 2009 (Qld)*, *Public Records Act 2002 (Qld)*, *Information Privacy Act 2009 (Qld)*, *Privacy Act 1988* and Australian Privacy Principles that govern standards, rights, and obligations around:

- The collection, use and disclosure of personal information
- An organisation or agency’s governance and accountability
- Integrity and correction of personal information
- The rights of individuals to access their personal information

#### **Surveillance system signage**

Signage to advise that VSS/CCTV systems are in operation is to:

- Be in accordance with the Information Privacy Act 2009 (Qld)
- Displayed in public areas at consistent intervals
- Be placed in line of sight or in a way that limits visibility by the public

### **3.3.2 Security equipment**

Security equipment should be obtained from reputable suppliers only. Where possible, HHSs should adopt an integrated approach to security, ensuring new/additional equipment is either compatible with existing equipment, systems, and processes, or does not hinder or disrupt their effectiveness or function. The security equipment and its installation should comply with all relevant standards and manufacturer’s recommendations.

Consider the following criteria in selecting a reputable supplier and/or security installer:

- Willingness to use only quality security equipment which is fit for the purpose and meets appropriate industry and Australian Standards

- The company's previous experience in supplying/servicing public or private health care organisations

**AS 4485.2:2021 s5.6 Equipment**, states:

*“Healthcare facilities should identify and periodically review the safety clothing and equipment requirements of security officers through a security risk assessment”.*

Security equipment may include, but may not be limited to:

- Torches, ligature cutting tools and notebooks
- Load bearing safety vest (or equivalent) and duty belts (at the discretion of the HHS)
- Personal duress devices and means of communication such as phones, mobile phones, pagers, and two-way / radios see [Appendix 14](#) A guide for two-way / radios communications
- Personal protective equipment (PPE): eye protection, face, shields, hi-vis vests, wet weather gear, and gloves (disposable and needle stick resistant)
- Body worn cameras (BWC). Refer to [Appendix 15](#) A guide for BWC procedures

Equipment should be carefully selected to ensure the control's capability effectively mitigates the identified risks and does not introduce new risks. HHSs should determine what equipment is individually provided for personal use and what equipment is shared provided to the security team or service).

Procedures relating to equipment should include the following topics as a minimum:

- Equipment uses and training
- Storage, cleaning, and maintenance
- Equipment inspection, collection and return practices (start and finish of shifts for shared equipment or at separation for individually provided equipment)
- Expectations for reporting of damages for equipment replacement

### 3.3.3 Body Worn Cameras (BWC)

BWCs can be used within healthcare facilities is to allow surveillance of public or high-risk areas and activities from the point of view of the wearer. BWCs are utilised only by clearly identifiable healthcare and appointed Security Officers or other authorised persons (under the *Hospital and Health Boards Act 2011* (Qld)). BWCs are to be used as an overt audio and visual recording device and are not permitted to be used in a covert manner. The three primary objectives which define the purpose of BWCs use are to:

- Act as a deterrent to unwanted behaviour of persons
- Gather evidentiary and intelligence material, which may be used in debriefs, investigations, and training, other practice improvement actions
- Enable a self-check mechanism for HSOs involved in acts associated with their role where they may be open to allegations of misconduct, whether those allegations are genuine or vexatious in origin

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

A key benefit to the functionality of BWCs compared to most static video surveillance equipment, is that BWCs also record sound, thereby ensuring the dialogue and other audible evidence associated with an incident can be captured and reviewed.

The use of BWCs has proven effective in providing video and audio evidence of interactions with patients, staff, and visitors. [Axon Body 2 and 3](#) are widely used by HHSs across QH.

BWCs can reduce the frequency and severity of incidents leading to violent confrontations, thus minimising the execution of skills involving the use of force and reducing the likelihood of complaints against clinical staff and HSOs. Footage collected through the activated BWC device is uploaded on a secure cloud storage via a docking station. Data saved to the cloud is uploaded automatically and managed and shared from the website. Please see [Axon Evidence](#) for information regarding granting access, sharing data, and general storage and use of videos, photos, and documents.

Please see the standing offer arrangement (SOA) number QPS15167 Evidence Management System and Related Products regarding arrangements for the provision of BWC hardware, software, data storage, support services, transition services, implementation services, training and ICT contracting services. To check if this is the current provider, please follow this link to [Search Offer Arrangements](#) or go to [govnet.qld.gov.au](http://govnet.qld.gov.au).

### 3.4 Entry / exit control (access control)

**HB188:2021 Access control**, states: “A deterrence effect can be increased by lowering the perceived viability of gaining access... Detection capabilities may be achieved using onsite security personnel or security system technology, such as alarm systems or electronic access control systems”.

HHSs should consider what type of access control restriction is suitable and most effective for areas, dependant on the intended restriction of the access point. This may be determined by a security risk assessment.

Access control systems may utilise numerous methods to facilitate security access to authorised persons and to restrict unauthorised persons from accessing areas or access to areas at designated times (such as the case for in patient areas that lock down outside of visiting times). Examples of secure access include:

- Proximity card / swipe card / bar code card / magnetic card
- Keypad PIN entry
- Key lockable doors, locks combination, pad locks etc

HHS work unit managers and the nominated person must be informed as soon as possible if a key or an electronic access control device be lost or damaged or if a PIN is compromised.

A staff separation or termination should allow work areas or units to remove individual access from workers whose employment has ended. Keys, proximity cards, ID cards (and so on) must be returned, the staff member’s credentials removed from access-controlled areas and information removed from staff databases.

Access control systems allow entry, exit, and door activity audits to be carried out on any controlled area. Work unit managers may request any such audits and should be accompanied by a request for electronic information for auditing purposes.

Security controlled access doors may be fitted (in some circumstances) with a remote door lock mechanism. This mechanism can be used to remotely lock or unlock a door to permit or deny access to persons to within an access-controlled area. Doors fitted with remote door locking mechanisms should be managed according to a locally developed access control protocol.

Keys, PINS or codes, proximity swipe card and the like should not be duplicated or communicated to any other person than to whom the access was granted.

### **Restricted areas**

Each HHS determined the appropriate resourcing for restricted areas. A restricted area may be considered burglar or intruder resistant (in part or in full) and if it possesses any of the following physical security features in line with AS4485:

- Specific controls established to restrict unauthorised access
- A means to identify authorised persons
- Video surveillance options
- A means of logging or recording access (entry / exit)
- A means of raising the alarm in the event of forced entry
- Signage indicating restricted access
- Tamper evident barriers, highly resistant to unauthorised entry/exit, with no unsecured openings
- Video surveillance and security alarm system with reliable communications link to an effective response

Access control to specific functional areas may require stronger considerations towards the level of restrictiveness. These areas include but are not limited to laboratories, pharmacies, clean utility and medication rooms, mortuary, mental health inpatient units, and plant rooms.

This action reduces potential risks to these areas may include unauthorised access, contamination of sterile areas, theft of medical supplies and restricted substances, theft of sensitive information, theft of personal belongings or medical equipment, threats, and acts of violence or potential disruption or cessation of critical infrastructure.

Areas applying physical security controls as treatments to risks should measure against the criticality, vulnerability of the areas, asset, and capability of the physical security controls.

Unauthorised entry could severely disrupt operations through malicious damage or deliberate attack. Typical control measures to restricted areas may include the following considerations:

- Plant room doors should be secure by construction
- Plant room doors which open into publicly accessible spaces may be alarmed to trigger a security response, alarms may be linked to CCTV systems to record and audit access

- Where practical plant rooms should be designed in a manner to prevent, deter or delay forced entry or wilful damage

### 3.4.1 Proximity swipe cards

HHSs should consider proximity swipe cards for ease of authorized access to restricted access points. Proximity cards offer the highest level of access security, allowing for individualised access restrictions based on the role and requirements of the user. Security is strengthened through the ability centrally manage activation and deactivation of cards, as well as the removal of human error and issues attributed to uncontrolled sharing of PIN codes. These systems are usually highly traceable, adding to ease of auditing with high accuracy.

### 3.4.2 Keypads

HHSs should consider keypads where proximity swipe card are not appropriate. PIN key locks (i.e., keypad locks) provide manual security measures to areas of a lower security risk. PIN codes should be changed regularly to prevent obvious wear on individual keys. A register of all PIN codes should be maintained by the responsible HHS department. PIN key locks should have a key override facility, being keyed to the facility master key provided to authorised personnel in the area. A list of names of personnel to which the PIN has been provided should be maintained.

**AS 4485.2:2021 s4.3.313.2 Setting the lock**, states: *“Although the setting of a combination lock could be jeopardised by the careless or negligence of users, combination locks can offer a greater level of control and convenience than key locks of equivalent quality”.*

### 3.4.3 Locks and combination locks

**AHFG:2018, s3.5.2 Doors, Security Issues**, states: *“As a risk management measure, all perimeter doors should be provided with locks to prevent unauthorised entry or exit. In the case of openings into a secure area or courtyard, security may still be breached in a variety of ways. Any decision to omit locks should be formally recorded.”*

HHSs should assess the need to implement locks and combination locks to restrict access to assets. Locks to all intruder-resistant and restricted areas should comply with the requirements of AS 4145.2 (Durability D3, Physical Security S3 and Keying K6) level 3 and AS 4145.2 (Durability D1, Physical Security S1 and Keying K3) level 1.

**AS 4145.1:2008 Locksets and hardware for doors and windows**, sets out requirements for mechanical locksets for doors and windows in buildings, specifies general design criteria, performance requirements, and procedures for testing mechanical locksets for their resistance to forced or unauthorised entry and efficiency under conditions of light to heavy usage.

### 3.4.4 Doors and windows (intercom systems)

HHS security risk assessments may identify the need to replace timber doorframes with a more durable material, such as a metal frame, to prevent manipulation or wilful damage.

Security guidelines

HHSs should ensure suitable provisions are made for afterhours use. Where perimeter doors are locked afterhours, consideration should be given to providing an intercom or tele-intercom device to allow staff to be alerted to and communicate with people seeking entry. It may be necessary to provide CCTV coverage of such doors and allow the caller to be observed and identified before being allowed entry. Entry and exit into a facility or department within a facility should be limited to appropriate numbers (not excessive) and with monitored access control where practical.

Where a security risk assessment identifies that additional window reinforcement is required, consideration may be given to applying shatter resistant film to glass, having glass replaced with laminated glass, or installing security grilles.

All glazed panels that are subject to potential damage / breakage, including doors, sidelights, windows, and balustrades, should be selected based on their capacity to achieve the following objectives:

- Prevent risks of patients accessing authorised personnel / staff only areas (restricted areas)
- Prevent risks of patients absconding or self-harming
- Avoid unintentionally impacting on staff access to safe place (potentially during times of duress)

**AHFG:2018 s3.5 Doors and associated hardware**, states: *“As a risk management measure, all perimeter doors should be provided with locks to prevent unauthorised entry or exit. In the case of openings into a secure area or courtyard, security may still be breached in a variety of ways. Any decision to omit locks should be formally recorded.”*

For improved safety and security, HHSs should consider safety glass, laminated glass, or impact resistant transparent panels (i.e., plastics) applied to glazed windows and glass panel doors in high pedestrian traffic areas and main access points.

**AHFG:2018 s3.9 Window types**, state: *“...To prevent unauthorised access through windows, a restriction device should be used. This applies particularly to areas that may accommodate children or people with cognitive impairment or mental illness. Refer: AS2047 Windows in Buildings - Selection and installation.”*

Safety glazing materials consist of laminated, wired glass, toughened, plastic materials (polycarbonates) and films. Some of these are defined in AS/NZS 2208:1996 Building safety materials.

Further information can be found in standards relating to windows including:

- AS 1288: Glass in Buildings - Selection and Installation
- AS 2047: Windows in Buildings - Selection and Installation
- AS/NZS 2208: Safety Glazing Materials in Buildings.

### 3.4.5 Key management

HHS should establish a key management system to control access. The system should enable original and duplicate key control system for keys to various departments and areas within the facility. HHS facilities should seek to limit the number of keys issued (within departments), and consider using a

Security guidelines

master key system. Keys to pharmacies and other drug storage and sensitive areas should not be part of the master key system, as access to these must be strictly controlled to prevent unauthorized access.

A key management procedure should require persons seeking temporary access to keys to sign for their collection and return. The key management responsibility may sit with different departments across each HHS. HHS key managements systems should consider the issuing of keys on a long-term basis and key registration processes.

### **Key registers**

A register of all keys issued is to be maintained within the facility. Requests for keys are to be signed by the head of department of the person requesting the key. In some cases, keys are required for short periods of time (e.g., by contractors), the return of the keys in these instances is to be closely monitored by staff.

### **Key issue – long term**

Some HHSs may consider issuing keys to certain staff on a long-term basis. This arrangement must include strong management and monitoring by the delegated unit response for key management. Long term key issue processes should include:

- a. Record receipt and return
- b. Regular audits to be carried out
- c. Procedures for reporting lost/stolen keys
- d. Procedures for keeping key issues appropriate and current
- e. Satisfactory security for the key

## **3.4.6 Security containers, cabinets, safes, and vaults**

Where appropriate HHSs should establish security containers that are designed for the safe custody of small and attractive assets (vital to operations or of high monetary value), money, and classified material. Security containers are designed in accordance with Commonwealth Government design parameters.

Safes and vaults provide varying degrees of protection depending on the construction and may be used to store valuable physical assets. Further guidance is available in AS3809 Safes and strongrooms.

Please see [Appendix 17](#) Selecting commercial safes and vaults to protect physical assets, other than classified assets, for minimum commercial safe and vault requirements in the applicable zones based on business impact level.

HHS should consider implementing secure receptacles / drop safes to assist with the safe storage of illicit drugs and weapons. These containers are heavily restricted. For further information please see section [Controlling risks through physical security, weapons and dangerous items \(illicit substances\)](#).

## **3.5 Security alarm systems**

### **3.5.1 Duress alarm systems (personal or mobile devices and fixed systems)**

Duress alarms may be necessary for the personal safety of staff working in areas subject to real or potential violence or aggressive behaviour. HHS should consider the following recommendations for duress use and installation:



- Decisions regarding installation and response may be informed by a security risk assessment
- Duress systems should be easy to operate
- Duress systems (buttons) should be easily identifiable, and staff should be orientated on their location and use
- The placement of the alarms needs to be considered carefully before installation to promote identification and reduce accidental activation (false alarms). Points to consider are accessibility, especially under stress, whether the alarm is silent or audible and type (e.g., button, knee or foot activated)
- Duress alarms are only as effective as the response to any activation.
  - Any response should be carried out by personnel capable of quickly assessing and managing the situation.
  - Responders should ensure their own safety and the safety of others
  - All persons providing a response should be trained in local activation and response. Protocol.
  - Where possible the preferred response will involve HSOs, an Internal Response Team (IRT), Emergency Response Team (ERT) or equivalent, or an escalation process to QPS
- A process should exist for reporting damages and faults, so that any issues with buttons are rectified as soon as reasonably practicable
- Consideration should be given to introducing personal duress devices for high-risk areas or when staff are working in isolation or areas with limited hard-wired duress devices
- All duress alarms should be tested / audited at a frequency informed by a security risk assessment process
- Personal duress devices promote the ability to raise the alarm whilst being carried on the person, this option is considered as both operationally functional and dynamic resource that promotes staff safety

## 7.5.2 Intruder alarms

HHSs should make informed decisions regarding the installation of, and response to, intruder alarm systems may be informed by a security risk assessment. Alarm systems should be:

- Easily operated by people with a minimum of training
- Clearly indicate status
- Protected against tampering with the system
- Highly resistant to false alarms
- Support alarm monitoring and a response is to be arranged for activations

Set out in **AS/NZS 2201.1-2007 Intruder alarm systems**, Part 1: Client's premises - Design, installation, commissioning, and maintenance, for additional information.

# Part C: Standard operating procedures for healthcare environments

## 1. Introduction

This guideline outlines suggested standard operating procedures (SOPs) that HHSs can implement to maintain a safe and secure healthcare environment. HHSs are encouraged to use this guideline to develop procedures to suit the specific needs and resource allocations of the HHS.

This guideline outlines requirements to be implemented in accordance with legislative obligations and accreditation recommendations in a manner consistent with Queensland Health objectives to ensure the safety and security of workers, patients, visitors, property, and assets.

This guideline aligns with the Queensland Health Safety Management System. This guideline utilises elements from relevant Australian standards to inform recommended physical security controls and draws from the Australian Government's Protective Services Policy Framework and Queensland Government's Protective Services Framework regarding security planning.

This guideline aligns with the **National Safety and Quality Health Service Standards, Comprehensive Care Standard** criteria for:

- 'Minimising patient harm' (through the development of staff and teams who share responsibilities to predict, prevent and manage aggression and violence)
- 'Minimising restrictive practices'

This document contributes to the **Department of Health Strategic Plan 2021–2025** objective to 'support and advance our workforce' through strategies that ensure the workplace is safe, rewarding, enhances wellbeing and adequately equips the workforce to perform at the highest level.

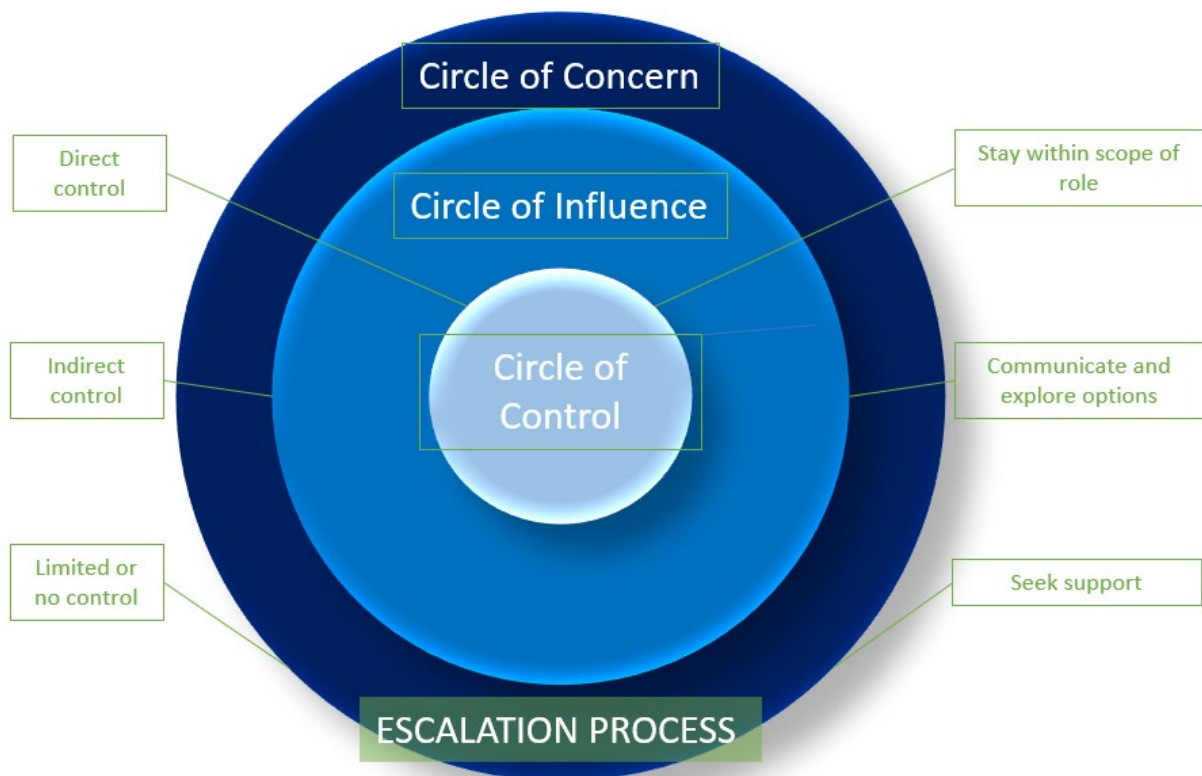
**Queensland Protective Security Framework (QPSF), Developing a Security Culture**, states:

*"An agency's security culture is the behaviour, actions and values that it wishes to adopt towards security. A positive security culture is critical to ensuring a successful protective security approach. Security policies and procedures alone will not deliver protective security outcomes. A strengthened security culture will only result from leadership, awareness, and expectations".*

HHSs should consider SOPs that contribute to a healthcare environment consistent with a '**person-centred care**' approach. This approach aims to support various services in providing safe, quality health care experiences that respects a person's individual preferences, needs, and values. HHS SOPs procedures should be designed to support the development of a '**positive security culture**'. Please see the dynamic risk assessment and escalation process (circle of control, influence, and concern,) adapted from Stephen Covey's '7 Habits of Highly Effective People'.



**Figure 11:** Dynamic risk assessment considerations



**Figure 12:** Escalation process (circle of control, influence, and concern)

## 2. Healthcare Security Models

HHSs should consider the various types of security models available to support the safety and security of healthcare environments. Security personnel may include HSOs and external security service providers.

Security services may be provided via:

- a) HSOs or facility workers performing security functions (in-house) (solely or in part), such as, Fire Safety and Security Officers, Safety and Response Officers, Protective Services Officers (PSOs), dual operational roles
- b) External security providers or private security firms employed under service agreements to a facility or HHS (contracted services), for example, providers that offer remote monitoring, patrols services, or cash in transit services
- c) Through a combination of a) and b).

**AS4485:2:2021 s5 Security Officers**, states: *“Each facility should determine the need for services of security officers. Security officers may need to perform a variety of functions within the healthcare facilities. The type of security service to be provided should be determined via security risk assessment. Security officers are an important service group within the facility structure and can assist patients, workers and others in routine and emergency situations”.*

The benefits of in-house security services ((a) above) include increased control over recruitment, training, operations, increased supervision, and better flexibility for changes to duties within changing clinical environments and legislation. Such changes to duties can become problematic when outside of the agreed service agreement of contracted services ((b) above), if contracted for. Hence the importance of strong tender processes, contract management and service agreements to minimise ambiguity.

Benefits of contracted services include industry experience and external management systems that require less internal responsibilities inherent with the inhouse model (managing an employment relationship). Consideration and consultation with stakeholders are required when deciding what type of services to utilise. This ensures services can deliver high care and professional expectations.

If a HHS is considering outsourcing security services, please refer to Department of the Premier and Cabinet [Queensland Government Contracting Out of Services Policy](#).

For any services that are contracted out, the comparable wage rates conditions apply. Further advice regarding outsourcing can be found in the **Queensland Public Health Sector Certified Agreement (No. 10) 2019, 6.5 Contracting Out 6.5.1, which states**, *“It is the clear policy of the employer not to contract out or to lease current services. The parties are committed to maximising permanent employment where possible. Please review the agreement closely before considering outsourcing”.*

**Section 3.1 Services currently provided in-house (i.e., by a government agency)**, of the above-mentioned policy states: *“It is the policy of the government that in order to maintain existing government jobs, there will be no contracting-out of services currently provided in-house other than in circumstances where:*

- *Actual shortages exist in appropriately skilled in-house staff*
- *There is a lack of available infrastructure capital or funds to meet the cost of providing new technology; or*
- *It can clearly be demonstrated that it is in the public interest that services should be contracted out.”*

## 2.1 The role of healthcare security

The role of healthcare security can be categorised into four main areas:



Prevention of Crime



Preservation of Peace



Protection of Information



Protection of Assets

**Figure 13:** HSO role in four parts

This guideline uses the generic term of **‘Healthcare Security Officer’ (HSO)** for any Queensland Health employed Security Officers, including, but not limited to:

- Fire Safety and Security Officer (FSSO)
- Safety and Response Officers
- Protective Services Officers (PSOs)

A generic role description (RD) has been established by the QSMN to be used as a reference to identify benchmarked responsibilities and to highlight the desired values and capabilities of the role. Please see the Onboarding and Upskilling, Security Managers toolkit and Generic Role Description.

The role of ‘security’ (HSOs and external security providers) within the healthcare environment is to be determined through the application of comprehensive risk management strategies and the specific needs of each HHS. This determines the expectations placed on the individuals fulfilling the role and guides the development procedural instructions based on HHS risk appetite and tolerance.

### 2.1.1 Authorisation and appointment under the *Hospital and Health Boards Act 2011* and *Tobacco and Other Smoking Products Act 1998*

Dependent on the HHS and its expectations of the security function, HSOs may be appointed as either authorised persons or security officers or both under the *Hospital and Health Boards Act 2011* (Qld) ('HHBA').

The HHBA, provides the following powers:

- To control traffic and give directions on health service land (s 174)
- Seize and remove a vehicle (s 177)
- Power to require name and address and other matters (s 185(2))
- Power to direct a person to leave the health service's land or part of the health service's land (s 183)

HSOs may be authorised to provide direction and respond to breaches of the Queensland Health Smoking Management Policy (Smoking Policy under the *Tobacco and Other Smoking Products Act 1998* (Qld) ('TOSPA') ([New no-smoking laws - Smoke-free Healthcare](#)) and [Smoking laws in Queensland, Queensland Health](#).

The TOSPA, provides the following authority:

- power to require name and address (s 38(2))
- power to direct person to stop smoking (s 40A(2))

## 3. Local standard operating procedures (SOPs)

HHSs should consider the following elements when developing new or reviewing established operational instructions such as duty statements, procedures, work instructions etc. The following guidance is not intended to replace, supersede, or substitute any existing local practices.

This guideline does not cover all the standard operating procedures and considerations required to establish effective security operations. HHSs are encouraged to explore the specific needs of their area and provide instruction where appropriate.

Procedures relating to security arrangements should be created and reviewed with a view to continuous improvement as outlined in AS45001. HHS and facility SOPs are to be implemented to identify local practices, and functions of the HSO role.

**AS 4485.1:2021 s2.2 Security framework**, states:

*“Each healthcare facility shall develop a security framework, including policy, procedures, and protocols, to effectively address security risks. Each facility shall establish governance strategies and systems that identify the responsibilities and accountabilities of all personnel concerned within the security framework”.*

Security risk assessments provide evidence to inform the development and continuous improvement of SOPs (or equivalent documents). SOPs are to be guided by the overarching security plan and aimed at reducing or eliminating threats, strengthening existing controls, and ensuring a safe environment. This

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

is achieved through layering of resources and control measures. Please refer to [Security planning and risk management](#).

### 3.1 Consultation, coordination, retention, and application

HHSs should consider a strategy for consultation with impacted local stakeholders, approval, publishing, and dissemination when developing and implementing SOPs.

Consultation with relevant security personnel is crucial as these positions are often considered subject matter experts with unique perspectives regarding operational requirements. Seeking input from frontline HSOs and leadership positions throughout the facility ensures instructions are relevant, efficient, and effective at all levels. Consideration must be given regarding the security model and how security services are provided.

To align with the local security plan and HHSs should review SOPs **every two years** (or sooner) in cases where changes to the risk environment are identified. Each HHS or facility may determine alternative processes for how and when SOPs should be reviewed.

The review should be led by the Security Manager / Security Administrator (or equivalent position or position assuming this function) and include input from local stakeholders. Stakeholders should form part of a consultation and dissemination list for the reviewing of existing SOPs and the introduction of new SOPs. This list should include HSOs as subject matter experts.

Approval should be gained from appropriate line management within the respective HHS organisational structure relevant to the security service. Subject to local HHS requirements, documents may need to be endorsed prior to publishing and published in accordance with local requirements.

Retention is to align with [Corporate records management policy framework](#). Any disposal of public records must align with the Queensland State Archives, General Retention and Disposal Schedule (GRDS) or have an authorisation under s 26 of the *Public Records Act 2002* for the disposal of common and administrative public records created by all Queensland Government agencies, states the following regarding disposal. Any disposal of public records without authorisation from the State Archivist may be a breach of the *Public Records Act 2002* (Qld).

The application of procedures considerations listed within this guideline must be lawful and special consideration towards 'all' related legislation is required. This document does not intend to outline each piece of legislation that may be related to each generic function or that may need to be considered when implementing procedure examples. This guideline may highlight common legislation for reference related to some functions.

HHSs and security services are required to be familiar with legislation which may impact performance of their duties.

## 3.2 Content for inclusion in SOPs

**AS 4485.1:2021 s2 Policies and procedures** states:

*“Where appropriate, security policies and procedures should be developed to address specific needs of the individual areas within the facility.”*

HHS SOPs should concisely and accurately describe the way workers are to perform certain security tasks. These SOPs ensure healthcare and security teams work in unison, expectations are clear, and tasks are completed cohesively with stakeholders, with a degree of consistency. Expectations can be set and expressed through consultation with relevant stakeholders such as leadership positions within Health and Safety Units (or equivalent), Emergency Departments, Mental Health Inpatient Units, and security services.

The contents of SOPs should address specific risks or required functions that reinforce a positive security culture, when establishing or reviewing written instructions for HSOs or facility workers performing security functions. Local SOPs may be summarised and consolidated in the HHS security plan and / or maintained as a list of separate procedures which work cohesively to inform operations and provide evidence of the security function.

HHS SOPs should be developed for HSOs activities, appropriate to the nature and level of the identified security risk. HHS SOPs should:

- Monitor compliance with instructions for pre-determined activities and reporting
- Prevent the potential misuse of equipment, and damage or loss of property
- Include protective security aspects of operational arrangements that promote protection from harm (or fear of harm), throughout the facility
- Prevent and respond to security incidents (including occupational violence and criminal activity) and to outline requirements and expectations

Operational instructions, such as shift specific duty statements or lists may consist of tasks that are to be performed, responsibilities associated with tasks, and any essential requirements for the performance of tasks such as who completes certain tasks, and where and when tasks are completed. This establishes clear understanding between line management and the HSO about their role and function. These documents can be beneficial for new starters in planning their shifts during orientation, induction phases of onboarding and may be provided to new starters as part of a welcome package or recruitment briefing.

Special consideration should be given to sensitive information that may jeopardise the integrity of the HHS or facility if published or disseminated. Procedures containing sensitive information may not be suitable for public disclosure. Below is a non-exhaustive list of examples that should be considered sensitive information:

- The frequency and type of patrols to be carried out and times of specific duties
- Detailed list of role, functions, and contact details
- Details of access control, and afterhours entry/exit procedures
- How to operate, respond to, and test security alarms, and other systems

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022



- Escalation processes to internal pathways and external services and other means for HSOs to gain support during and post incident

### 3.2.1 Equipment changes and handover or equivalent considerations

HHSs may consider establishing a written instruction or checklists for HSO handovers conducted at the start and finish of each shift. This may consist of expectations such as:

- Location and time of handover
- Who is expected to attend?
- How the handover is to be facilitated
- Who facilitates the handover?
- What information is relevant for oncoming group / shift

A structured and repeated handover inclusive of equipment checks ensures HSOs have the appropriate resources and information at the commencement of their shift. In addition, this process ensures:

- Equipment is functional, assigned appropriately, and collected by the appropriate HSOs, please see [security equipment](#), [Controlling risks through physical security](#).
- Security keys and vehicle keys and logbooks / sign out records (if appropriate) are retrieved by oncoming shift please see [key management](#), [Controlling risks through physical security](#)
- Correspondence is enabled through awareness of important emails and bulletin / data / notice, or white boards and any special or specific instructions relevant for the commencing shift
- Oncoming HSOs are briefed to understand any additional duties, issues or risks that may impact the shift and previous team is relieved

**AHFG:2018 s6.5.6 Services and equipment spaces, state:**

*“Regular security patrols for all areas to deter, detect and respond to incidents should be included as part of operational security procedures.”*

### 3.2.2 Patrols

Patrols serve as to deter, detect, delay, and respond to criminal activity through increased overt monitoring of an area facilitated by a uniformed security presence and are an effective control to improve the safety and security of an area.

Dependent on local security management, HHSs should consider procedures for conducting patrols that set performance indicators, expectations, and may include defining patrol zones that divide the facility campus into more easily monitored areas, improving response time and visibility. This can be represented on a map for HSO reference (this may be provided in recruitment briefings and displayed in security offices or controls as required).

Active patrols are an effective risk mitigation strategy to reduce HHS vulnerabilities. HSOs should aim to achieve as many patrols of their assigned areas as practical during their shift.

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

Patrol routes should be at the officer's discretion but should be random in nature and schedule, when conducted in addition to or outside of key stipulated times required to ensure patrol zones receive the desired attention. It may be necessary to stipulate key times for patrols and identify high risk areas to ensure these areas are sufficiently covered.

Random patrols conducted frequently decrease the likelihood of patrols being circumvented by persons who observe the security system / program with the intent to penetrate controls or commit offences. This may occur if an individual intentionally observes and learns patrol timeframes or periods of time between patrols.

HSOs should spend a significant portion of each shift patrolling, either on foot or in a security vehicle (dependent on HHS resources), internal and external to the facility buildings. The discipline of patrolling is the very essence of the security function and considered the base for all other duties aimed at preventing crime, preserving peace, and protecting information, and assets. The number of patrols required each shift, the patrol area, and the type of patrol (internal or external, on foot or vehicle) may be informed by a security risk assessment.

Patrols have the following purposes:

- To ensure vulnerable or critical points or key areas are frequently checked /monitored to maintain security and effectiveness against intrusion for any unauthorised purpose
- To check for intruders and identify potential trespassers or the unauthorised presence of persons
- To provide the opportunity to ascertain whether suspicious persons have reasonable cause / justification to be in the areas or buildings (and persons intentions)
- To provide a unique opportunity for HSOs to personally observe activity, and monitor individuals, and/or situations, which could pose a threat to the safety and security of patient's, visitors, staff (and others) and assets (property, infrastructure etc.)
- To increase a HHSs capacity to deter criminal activity (such as theft) through an active uniformed presence and to detect potential breaches to facilities and restricted areas within facilities
- To check barriers, access control (doors and windows) and the functionality of various physical security controls (such as lighting), typically includes non-technical visual inspection and informal physical assessment of a designated patrol zone
- To report any damages and hazards through local arrangements
- To check for potential fire hazards and to assess firefighting equipment (such as status of fire indicator panels and mimic panels)

Patrols completed by HSOs on foot offer a unique opportunity for direct, personal interaction with members of the public / community, staff, and patients. Vehicle patrols allow officers to efficiently cover large external areas safely.

Effective and active patrols are enabled by HSOs with the correct knowledge, skills, and attitude.

### 3.2.3 Securing buildings

Securing buildings includes actions typically carried out by HSOs to ensure a building or property is secure. Activities may include:

Security guidelines

- Conducting lock up checks (to ensure areas are locked down typically after hours)
- Lock up duties carried out outside of normal business hours or at close of business times.
- Unlock duties carried out prior to an area commencing business
- Arming security, intruder, or building alarms outside of normal business hours or at close of business times
- Disarming of security, intruder, or building alarms prior to an area commencing business

Lock up checks or lock and unlock duties are a crucial component of any patrol function. This includes the physical checking of doors, windows and access systems and ensuring these access points and potentially vulnerable areas are monitored to promote the security of the facility to effectively restrict access as intended.

SOPs for this practice should include locking doors where required at specific times, testing the locking mechanisms at designated access points ensuring points are free of obstruction and, where relevant, checking automated doors lock down at specific times and rectifying access control issues as they arise.

Special attention should be given to restricted or authorised personnel only areas, critical, valuable, or attractive assets, sensitive areas, and vulnerable access points.

Documenting and reporting issues or inefficiencies of various areas is encouraged. Taking appropriate action to mitigate and remedy issues (within the capacity of the role) and escalating issues to the appropriate parties responsible for the maintenance of these systems (such as Building Engineering and Maintenance Services or appropriate department) is also encouraged.

Patrols of this kind may include the requirement to arm or disarm (activate / deactivate) building security alarms, typically for areas that are not staffed or in use after hours. Local instructions specific to the installed equipment should guide how this is achieved, associated times, and who to contact if issues are experienced (facility stakeholders and alarm monitoring companies or internal equivalent control room arrangements).

PINs / alarm codes must not be shared outside of the security service. Please see [entry / exit control \(access control\)](#) of [Controlling risks through physical security](#).

### 3.2.4 Responding to security alarms

**AS/NZ4421:2011 s4.9 Alarm response**, provides the below direction, which may be used as a guide to developing local procedures: *“Alarm investigation conducted at a site should follow set procedures covering:*

- Actions on arrival at site*
- Requirements for external and internal inspections of premises on the site*
- Actions to be taken*
- Communications and other procedures with operations room and*
- Submission of reports*

HHS SOPs should enable an effective and appropriate response to activated alarms. HSOs responding

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

to alarms should conduct an informal dynamic risk assessment and seek advice or confirmation through communicating with their supervisor (or equivalent on duty or oncall management) or control room operator prior to entering an area and conducting an investigation (open communication is key to the maintenance of safety).

HSOs may respond with the support from colleagues (in attendance), dependent on local resourcing and expectations, particularly if trespass is likely.

Appropriate safe practices and response to activated intruder alarms and duress alarms may be built into local response procedures referencing escalation pathways to gain additional support internally (with IRT, ERT, or equivalent response team) or through QPS through facility specific code black processes (dependent on local arrangements). Other related instructions may include the management of incidents of trespass or intruders, promoting safe response and dynamic risk assessment.

In some HHSs, an activated duress alarm will automatically declare a Code Black response and be used as the method to engage an appropriate pre-determined and resourced response.

**AS 4485:2021 4.3.1 Duress alarms** states: *“The nature of the response to a duress alarm activation should be determined locally. Whoever responds should be quickly on the scene and capable of assessing the situation they may be confronted with (e.g. an assault) in a competent and safe manner”.*

SOPs should outline that those responsible for responding to security alarm activations should ensure their own safety first, followed by the safety of others present. Security response to activations should be facilitated in a manner so as not to escalate the threatening persons and align actions with training in local activation and response protocols.

For information regarding physical control elements of security alarms please see sections: [Duress alarm systems \(personal and fixed\)](#) and [Intruder alarms](#) of [Controlling risks through physical security](#).

### 3.2.5 Security escorts and staff welfare checks

HHSs should consider establishing security functions (i.e. staff escorts and welfare checks) as stand-alone procedures or embed within existing procedures (e.g. patrols).

#### *Examples of staff security escorts*

- *Between the hours of 2240Hrs and 2320Hrs, HSOs conduct additional external patrols of car park areas and escort staff to and from their cars as required*
- *Throughout the night, staff working afterhours are encouraged to call security to escort them between buildings*

#### *Example of staff welfare check*

*HSOs working the night shift were informed during handover that the Mental Health Unit had experienced issues throughout the day, HSOs conducted random check-ins on staff throughout their shift to make sure nursing staff were supported afterhours*

At times where an increased risk is identified such as in high-risk areas, areas exposed to recent security issues, areas prone to crime, or in out of hours / afterhours environments, additional security

Security guidelines

measures to ensure staff safety may be considered by the HHS. SOPs may accommodate additional measures where required and appropriate to mitigate specific risks as determined necessary by the HHS. Escorting staff after hours supports the safety of staff travelling to and from their work areas, particularly external areas, and carparks. Periodic welfare checks or patrols on wards and staff will assist in promoting a culture of safety. Checking on the welfare of staff may mitigate risks for isolated and secluded work areas, particularly afterhours).

These activities may be supported by physical security controls such as duress and intruder alarms, which may work to reduce risk exposure to unstaffed, or vulnerable areas.

Proactive procedures promote an understanding of the risks that threaten staff safety and the actions taken by local security services to control risks. Welfare checks and staff escorts conducted while on patrol can be implemented to:

- Contribute to a comfortable work environment for staff
- Promote a positive security culture
- Strengthen professional relationships

**AS 4485.2:2021 s4.3.4 Car park security and control** states: *“Parking areas should be regularly patrolled by security and security escort should be offered between the workplace and parking areas.”*

**AS 4485.2:2021 s6.6.8 Movement of workers and other at night** states: *“The period of greatest risk is at night when there are fewer people on the premises and there are more opportunities for threatening or criminal activity under the cover of darkness.”*

Peak times and scheduled activities are to be determined by each HHS based on specific needs of its facilities and risk exposure (for example, staff changeover times). Requests may come from wards, departments, facilities, or staff.

A security risk assessment should determine the specific needs of work areas, whilst consultation with HSOs will ensure activities are practical.

### 3.2.6 Transporting currency

Storage, handling, and transport of currency can be associated with risks of increased potential for violence and loss. These potential risks need to be considered by HHSs when developing SOPs to addressing the personal security and safety of people responsible for a healthcare facility’s cash activities.

A security risk assessment inclusive of contributing risk factors associated with the transport of currency will inform practices to ensure risks are mitigated to a reasonable level. Each HHS is responsible for addressing security risks associated with the transport of currency, factors may include:

- Predictability of route and routine
- Availability of HSOs to conduct security staff escort (and suitable contingencies)
- Visibility for staff and access to help or support

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

- Physical security controls to ensure staff safety and enable an emergent response
- Means to escalate and activate an emergency response (code black / QPS) or extract from a situation if there are safety concerns regarding exposure to actual or perceived threats

HHSs should consider the following elements in relation to transporting currency:

- Persons carrying consignments of significant value should be aware of the risks involved and be provided with an appropriate means of carriage / transport and security escort if required to reduce vulnerability to potential threats
- Persons frequently transporting currency between areas should vary the time and route taken so not to be predictable (where practical)
- In circumstances where a significant threat exists, consideration should be given to engaging professional cash transit couriers / security providers in consultation with local services (please refer to security models)

Depending on local arrangements, typical activity may include the following examples:

- HSOs may be engaged to assist in transporting cash to and from areas in the facility (within jurisdiction) dependant on local practices
- HSOs may escort other HHS staff to and from areas with consignments of money
- External service providers may service ATMs and businesses positioned on site (on health service land), however businesses on site may organise their own secure transport activities
- For areas off site (not on health service land – not in jurisdiction of HSOs) the facility may arrange external service providers to ensure the safe transport of currency

### 3.2.7 Newborn and paediatric abductions

HHSs should develop and maintain SOPs regarding the abduction of newborn and paediatric patients. This action may be built into existing emergency plans, SOPs or exist as a stand-alone instruction.

Paediatric security considerations may include at-risk children due to social or environmental factors. In some medical, legal, or social circumstances, infants or paediatric patients may be separated and placed in special care units or wards. Some admissions may be the subject of court orders and subject to access restrictions.

The attempted or actual abduction of an infant or child may occur for several reasons. These include family and custody disputes that may result in attempts to remove the child from the facility, without a lawful reason to do so.

All child abduction protocols should be in writing and known to HHS personnel who are required to provide a response. If these protocols are activated, healthcare personnel, including HSOs, must be instructed to be on alert for any unusual behaviour displayed by individuals. Procedures must apply to both to nurseries and to the paediatric settings.

These patients should be considered as persons with protective status and procedures may be enabled to prevent potential newborn and paediatric abduction. Child protection, maternity, and paediatric units may work closely with local security services to ensure procedures exist to increase the presence of security within the affected area and determine appropriate responses to potential situations. Preventative or precautionary measures such as engaging and positioning HSOs in an area

to provide a presence where there are risks of abduction or in situations where threats have been made, should be considered.

Media play a key role in publicising search efforts in the event of a newborn abduction. The HHS may develop a media plan, which should be activated if an infant / child goes missing. An [Amber-alert](#) may be considered by the QPS to broadcast urgent and relevant information through the media.

SOPs for responding to a possible abduction may include the following processes:

- Immediately notify the facility security, management stakeholders, and QPS
- Secure the facility, posting an appropriate person at appropriate exits and direct visitors to exit through a controlled point (if appropriate)
- Consider locking down areas of the facility to increase effectiveness of access control
- All available HSOs and staff may be requested to join a coordinated search the entire interior and exterior of the facility starting with the unit, whilst other officers review CCTV footage
- Obtain a clear description of the event and factors leading up to the event from appropriate persons involved and enquire into the child's possible location
- Where appropriate, allow all parent(s) / guardian(s) of the allegedly abducted child to move to a quiet area and appropriate staff members may be assigned to be with them during this time
- Secure the scene to preserve any evidence that may be collected or required by QPS (such as CCTV footage) and at shift change
- All unit staff must remain in the area until excused by QPS
- On advice HHS leadership or QPS:
  - Escalate the incident to the Director of Nursing to brief all unit staff and notify surrounding healthcare facilities or wards of the incident; provide a full description of the infant / child and possible abductor
  - All employees should be instructed that all enquiries, including media, are to be referred to the HHS designated spokesperson, as assigned by the HHS
  - Facility switchboard operators must be prepared for a potential influx of calls and should be provided with contact details for whom and where enquiries and information are to be directed. This may include the establishment of a designated hotline

### 3.2.8 Responding to wandering or missing patients

**AS 4485.2:2021 Missing patients**, states: *“Healthcare facilities should establish protocols and procedures for dealing with missing patients.”*

To ensure the safety of vulnerable or at-risk patients, HHSs should consider SOPs for reporting, locating, and returning wandering or missing patients. SOPs must consider appropriate legislation in relation to patient care in relation to the patient's status (voluntary / involuntary).

The *Guardianship and Administration Act 2000* (Qld) ('GAA') seeks to strike an appropriate balance between, the right of an adult with impaired capacity to the autonomy in decision-making, and the

adult's right to adequate and appropriate support for decision-making. When responding to or managing events related to wandering or missing patients, the GAA and other acts related to involuntary treatment should be considered.

Wandering or missing patients should be reported to the facilities security services (or equivalent responsible designated services) as soon as it is ascertained that the patient is missing.

The report should contain a full description and characteristics of the patient and factors that may assist security services in locating and effectively communicating with the wandering or missing patient. This may include:

- Name, age, or date of birth (D.O.B), and description of patient
- Patient status (voluntary / involuntary and information specific to the relevant legislation), examples:
  - [Guardianship and Administration Act 2000](#)
  - [Mental Health Act 2016](#)
  - [Public Health Act 2005](#)
- Relevant medical information, injuries, special communication needs, and specific safety concerns
- The likelihood of potential aggressive behaviour and any other relevant information that may assist in finding the patient, verbally de-escalating the patient and reasoning with the patient about their return to the ward / department

If HSO's (or equivalent responsible designated services) haven't received the appropriate information to enable an effective search, clarification should be sought from the ward / department requesting assistance. HSOs should search within the parameters of the healthcare facility (hospital and health service land) only. If there is concern that the person has moved outside of HSO jurisdiction, QPS should be engaged for support.

All staff should be aware of their ability to escalate to QPS if there are legitimate concerns that the person has absconded from the facility (while under an Act which statutorily compels them to remain at the healthcare facility to receive treatment) or concerns exist for their health, safety, and wellbeing (regardless of whether the patient is receiving treatment involuntarily under an Act or not).

If HSOs locate the wandering or missing patient, HSOs are to inform the related ward / department at the earliest convenience. HSOs are encouraged to communicate and engage with the patient if safe to do so or wait for support to escort patient back to the relevant ward / department.

If assistance is required from ward staff / clinical staff to persuade the patient back the related ward / department or in cases where the patient refuses to return, HSOs should be aware of local support available to them.



In cases where the patient is threatening the safety of others or themselves, a Code Black may be initiated to ensure the safety and wellbeing of the patient. Whilst awaiting an appropriate response, staff may consider withdrawing to a safe distance and maintaining observations of the patient.

*Examples of responding to a wandering / missing patient:*

- *Medical ward nursing staff call HSOs and explain an elderly patient known for wandering was missing from the ward (receiving treatment under the GAA). HSOs search the external areas of the facility and locate the elderly patient. HSOs contact the medical ward and a nurse responds. Staff successfully communicates with the patient and the patient agrees to return to the ward.*
- *HSOs are assisting nursing staff locate a missing patient. Together, staff locate the patient. As staff approach in a non-threatening manner, the patient begins to use offensive language and is showing high risk indicators for potential aggression. Staff maintain a safe distance from the patient and activate a Code Black to enable a coordinated response. The patient walks near a roadway and is standing on the footpath (out of the facility jurisdiction). Staff withdraw and monitor from a distance so not to intimidate the patient and to reduce the likelihood of the patient walking into traffic. Staff contact QPS for urgent assistance.*

### 3.2.9 Involuntary patients with high risk of absconding

Involuntary patients who are not permitted to leave a facility due to being placed under an Act (such as the [Guardianship and Administration Act 2000](#) (GAA:2000), [Mental Health Act 2016](#) (MHA:2016) or [Public Health Act 2005](#) (PHA:2005)) may display strong emotional reactions and physical outbursts or potential aggressive behaviour. These patients may be distracted by distressing thoughts, experience difficulty communicating and interpreting information and understanding why they are not permitted to leave. Individual risk factors may be mitigated through acknowledging the patient's frustration and situation, expressing empathy, and practicing active listening and verbal de-escalation.

HHSs should consider developing SOPs to manage patients who attempt to abscond, succeed at absconding from health facilities, or leave the facility without permission from medical staff, whilst receiving treatment under the Act as an involuntary patient. SOPs may improve the efficiency of activities and knowledge of staff with the expectation to manage involuntary patients or respond to events of absconding patients.

SOPs may promote HSOs and other staff conducting a dynamic risk assessment to ensure safe engagement with the patient as they attempt to abscond and ensures appropriate intervention actions are considered, including support from clinicians or emergency services to return a patient if attempts to abscond are successful. This promotes a systematic response to minimise risk to patient and staff safety with clear expectations.

Precautionary procedures to increase the presence of security may be enacted to prevent the patient from absconding as this provides increased monitoring of the patient, communication with the patient (if safe to do so) and reassurance to the patient through the use interpersonal skills, where risk appropriate.

If HSOs and other staff in the area cannot safely persuade a patient to remain within the facility or safely prevent the patient from absconding, focusing on nonthreatening verbal communication, an activation of Code Black procedures or escalation to the QPS should be considered.

Facilities without an available security presence may consider engaging QPS proactively if increased supervision is required to support clinical staff.

HHS SOPs should consider:

- Encouraging communication between QPS, clinical staff (ED) and security services
- Processes to engage the security service where appropriate for assistance at the request of the of the department and inform security services of the situation
- Establishing appropriate supports in consultation with HSOs
- Following advice from previous section: [Responding to wandering and missing patients](#), if a patient attempts to abscond
- Where a patient is involuntarily receiving treatment under a specific act, HSOs may be accompanied by clinical staff or at a minimum, acting on clinical direction to promote a safe, person-centred, and coordinated response
- Consider activating a Code Black if the patient is threatening or escalate to QPS where the patient successfully absconds

#### *Examples of involuntary patient with high risk of absconding*

*ED nursing staff inform security services of the presence of an involuntary patient with a high potential to abscond and request a presence within ED to assist with observation of the patient receiving treatment under the PHA (Emergency Examination Authority (EEA)). HSOs maintain a safe static position in the area.*

- a) Involuntary patient attempts to abscond: HSOs intervene and persuade the patient to remain in the area*
- b) Involuntary patient threatens staff and becomes increasingly aggressive; staff activate Code Black*
- c) An involuntary patient absconds from ED; QPS are contacted by treating clinicians to return the patient who has not yet been medically cleared for discharge*

### 3.2.10 Managing an Emergency Examination Authority (EEA)

HHSs should develop local SOPs to manage EEA presentations at facilities if required.

QPS and Queensland Ambulance Service (QAS) may detain and transport a person to a public sector health service facility in emergency circumstances under the emergency examination authority (EEA) provisions of the PHA. This may apply where the QPS or QAS officers reasonably believe that:

- The person's behaviour indicates the person is at immediate risk of serious harm, **and**
- The risk appears to be the result of major disturbance in the person's mental capacity caused by illness, disability, injury, intoxication, or other reason, **and**
- The person appears to require urgent examination

Most patients under EEA are adequately managed in the ED environment, however there are patient presentations that require increased preventative measures and monitoring due to a high likelihood of attempts to abscond. Please see [Chapter 4A Health of persons with major disturbance in mental capacity of the PHA regarding:](#)

- The health of persons with major disturbance in mental capacity, including detention in treatment or care place and examination
- [Returning persons who abscond from a Public Sector Health Service Facility while under an Emergency Examination Authority.](#)
- Please refer to the PHA for all appropriate information regarding EEA management and the following information:
  - [Emergency examination authorities | Queensland Health](#)
  - [Emergency examination authorities - Frequently asked questions \(PDF 306 kB\)](#)
  - [Powers and responsibilities under Chapter 4A of the Public Health Act 2005 \(PDF 210 kB\)](#)
  - [EEAs: Information for Hospitals and Health Services \(PDF 288 kB\)](#)
  - [Information regarding searches of a person under an EEA \(PDF 238 kB\)](#)

### 3.2.11 Increasing security presence

HHSs should consider SOPs to strengthen or increase the presence of HSOs or other delegated personnel stationed at or within a specific area to minimise potential risks to patients and/or staff. SOPs should guide HSOs providing additional support for areas identified with increased needs. This practice is often referred to as a security observation, security presence, static patrol, stand by, or security special.

Local practices should be risk appropriate. A security risk assessment including staff capacity and availability may inform how additional supports could be provided by the security service. Security risk assessments will be informed by situational information and assessed by security management. Security management may be engaged to provide operational advice.

Consideration may be given to the provision of ad hoc services (to requesting departments requiring additional presence, if appropriate) or the use of on-duty HSOs (both cases to be determined by the HHS).

The intention of the static positioning of one or more HSOs is to:

- Provide a higher degree of observation
- Identify early warning signs / triggers
- Escalate / activate local response procedures (if required), such as Code Black

To avoid unwarranted pressure being placed on the security services, it is preferred if HSOs are engaged in a consultative and collaborative manner, in cases where:

- Other practical options have been exhausted; or deemed ineffective to manage the threat
- This activity is a standard expectation, shift requirement or standing order
- The request can be safely facilitated

For areas without specific shifts for this function or similar, such as dedicated ED shifts or officers, consideration should be given to appropriate resource allocation. In situations where no threat can be identified, the threat is resolved, the risk has been significantly mitigated, or there is no benefit to maintaining the increased presence, consideration may be given to standing down or deactivating the security special / presence.

This action may be substituted with alternative activities, such as increased patrols and periodic welfare checks on the area to allow HSOs to return to usual duties. These options may be appropriate to reduce pressure placed on security services when experiencing competing priorities. A dynamic risk assessment is encouraged prior to any actions. The presence of security should only be removed from the area if attending to other priority duties.

HSOs providing the presence should be encouraged to always consider their own safety and position themselves at a point of safety to enable monitoring from a practical distance. This enables safe access to support staff and the patient where appropriate and ongoing assessment of risk.

Maintaining an appropriate distance allows the HSOs to:

- Observe the whole scenario and identify potential and real risks as they emerge, (known as a dynamic risk assessment)
- Decrease the likelihood of an attack by maintaining a presence without intimidating or antagonising the patient
- Respect the personal space of the patient, whilst affording HSOs time to react

*Example scenario: HSOs are providing a security special / presence within ED for a known aggressive person on an EEA (under PHA). As staff approach to communicate with the patient, HSOs correct their positioning and move closer to enable an effective safe response (if required). As staff move away, so do the HSOs. It is expected that HSOs work collaboratively, and under the direction of the clinician delivering care.*

When facilitating a security presence, the HSOs focus should be on effective verbal de-escalation and an understanding of how to engage local incident response resources such as Code Black activation, which is available to support HSOs at all times. The HSO must also be aware of escalation processes to engage support from the QPS through 000.

HSOs may share workloads to support each other, and the wellbeing of colleagues assigned to specific duties related to security presence / special. HHSs are encouraged to develop contingent arrangements to be utilised in cases where a request for an increased presence cannot be fulfilled to the extent requested.

### 3.2.12 Patient search and escort (*Mental Health Act 2016 (Qld)*)

HHS SOPs should consider increased security presence during patient searches and escorts (facilitated by clinical staff) depending on the level of risk present.

HHS SOPs should consider when it may be appropriate for Authorised Persons (defined in MHA) to facilitate searches on patients and their possessions whilst receiving treatment under the MHA:2016. Depending on the level of risk present, support from HSOs may be required to maintain a presence whilst the search is being conducted. HHS SOPs should also consider the utilisation of HSOs to accompany Authorised Persons in transporting patients under the MHA:2016 within Authorised Mental Health Services for [Examinations and assessments](#).

HHS SOPs for patient searches may consider the following processes:

- Authorised Person under the MHA develops a plan to carry out search
- Authorised Person under the MHA:2016 engages security services for a collaborative response
- If the patient becomes aggressive or threatening on during search, procedures should enable escalation to engage either a Code Black response of QPS (as appropriate)

HHS SOPs for patient escorting may consider the following processes:

- Authorised Person under the MHA:2016 develops a plan to transport the patient
- Authorised Person under the MHA:2016 engages security services for a collaborative response
- If the patient becomes aggressive or threatening on route procedures should enable escalation to engage either a code black response of QPS (as appropriate)
- Please refer to the MHA:2016 and the following information:
  - [Mental Health Act 2016 | Queensland Health](#)
  - [Clinical Guidelines and Procedures website](#).
  - [Transport of patients: MHA training videos | Queensland Health](#)
  - [Transport, movement, and patient absence](#)

Please see: [Key topics: Mental Health Act 2016 | Queensland Health](#)

### 3.2.13 Weapons and dangerous items (illicit substances)

**The Drugs Misuse Act 1986 (Qld)**, states: “...it is a crime for a person to unlawfully have possession of and/or supply a dangerous drug, or a relevant substance or thing. This includes illicit drugs and drug paraphernalia”.

HHS SOPs should be developed for the control of weapons and other dangerous items such as illicit substances that may be brought to healthcare facilities. Procedures may focus on safe response,

retention, storage, and disposal of potential weapons and dangerous items (illicit substances), in accordance with AS1940:2017 The storage and handling of flammable and combustible liquids.

A safe (secure receptacle / drop safe) is an effective control if strict access control over the resource is maintained. Please see section [Security containers, cabinets, safes, and vaults](#) in the: [Controlling risks through physical security](#) for further information.

HHSs should consider SOPs to support facilities with temporary storage options and protocol that is aligned with the *Weapons Act 1990* (Qld) and *Drugs Misuse Act 1986* (Qld) to enable a process for QPS to receive illicit substances and weapons from facilities, where appropriate, such as in times of an open investigation into an incident involving a crime, where such items may serve as evidence.

SOPs may include:

- Instructions for processing found items or items handed over to security services by a patient, staff, visitor, or other means
- Response and intervention expectations for when an illicit drug or weapon is identified or when a patient/consumer or visitor is suspected to be in the possession of an illicit drug or weapon
- Management and disposal of illicit drug/weapon based on local arrangement, resources, and efficient processes for escalation to relevant authorities (QPS) (for response to incidents or collection of items)

In the course of their duties HSOs may come into possession of property including illicit substances and weapons, which creates a risk within the health service (in terms of accountability and possession), and an obligation to store and maintain said property in the condition it was received, and account for every item in possession for handing over to QPS.

Where a person is suspected of carrying a weapon or using or possessing illicit drugs, appropriate action may be taken to ensure the security and safety of all persons. This may include an approach that emphasises awareness, prevention, and discreet incident management (where practical and safe to do so), and the following considerations:

- Isolate and contain the impacted area, and calmly withdraw staff, visitors, and patients to a safe space (where practical and safe to do so), while awaiting a response or advice from QPS
- The person should be observed from a safe distance until appropriate assistance arrives
- If the person becomes threatening to the safety and wellbeing of themselves, tactically withdraw and engage Code Black procedures and request urgent assistance from QPS via 000
- The priority should be placed on maintaining safety for all persons in the area and extraction or evacuation of the area may be considered, with escalation to management, and response stakeholders
- Non-threatening communication and verbal de-escalation strategies must be deployed from a safe distance to mitigate aggressive behaviour if it arises
- If communication and attempts at verbal de-escalation are failing, it may be appropriate to cease communication so as not to further escalate the person. If this occurs, it is important that observation of the patient is maintained and the situation is escalated to QPS

- Dependent on local arrangements, QPS may collect and dispose of the illicit substance or weapon and investigate the matter, interview the person, and/or take action that is deemed appropriate at the time
- If QPS do not collect items, appropriate means of disposal is to be organised by the HHS, with consideration to be given to the possession of illicit substances or weapons, and appropriate documentation, including signatures from relevant involved parties.

### 3.2.14 Lost and found property

**AS4485.2:2021 Lost property**, states: *“Patients, visitors and workers should be encouraged to report all losses, both personal and facility, as soon as the loss is noticed, as delays in investigation reduce the opportunity of a positive outcome”.*

HHS SOPs should consider the management of lost and found property to ensure risks related to property loss and damage are minimised. In addition to making positive contributions to theft prevention, a proactive lost and found procedure should promote returning property to the rightful owner in a timely manner. The following is only relevant to security services undertaking this responsibility within their own HHS, this function may or may not fall within the remit of ‘security’.

HHS SOPs to effectively manage and control lost property should include tasks such as:

- Collection or receiving of items (including receipt of documentation i.e., time, date, and name person responsible for handing over the items)
- Recording and itemising of lost property items
- Investigating and attempting to contact the owner
- Process for fielding enquiries
- Storing (retention period)
- Disposal of unclaimed items (waste or charity donations)
- Periodic auditing of inventory and documentation

### 3.2.15 Unauthorised photography and filming (on HHS land / facilities)

HHS SOPs should consider the inclusion of legislative obligations in relation to filming and photographic images of individuals, buildings, structures on HHS land, and facilities, and should outline that any images must be authorised and controlled. This is to ensure the site’s integrity and security is not compromised, to ensure privacy legislation and confidentiality policies are upheld. This includes the use of personal mobile devices to film and take photos on HHS land.

All requests by external bodies for filming/photographic images must be referred to the relevant HHS Communications, Engagement and or Corporate Affairs Department (or equivalent) for approval.

If a staff member observes an individual or group taking photographs or filming, they should report to security services (or to the delegated response area) pursuant to local processes. If security (or equivalent) observes or are informed of an individual or group taking photographs or filming

individuals, buildings / structures on HHS land / facilities, security should attend, investigate, and seek to confirm whether authority has been granted.

Should local security services ascertain that the photography or filming is not authorised, officers are to take the following action as appropriate:

- Direct the individual/s to cease and desist from taking further photographs/filming
- Explain the rationale behind this direction in conjunction with this procedure

Where appropriate, explain that, should there be non-compliance with this direction, the individuals concerned will be considered to be committing the offence of “conduct causing a public nuisance” under s. 182 of the [Hospital and Health Boards Act 2011](#). If necessary, QPS should be contacted.

Patients and family members are to be encouraged and given the opportunity to ask questions and clarify information. Staff are responsible for providing information in a way that is understandable and that meets their needs and are to check consumer’s understanding of discussions.

### 3.2.16 Approaching media personnel (on HHS land / facilities)

Each HHS should develop procedures and related SOPs for approaching media personnel. HHS Communications, Engagement and or Corporate Affairs Department (or equivalent work unit), may advise and assist the local security service with directions to facilitate communications between parties in special circumstances.

HHS SOPs should outline specifications regarding media representatives often required to seek approval from the authorised management authority (HHS specific requirements may exist) to film on site. Any unauthorised attendance by members of the media at a health facility must be reported to the authorised media officer or executive representative of the HHS. This may be dependent on local arrangements please check with your communications / marketing team or equivalent.

Any staff member that receives an inquiry for access to a health facility from the media must refer them to the authorised media officer or HHS executive representative. The authorised media officer or HHS executive representative may escort / accompany media representatives.

Expectations for security services may involve speaking to onsite media personnel, escorting and/or providing a presence to support communications / marketing teams in responding to onsite presentations, attaining credentials, passing on relevant information, and upon advice from HHS Communications, Engagement and or Corporate Affairs Department (or equivalent work unit), HSOs may request / direct unauthorised media to leave the facility. Media personnel may film or photograph the hospital campus buildings and other facilities from a position offsite (outside of HSO jurisdiction).

All communications must be polite and professional and represent the health service positively. HSOs should avoid engaging in debates or arguments with media personnel. If personnel refuse to stop filming, or disobey directives, HSOs should remove themselves from the situation and escalate concerns through local processes.



*Example of filming on HHS land:*

- *Staff complain of suspicious persons (possibly a media crew) filming onsite and enquire whether the group has received permission to do so:*
  - *HSOs liaise with the group to identify them and enquire if they had received permission to film.*
  - *HSOs then contact the appropriate HHS Communications, Engagement and or Corporate Affairs Department (or equivalent work unit) for advice.*
- *If not permitted: HSOs inform the group (on advice) and request, they cease filming.*
- *If the group refuses to cease filming: HSOs may remove themselves from the situation and escalate to QPS.*
- *If permitted: HSOs liaise with the enquiring staff and confirm the group has received permission to film.*

### 3.2.17 High-profile visits

HHS SOPs should ensure that all high-profile visits are dealt with appropriately and managed with discreet and effective security arrangements, established through consultation with positions responsible for Facility Management, Public Affairs, Marketing, Communications, Engagement and or Corporate Affairs Department (or equivalent work units), and management of security services.

Additional or increased security measures may be necessary to mitigate potential risks related to the high-profile visitor or may occur due to the political nature of the high-profile visit.

HSOs should be encouraged to maintain open lines of communication during such visits, identify any risks or expectations, decrease the likelihood of negative impacts (where foreseeable). Clear internal communication ensures collaboration across departments.

Useful information includes:

- The name of the high-profile visitor
- The intent of the visit
- The facility / area of facility being visited
- Areas of arrival / departure
- Times, date, and duration
- Expectations or requests to be facilitated by the local security teams

A security risk assessment may identify the need for additional or increased security arrangements such as an increased security presence / static patrols, ad hoc staffing resources, and so on.

It is common for requests to be made for the blocking off or reserving of carparks and cordoning off areas in preparation for visits.

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

For further information please see the [Elected members of Parliament, Senators and candidates for political office seeking to visit a Hospital and Health Service, Queensland Ambulance Service facility or Statutory agency QH-GDL-960:2015](#), which sets out the requirements to ensure safe, effective, and respectful access to Queensland's public health facilities by both State and Federal elected MPs and Senators, when they visit HHS, QAS and statutory agency facilities in their official capacity, and to outline the appropriate protocols for any candidates for political office, seeking to visit these facilities.

### 3.2.18 Helicopter landing activities

Each HHS or facility with a Helicopter Landing Site (HLS) should have the below mentioned manual, and procedures (or equivalent) concerning safe patient transfer from aircraft to facility. Dependent on local arrangements security services may be engaged to facilitate:

- Safe patient transfers and secure landings (with appropriate supports dependent on local arrangements)
- Maintain strict access control to the area (particularly during times on landings)
- Facilitate safety inspection functions such as auditing via checklists, reporting hazards and repairs where required, and monitoring general maintenance and cleaning:
  - Checklists (or equivalent) may include HLS Safety Officer Pre-Landing & Departure Safety Checklists and HLS General Safety and Security Inspection Checklists (or equivalent) as determined necessary by each HHS

The [Helicopter landing sites Queensland Health Guideline QH-GDL-447:2021](#) outlines mandatory requirements and recommendations regarding best practice for the planning, implementation, and management of HLS owned and/or operated by HHSs throughout their life cycle.

Each area is required to have a HLS Operations Manual. As per QH-GDL-447:2021:

*“The HLS Operations Manual should be available at each HLS. The structure and content for a HLS Operations Manual is at the discretion of each HHS and it is recognised there are likely to be additional site-specific matters that need to be addressed. The HLS Operations Manual will typically contain the following details:*

- Authorised HLS users
- HLS usage limitations
- HLS descriptive information including approved plans and photographs
- Helicopter operating requirements
- Normal management procedures; and

HHSs may establish associated procedures regarding HSO expectations in relation to HLS functions and the expectations of other carrying out functions related to the HLS. These procedures are often referred to as helicopter transfer procedures / patient transfer procedures (or similar), and consist of processes to ensure that aero-medical operations are managed as outlined in [Helicopter landing sites QH-GDL-447:2021. Enabling](#) facilitation of safe and effective patient transfer from the helicopter to the Emergency Department and Intensive Care Unit (or other predetermined area as identified by the accepting treating team).

Security guidelines

Procedures may outline specific tasks regarding the methods of helicopter transfers (such as):

- Single patient transfer (1 patient)
- Dual patient transfer (2 patients)
- Hot load (engines are running and rotor is turning). This is an exceedingly rare event that would occur only under extreme circumstances, such as in a mass casualty event in which there are multiple helicopters bringing patients to the hospital
- Collection of or off-load of resources or personnel
- Pre-landing notification (communications from Aeromedical Coordinator or equivalent to appropriate facility stakeholders and internal activations)
- Access control restrictions to HLS and resources
- Fire and safety precautions, emergency response, and general transfer protocol

Dependent on local arrangements, HLS roles and responsibilities that may be assigned to healthcare security services and HSOs, may include (but may not be limited to):

- HHS HLS Contact Officer
- Local HLS Operator
- HLS Controller (shift position)
- HLS Safety Officer / Helicopter Landing Site Safety Officer.

Please refer to local naming conventions, practices, and instructions for further information regarding responsibilities and training.

### 3.2.19 Emergency responses

Emergency response SOPs may be established to support local emergency plans and supplementary plans. Consideration should be given to the following phases when developing or reviewing written instructions:

- **Alert:** emergency possible – increase level of preparedness
- **Standby:** emergency imminent – prepare for implementation of response
- **Response:** emergency situation exists – implement response according to facility plans and in collaboration with facilities as necessary
- **Stand Down:** emergency abated – return to usual business.

[AS 4083:2010, Planning for emergencies – health care facilities, s2.2 Specific emergency](#), defines the below emergency events and colour codes:

- a) Fire / smoke: **code red**
- b) Evacuation: **code orange**
- c) Bomb threat: **code purple**
- d) Infrastructure and other internal emergencies: **code yellow**
- e) External emergency: **code brown**

Security guidelines

- f) Personal threat (armed or unarmed persons threatening injury to others or themselves, or illegal occupancy): **code black**
- g) Medical emergency: **code blue**

To promote cohesive governance and aligned response practices, local SOPs (including security incident procedures) should align with local emergency procedures for the above-mentioned emergency colour codes. Deviation or addition to emergency colour codes is strongly discouraged. Please refer to [Appendix 18](#) Emergency response procedures (colour codes) for further information.

### 3.2.20 Security incidents

**AS 4485.2:2021 s 8 Incident procedures**, states: *“All security incidents, suspected incidents and near misses should be reported and investigated. A security incident is deemed to have occurred when there is –*

- a) *actual or attempted harm to a person within a healthcare facility or its grounds,*
- b) *a threat or perceived threat to harm, or suspicious activity toward a person or facility, or incite a fear of risk within a healthcare facility or its grounds,*
- c) *loss of, or damage to attractive assets or dangerous items owned or in the possession of the facility, or belonging to any person to whom it owes a duty of care or*
- d) *loss, compromise, or misuse of sensitive or vital information.”*

HHS SOPs for security incidents may:

- Exist to enable a response to the security incident that is safe, effective, appropriate, and lawful. They should consist of an informal dynamic risk assessment (conducted in real time) prior to any actions taking place
- Identify internal escalation processes to activate and acquire additional support (as necessary) or externally to QPS for situations that are out of the control of responding HSOs, IRTs, ERTs (or equivalent response teams) and situations that have exhausted internal capabilities to safely manage the situation. It is unreasonable to expect internal processes to control dangerous situations without identifying potential pathways to escalate incidents to QPS (if and when required)
- Enable investigative actions that may determine what occurred, why it occurred, how it occurred and when it occurred. From this point, the impact to business or compromise of security integrity and damage can be understood and recommendations may follow to eliminate or manage the associate risk, minimising the likelihood of re-occurrence.

**AS 4485.2:2021 s 8.2 Preservation of crime scene evidence**, states: *“It’s important to maintain the security and integrity of a crime scene and to prevent evidence from being contaminated, destroyed, lost or altered”.*

### 3.2.21 First response and preservation of crime scene

HHS SOPs should consider identifying the priority of first responders to be the safety of all persons including self, protecting life, removing persons from danger, and emergency medical assistance

Security guidelines

(providing first aid and getting the injured person professional medical attention), if an injured person is at the scene, they must receive medical attention if safe to do so. This may include consideration to Code Blue / MET (Medical Emergency Team) call procedures and engaging external emergency services (QAS, QPS, QFES).

HSOs may be called up on to assist with the preservation of the scene of a crime (if the scene is within their jurisdiction) until investigating QPS arrive and take lead of the situation. The area should be monitored upon arrival to determine whether there is a requirement to preserve or maintain an area associated with an incident for the purpose of further investigation.

Every effort should be taken to preserve the integrity of the crime scene and evidence. Access to the scene must be heavily restricted to ensure nothing is moved or touched to minimise the loss of valuable evidence.

It may be appropriate to take steps to secure the area from curious onlookers and others. Take precise notations of time and events as they occur, including all persons who have entered and exited the scene for example members of staff providing assistance and those involved in the incident.

Extreme caution must be used when entering the scene. Movement should be calm and deliberate and HSOs should be aware that possible evidence (fingerprints etc) might be found on doors, door locks and knobs, light fittings, floors, and walls. Ensure gloves and appropriate PPE is worn.

If property or people are moved in the interests of life preservation or establishment of death, notes should be taken of what was moved from where and where it was moved to.

Where it is confirmed that a person is deceased, the scene should not be disturbed, however the use of privacy / trauma screens would be considered appropriate.

Any items at the scene that pose an immediate risk to safety should be removed and placed in a suitable secure location, such as Illicit Substances and Weapons safe, or a secure receptacle. Items should be handled only by one person and secured appropriately. Please see section on [weapons and illicit substances](#).

HSOs and facility management positions may be required to liaise with QPS investigating officer and provide initial support to secure the scene. The investigating officers may stand down first responders at their discretion. Police have power to access and declare crime scenes and conduct activities of investigation in crime scenes, under the *Police Powers and Responsibilities Act 2000* (Qld).

In addition to the above and dependant on local arrangements there may be occasions where HSOs are required to preserve Workplace Health and Safety (WHS) incident scenes until such time as WHS teams / Worksafe QLD Inspectors arrive on scene. If this is a requirement SOPs should reflect this task.

### 3.2.22 Post incident management

**AS 4485:2021 s8.3.2 Investigation**, states: *“Investigations into security incidents provide a valuable insight into whether existing security arrangements are effective. Investigations are also useful in the risk management process.”*

HHS SOPs should consider establishing post incident management processes to support HSOs and other staff after being involved in security incidents or after being exposed to occupational violence. This may be facilitated by leadership position inside the security service, ERT / IRT (or equivalent) or from the affected work area.

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

Post incident investigations may include the following considerations:

- Immediate or preliminary investigations should be carried out by appropriate persons, such as Security Manager / Security Administrator (or equivalent position or position assuming this function), following established internal processes
- Threats, assaults, and criminal activity should be reported to appropriate leadership positions within the organisation and via RiskMan. Depending on the nature of the incident, QPS involvement may be required (if there is indication of a criminal offence police must be informed immediately).
- Interviews with involved parties or eyewitnesses are required to ascertain the appropriate information and review of incident reports, available footage may be made available through local processes and dependent on local arrangements

Post incident considerations, may include but may not be limited to:

- Procedure for reporting the incident and initiating investigation and support
- Instructions for debriefing and investigation of the incident to identify when it occurred, who was involved, and what could be done to prevent recurrence
- Procedures for providing support to any person(s) involved in or affected by the incident
- Exploring points of view to determine the effectiveness of operations, clarity of objectives, strategies, communication, and equipment, which may see a reinforced value of training, procedures and equipment use

The Occupational Violence (OV) Incident Response Kit has been designed specifically to support managers to navigate the process following the occurrence of an OV incident and provide immediate and long-term support to employees.

QOVSU have also developed an OV Toolkit for Employees. This has been designed to support employees following an OV incident. Both the OV Incident Response Kit and OV Toolkit for Employees are tailored to the HHS. For further information please see the [Factsheet: Incident Response Kit](#) and [Incident response kits](#).

The severity and outcome of an incident will determine the measures required for appropriate post-incident management. Appropriate measures could include:

- Providing medical treatment
- Providing relief staff (to allow individuals exposed to the incident time to recover and regain composure)
- Incident debriefing / operational debriefing
- Employee support options.

Establishing a post incident debriefing procedure may outline expectations for meetings held at the end of an incident or event. This presents the opportunity for all participants involved in an incident to review plans and operations including, pre-determined arrangements, the response to the incident, and its effectiveness or performance.

Post incident debriefs provide the opportunity to share feedback, identify gaps in performance or processes and utilise the meeting as a mechanism to acquire and promote learnings and staff development.

Post incident debriefs may be conducted as hot debrief or after-action review (AAR), facilitated as soon as practicable, as a hot debrief within 72Hrs post event, and cold debrief / post event analysis (PEA), within 6 weeks post event. Consideration should be given to facilitating a multidisciplinary review of the incident, with local practices as determined by the HHS.

Factors for facilitating debriefs include, but may not be limited to:

- Using non-emotional language and maintaining professionalism
- Ensure as far as practical that the environment is comfortable for staff to meet
- Promote accountability and only constructive feedback
- Document the name of the person(s) facilitating the debrief, date, time, those in attendance and relevant outcomes and actions

The healthcare facility may identify people who are suitably qualified or experienced or in the best position to:

- Coordinate the post-incident response
- Conduct debriefings and
- Provide counselling (or advice on means to arrange counselling and associated resources)

In alignment with the QH Health, Safety and wellbeing consultation standard, the post OV incident feedback and review process should promote consultation with workers, support workers, and Health and Safety Representatives to participate in managing OV risks.

The [Queensland Health Operational Briefing and Debriefing Guide](#) prepares outlines how, debriefing tasks are to be completed and roles of each task in the response of the event or activity. This guideline recommends briefings should follow the SMEACS-Q format, as outlined below:

- Situation - the current and predicted situation of the event
- Mission - event or activity objective of the group
- Execution - how the mission will be accomplished; what agencies are involved?
- Administration and Logistics - recording requirements, logistical arrangements
- Command and Communications - Emergency Operation Centres activation status; business continuity plans activated, etc.
- Safety - hazards (known and potential)
- Questions - from and to the audience (to confirm understanding)

**AS 4485:2021 s8.4.5 Post-trauma**, states:

*“Involvement in, or exposure to, workplace incidents such as traumatic events or critical incidents can lead a person to experience distress” ... “Supervisors should monitor for level of distress through engagement and observation, as it can lead to a decline in performance and in overall levels of wellbeing. Supervisors should provide access to support and assistance where impact of trauma are identified (e.g. Employee Assistance Program).”*

### **Counselling, psychological support and OV incident response kits**

Counselling and psychological support is accessible via the Employee Assistance Service (EAS) who provide a confidential and anonymous service for staff to access ongoing support. This may assist staff when navigating their physical, emotional, and behavioural responses to critical incidents in the workplace. This service is of no cost to staff or departments and should always be offered and readily available to those who request it.

#### **Employee Assistance Service (EAS)**

For HSOs experiencing work-related issue affecting performance or wellbeing, face-to-face or telephone counselling and/or online resources are available free of charge. Local EAS providers can be found through the following link: [employee-assistance-service-providers](#).

### **3.2.23 Documentation and reporting**

**AS 4485.2:2021 s8.3.1 Reporting**, states: *“Security departments should compile and maintain reports, occurrence logs, shift reports and any other documentation relevant to the performance of the section’s duties”.*

HHS SOPs should consider requesting HSOs carry a notebook throughout their shift. This notebook is to document duties as completed and information that has been collected throughout their shift. The writing styles are at the discretion of the HSO completing the entries, however, entries must be factual and reflect a sequence of activities in a time / date specific manner in a chronological order. The notebook is the first line of documentation used, prior to formally documenting information in the Shift Log / Incident Report. Reports should consider the following: who, what, when, where, how, and why, an incident happened, or activity was completed.

HSOs are to record the date and shift times (preferably in 24hr time) and any incidents attended to during the shift. Writing is to be legible, in pen and on numbered pages. HSOs may be ordered to produce their notebook in court (if necessary); therefore, entries are to be correct and professional.

Valuable information is captured through reports and occurrence / shift logs (or equivalent) maintained by HSOs every shift. Information entered and recorded may represent a more formal version of the notes initially documented in notebooks. Information is collected to record activities and sharing intelligence and data, contributing to the continuous improvement and capability of the security service.

Reports and occurrence / shift logs of this nature are to maintain records of all incidents, significant events, security related information and activities carried out with indications of what work was done,



when, and by whom. Entries are to be time specific, factual, complete, clear, and concise, with events noted in a chronological order.

Incident reports may follow HSO attendance at security incidents emergency codes, including Code Red and Orange, Code Purple, Code Black, or upon responding to any other event involving aggression, occupational violence, or security related incident. HSOs are responsible to completing and submitting incident reports in a timely manner, ensuring information is accurate, factual, clear, and concise. Dependent on local arrangements incident reports (of the above nature) may be maintained within the reports and occurrence / shift logs previously mentioned as occurrences or entered in RiskMan.

RiskMan is the state-wide integrated safety information system. It will guide and prompt information where appropriate. As standard code black reporting protocol, incident reports are to be completed by the work unit or person who activated or initiated the Code Black, however HSOs can complete a RiskMan incident report at their discretion. HSOs may complete a [RiskMan](#) incident report for incidents involving personal injury, near miss, to report an identified risk or hazard, and add to existing incident reports.

HSOs should contact their local Health and Safety Unit / WHS representative if they require assistance navigating the system or completing a RiskMan incident report.

# References

## Legislation

- [Building Fire Safety Regulation 2008 \(Qld\)](#)
- [Criminal Code Act 1899 \(Qld\)](#)
- [Guardianship and Administration Act 2000 \(Qld\)](#)
- [Hospital and Health Boards Act 2011 \(Qld\)](#)
- [Human Rights Act 2019 \(Qld\)](#)
- [Information Privacy Act 2009 \(Qld\)](#)
- [Mental Health Act 2016 \(Qld\)](#)
- [Public Health Act 2005 \(Qld\)](#)
- [Police Powers and Responsibilities Act 2000 \(Qld\)](#)
- [Privacy Act 1988 \(Qld\)](#)
- [Tobacco and Other Smoking Products Act 1998 \(Qld\)](#)
- [Work Health and Safety Act 2011 \(Qld\)](#)
- [Work Health and Safety Regulation 2011 \(Qld\)](#)

## Standards

- AS 4083:2010, Planning for emergencies – health care facilities
- AS 4485. 1 & 2:2021, Security for Healthcare Facilities
- AS/NZS 4421:2011, Guard and patrol security services
- [Australian Commission on Safety and Quality in Health Care](#)
- HB 167: 2006 Security risk management
- HB 327:2010 Communicating and consulting about risk
- HB 188:2021 base building physical security handbook – terrorism and extreme violence
- [Health, safety and wellbeing risk management standard QH-IMP-401-3:2020](#)
- ISO 31000: 2018 Risk management
- ISO 45001:2018 Occupational health and safety management systems

## Supporting documents

- [Australasian Health Facility Guidelines 2018](#)
- [Crime Prevention Through Environmental Design Guidelines for Queensland 2021](#)
- [Elected members of Parliament, Senators and candidates for political office seeking to visit a Hospital and Health Service, Queensland Ambulance Service facility or Statutory agency QH-GDL-960:2015](#)
- [Health Safety and Wellbeing Risk Management Standard QH-GDL-401-3-1:2021](#)
- [Helicopter landing sites Queensland Health Guideline QH-GDL-447:2021](#)
- [How to manage work health and safety risks Code of Practice 2021](#)
- [Information Security QH-POL-468:2019](#)
- [Protective Security Policy Framework 2018](#)
- [Queensland Public Health Sector Certified Agreement \(No. 10\) 2019](#)
- [Queensland Health Capital Infrastructure Requirements Volume1](#)
- [Queensland Health Wayfinding Design Guideline 2010](#)

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

# Appendices

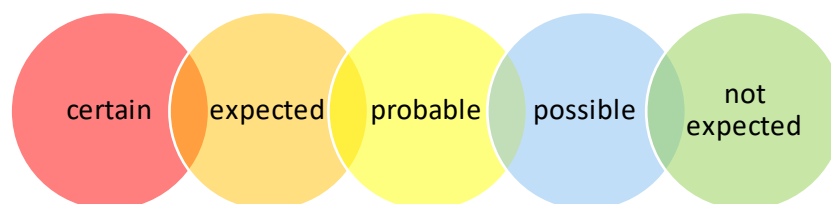
## Appendix 1

### Security risk environment and national threat levels.

Summarised from HB188, methods for threat identification may consider the below:

- Identification of existing building vulnerabilities includes factors that:
  - Increase the attractiveness of a building as a target
  - Enable offenders conduct hostile reconnaissance to identify and exploit weakness
  - Reduce the effectiveness of security measures or risk treatments
- Information gathered from previous incidents and targeted attacks (actual and attempted)
- Identification of known motivations and malicious capabilities, potential threats can be identified through a consideration of the current threat environment, this information can be sourced through):
  - Online crime map (QPS) [Maps and statistics | QPS \(police.qld.gov.au\)](https://www.police.qld.gov.au/maps-and-statistics)
  - The QPS annual report [Reports and publications | QPS \(police.qld.gov.au\)](https://www.police.qld.gov.au/reports-and-publications) and [Queensland Counter-Terrorism Strategy](#)
  - Australia's current National Terrorism Threat Level [Current National Terrorism Threat Level](#) and [www.nationalsecurity.gov.au](http://www.nationalsecurity.gov.au)
  - Queensland's approach to countering terrorism is outlined in the Queensland Counter-Terrorism Strategy on [Safeguarding Queensland](#) website.
  - [Queensland Police](#)
  - [Emergency Services and Safety](#)

The National Terrorism Threat Level is a five-level scale (see figure below), this scale informs the public of the likelihood of an act of terrorism occurring in Australia. If Government makes a change to the level, it will explain why there is a change.



## Appendix 2

### Assessing sensitive and security classified information, (PSPF)

			Sensitive information	Security classified information		
	UNOFFICIAL OFFICIAL	OFFICIAL	OFFICIAL: Sensitive	PROTECTED – NOT FOR GENERAL DISTRIBUTION	SECRET	TOP SECRET
	No business impact	Low business impact	Low to medium business impact	High business impact	Extreme business impact	Catastrophic business impact
Compromise of information confidentiality would be expected to cause:	No damage	No or insignificant damage	Limited damage to an individual, organisations, or government	Damage to the national interest, organisations, or individuals	Serious damage to the national interest, organisations, or individuals	Exceptionally grave damage to the national interest, organisations, or individuals

For further information please see [Business impact levels for consequence of threat](#), PSPF (example).

## Appendix 3

**Consequence assessment,** (Health, safety, and wellbeing risk management guideline QH-GDL-401-3-1:2021)

Type of consequence	Negligible	Minor	Moderate	Major	Extreme
People, property, and environment	No structural or equipment damage No environmental damage No injury/illness or first aid treatment only. No time lost (SAC 4)	Minor structural or equipment damage Limited escape to onsite environment Medical treatment required for injury. A full shift has not been lost (SAC 3)	Moderate structural or equipment damage Some offsite environmental damage Lost time or injury or illness without permanent impairment (SAC 2)	Major structural or equipment damage Some offsite environmental damage Serious injury or illness with permanent impairment (SAC 2)	Catastrophic structural or equipment damage Significant offsite environment impact A loss of life (SAC 1)

Appendix 4 **Likelihood (probability) assessment**, (Health, safety, and wellbeing risk management guideline QH-GDL-401-3-1:2021)

Likelihood

Almost certain	Expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Might occur occasionally
Unlikely	Could occur sometime but not expected
Rare	May occur only in exceptional circumstances

## Appendix 5 Security control rating, (HB 167) (example)

Control rating	Symbol used	Description
Excellent	✓ x3	<ul style="list-style-type: none"> <li>all key security risks are efficiently and effectively managed</li> <li>controls are optimal to meet the level of security risk</li> </ul>
Good	✓ x2	<ul style="list-style-type: none"> <li>majority of key security risks are effectively managed</li> <li>small improvements in controls are possible</li> </ul>
Adequate	✓	<ul style="list-style-type: none"> <li>key security risks are managed effectively</li> <li>control improvements are recommended</li> </ul>
Long term requirement	-	<ul style="list-style-type: none"> <li>security risks are managed currently, but sustainable effectiveness is questionable in the long term</li> <li>significant control improvements are needed in the long term</li> </ul>
Immediate requirement	X	<ul style="list-style-type: none"> <li>controls fail repeatedly, or imminent failure is likely</li> <li>significant improvement is required</li> </ul>
Non-existent	XX	<ul style="list-style-type: none"> <li>no effective management of security risks is occurring</li> <li>Introduction of controls required immediately</li> </ul>
	?	<ul style="list-style-type: none"> <li>indicates that further validation is required before rating can be provided</li> </ul>

## Appendix 6

### Security in depth factors R2D3, (HB 188) (summarised)

Principle	Definition (R2D3 model)
Deter	Deterrence controls provide a psychological barrier to discourage offenders from considering the building in question as an attack target, or from initiating an attack
Detect	Detection controls should enable the timely detection of unauthorized access, suspicious activity or other behaviour associated with threat sources
Delay	Delay controls should be designed to obstruct the progress of offenders during any attempted incursion into a building site or attack scenario
Respond	Response controls should also be put in place to prevent or counter the incursion, damage, or other impact associated with the attack scenario
Recover	Recover controls should be applied to reduce business interruption and restore operations in a timely manner after an actual or attempted attack

Components of a security control environment, based off HB 167 (example of how controls can be measured)

	Deter	Detect	Delay	Respond	Recover
Patrols	Yes	Yes	Yes	Yes	Partial
Signage	Yes	No	No	No	No
Barriers	Yes	No	Yes	No	No
Lighting	Yes	Yes	No	No	No
Security risk assessments and planning	Partial	Partial	Partial	Partial	Partial
Lock and unlock / lock up check	No	No	Yes	No	No
Security access systems	Yes	Partial	Yes	No	No
Security alarms (intruder and duress)	Yes	Yes	No	Yes	Yes
Surveillance	Yes	Yes	No	Partial	Partial



## Appendix 7

**Threat matrix (capability vs intent), (HB167 & HB188) (example)**

		Intent		
		Little	Expressed	Determined
Capability	Extensive	Medium	High	Extreme
	Moderate	Low	Significant	High
	Low	Low	Medium	Significant

## Appendix 8

### Vulnerability matrix, (HB 167 & HB 188) (example)

Vulnerability rating	Assessment criteria
Very high / extreme	<ul style="list-style-type: none"> <li>controls are non-existent, critical, and urgent improvements have been identified</li> <li>it is almost certain controls will be breached or fail</li> <li>there is recent evidence of widespread control failures</li> <li>there are no mitigations, redundancies or contingencies in place, severe disruptions to business are likely</li> </ul>
High	<ul style="list-style-type: none"> <li>controls are largely ineffective, significant areas for improvement are identified</li> <li>there is an increasingly likely probability of the controls being breached</li> <li>there is recent evidence of significant numbers of controls being breached</li> <li>few contingencies are in place and significant disruptions to the business are expected</li> </ul>
Moderate	<ul style="list-style-type: none"> <li>most controls are functioning, but a number of areas for improvements are identified</li> <li>there is moderate possibility of controls being breached and limited evidence that controls will fail</li> <li>there is recent evidence of a small number of controls being breached</li> <li>contingencies are in place for only a few key areas of the business to manage potential disruptions</li> </ul>
Low	<ul style="list-style-type: none"> <li>controls are effective, but small improvements could be made</li> <li>there is a low probability of the controls being breached in the future</li> <li>there are no recent examples of controls being breached</li> <li>adequacy of the controls is assessed on a regular (minimum annual) basis</li> <li>contingencies are in place for key areas of the business to manage potential disruptions to the business</li> </ul>
Very low	<ul style="list-style-type: none"> <li>controls are optimum and are sustainable</li> <li>there is an extremely low probability of the controls being breached or that control measures will fail</li> <li>adequacy of the controls is assessed on a regular and frequent basis</li> <li>rigorous and effective mitigations, redundancies and comprehensive contingencies are in place to manage potential disruptions to the business</li> </ul>

## Appendix 9

### Criticality matrix, HB 167 (example)

Criticality rating	Impact (example only)
Extreme	<p>Loss of asset results in:</p> <ul style="list-style-type: none"> <li>• complete cessation of all functions</li> <li>• no short-term recovery capability</li> <li>• prolonged loss of services (extending several months)</li> </ul>
High	<p>Loss of asset results in:</p> <ul style="list-style-type: none"> <li>• complete cessation of one or more functions</li> <li>• no short-term recovery capability</li> <li>• prolonged loss of services (extending several weeks)</li> </ul>
Significant	<p>Loss of asset results in:</p> <ul style="list-style-type: none"> <li>• cessation of one or more functions</li> <li>• limited short-term recovery capability</li> <li>• loss of services (extending days to weeks)</li> </ul>
Moderate	<p>Loss of asset results in:</p> <ul style="list-style-type: none"> <li>• reduced effectiveness of one or more functions</li> <li>• possible short-term recovery capability</li> <li>• partial or temporary loss of services (days)</li> </ul>
Low	<p>Loss of asset results in:</p> <ul style="list-style-type: none"> <li>• little impact on functions</li> <li>• possible immediate recovery</li> <li>• no loss of services</li> </ul>

## Appendix 10

**Example Security Risk Assessment templates**, (based off HB 167) examples only – please copy and paste in an appropriate document and add additional lines and photos / images where needed

### General site information

General site information	Facility name:
Date of assessment	
Person conducting risk assessment	Name: Phone no. Email:
Facility (consider adding a map)	Facility name: Organisation: Address:
Description of facility	<i>Services provided by the facility and facility location, size, positioning, boundaries, surroundings, major geographic features, land use and impacts</i>

Criticality and vulnerability template (example)

<u>Asset / Service / Facility</u>	<u>Location &amp; HHS</u>	<u>Risk scenario</u>	<u>Criticality (description &amp; impact)</u>	<u>Criticality rating</u>	<u>Vulnerability (description / assessment criteria)</u>	<u>Vulnerability rating</u>
<p><i>Reiterate or summarise key services provided by the facility and add current / existing services</i></p>	<p><i>Facility location, size, positioning, boundaries, (summary)</i></p>	<p><i>Identify risks, consider summarising factors relevant below:</i></p> <ul style="list-style-type: none"> <li><i>tangible and intangible sources of risk or cause of risk and indicators of emerging hazards</i></li> <li><i>threats and opportunities</i></li> <li><i>vulnerabilities and capabilities</i></li> <li><i>consequences and impacts</i></li> <li><i>previous criminal activity or events</i></li> </ul>	<p><i>If elements of the risk scenario (left) where not controlled effectively, what would be the impact on facility and services (previously identified)?</i></p>	<ul style="list-style-type: none"> <li>- <b>Extreme</b></li> <li>- <b>High</b></li> <li>- <b>Significant</b></li> <li>- <b>Moderate</b></li> <li>- <b>Low</b></li> </ul> <p><i>Provide details impact details (in brief)</i></p>	<ul style="list-style-type: none"> <li>- attractiveness of assets</li> <li>- effectiveness of existing controls</li> <li>- ability to treat to and recover from a security incident</li> <li>- culture and application of security arrangements</li> </ul> <p><i>Provide brief explanation / description of factors that increase the vulnerability of the facility and services.</i></p>	<ul style="list-style-type: none"> <li>- <b>Very high / extreme,</b></li> <li>- <b>High,</b></li> <li>- <b>Moderate,</b></li> <li>- <b>Low,</b></li> <li>- <b>Very low</b></li> </ul> <p><i>Provide details of assessment criteria (in brief)</i></p>

Threat source identification and assessment template (example)

Threat (description)	Threat source	Threat type (scenario)	Intent	Threat capability	Threat rating (capability vs intent)
<p><i>Provide brief explanation / description and evidence where available.</i></p> <p><i>Consider the below examples, if not relevant; remove.</i></p>	<ul style="list-style-type: none"> <li>- <b>non-deliberate criminal risk</b></li> </ul> <p><i>Add details if required</i></p>	<ul style="list-style-type: none"> <li>- <b>malicious threat</b></li> <li>- <b>opportunistic threat</b></li> <li>- <b>threats of terrorism</b></li> <li>- <b>incidental threat</b></li> </ul> <p>- <i>Add details if required</i></p>	<p>Expressed or implicit objective</p> <ul style="list-style-type: none"> <li>- <b>little</b></li> <li>- <b>expressed</b></li> <li>- <b>determined</b></li> </ul> <p><i>Intent refers to the aims, desires, motivational factors, or objectives associated with the threat, add details if required.</i></p>	<p>Attributes of a prospective threat that make it credible</p> <ul style="list-style-type: none"> <li>- <b>extensive</b></li> <li>- <b>moderate</b></li> <li>- <b>low</b></li> </ul> <p><i>Add details if required</i></p>	<p>Threat = capability x intent</p> <ul style="list-style-type: none"> <li>- <b>low</b></li> <li>- <b>medium</b></li> <li>- <b>significant</b></li> <li>- <b>high</b></li> <li>- <b>extreme</b></li> </ul> <p><i>Add details if required</i></p>
<b>Theft</b> (personal and health service property)					
<b>Trespass</b> (unauthorised access)					
<b>Vandalism</b> (property damage)					
<b>Assault</b> (patient, visitor, public, staff)					

<u>Threat (description)</u>	Threat source	Threat type (scenario)	Intent	Threat capability	Threat rating (capability vs intent)
<b>Human error</b> (accidental and nondeliberate actions)					
<b>Natural hazards / disasters</b>					
<b>Equipment failure</b>					
<u>Examples: Special security considerations / not mandatory (for example of lower likelihood and higher consequence) factors</u>	Only add if relevant				





Security control assessment template (example)

Physical control measure (examples below)		Yes	No	Control rating	Control description / details	Vulnerabilities	Proposed security improvements & treatment
<b>Item (as per below)</b>	Description in brief (as per below)			✓ <b>x3 Excellent</b> ✓ <b>x2 Good</b> ✓ <b>Adequate</b> - <b>Long term requirement</b> <b>X Immediate requirement</b> <b>XX Non-existent</b> ?	Add further details to describe current control capabilities	What are the current vulnerabilities?	<b>Consider treatments:</b> <ul style="list-style-type: none"> <li>• hierarchy of control measures</li> <li>• risk treatment processes</li> </ul> risk treatment options
<b>Present state of security</b>	- security plans - standard operating procedures (SOPs) - previous security risk assessments - and related business contingency plans (BCPs)						
<b>Security personnel</b>	Security model (internal or external, security provider)						
	Security management						
	No. of security personnel and description of responsibilities - security patrols (and related services)						

Physical control measure (examples below)

**CPTED (Crime prevention through environmental design)**

- territoriality / ownership
- natural surveillance and lighting
- natural access control
- image and management / maintenance

**Workplace design and physical security controls**

Security personnel equipment

- torches
- ligature cutting tools
- notebooks
- load bearing safety vest and duty belts
- phones, mobile phones, pagers, and radios
- PPE: eye protection, face, shields, hi-vis vests, wet weather gear, and gloves (disposable and needle stick resistant)

Landscaping

- deter unauthorised access
- doesn't impede on existing controls

Lighting

- motion detection / security lighting
- location of lighting
- number of lights

Yes	No	Control rating	Control description / details	Vulnerabilities	Proposed security improvements & treatment

	Yes	No	Control rating	Control description / details	Vulnerabilities	Proposed security improvements & treatment
Physical control measure (examples below)						
<ul style="list-style-type: none"> <li>- adequacy of lighting quantity and placement</li> <li>- compliance to standard</li> </ul>						
Barriers (fences, walls, gates, boom gates, permanent bollards, guard, handrails etc.)						
Signage (visibility, informative and appropriately placed)						
<b>Surveillance monitoring controls</b>						
Video surveillance systems (VSS) / Closed circuit television (CCTV) <ul style="list-style-type: none"> <li>- coverage at high risk, main entrance, and foyer areas</li> <li>- location</li> <li>- number of cameras</li> <li>- adequacy of cameras quantity and placement</li> <li>- storage of footage</li> <li>- compliance to standard</li> </ul>						
Body Worn Cameras (BWC) <ul style="list-style-type: none"> <li>- number of cameras</li> <li>- ethical use and storage of footage</li> </ul>						
Proximity swipe cards and access						

Physical control measure (examples below)

**Entry / exit control (access control)**

- Keypads
- Staff identification
- Visitor control
- Locks and combination locks
- Doors and windows
- Intercom system
- Key management
  - types of keys
  - number of keys
  - location of keys
  - register and issuing of keys
- Other means of entering facility
- Security containers, cabinets, safes, and vaults
- Duress alarm systems

Yes	No	Control rating	Control description / details	Vulnerabilities	Proposed security improvements & treatment

Physical control measure (examples below)

**Security alarm systems**

- personal devices
- fixed systems
- number of devices
- location of devices
- response to activations

Intruder alarms

- coverage at high risk, main entrance, and foyer areas
- Response to activations

Yes	No	Control rating	Control description / details	Vulnerabilities	Proposed security improvements & treatment

### Security risk treatment plan template (example)

No.	Risk description and rating (examples below)	Risk treatment strategy and option	Complete by (date)	Responsibility and commitments
1.	Refer to ' <b>Risk matrix</b> ' ( <b>consequence vs likelihood</b> ) and provide explanation (utilising information to describe the criticality rating, vulnerability rating, threat rating, and control rating sections.	Previously outlined in ' <b>Security control assessment template (example)</b> ', column: ' <b>proposed security improvements &amp; treatment</b> '	<b>Propose actions and link dates, this may align with other factors committee meetings, business cases etc.</b>	<b>Who is endorsing, sponsoring, or supporting proposals and what role will they play moving forward?</b>
2.				
3.				

### Strategic security risk management activities plan (example)

Objectives	Outcomes	Stakeholders	Strategy / Actions	Resource allocation	Timetable	Reporting / Monitoring	Performance indicators
E.g., Ensure commitment to principles of good security risk management practices and promote positive security culture	Link risk No. 1 (or other) as per ' <b>Security risk treatment plan template (example)</b> ': consider condensing the ' <b>risk description and rating</b> ' with the ' <b>risk treatment strategy and option</b> '	Consider listing persons identified in ' <b>responsibility and commitments</b> ', and other relevant persons	Implementation process (in brief) to plan actions emerging from the ' <b>risk treatment strategy and option</b> '	Current and available, and proposed	May be linked to specific actions within the ' <b>Strategy / Actions</b> ' column	Progress and milestones	Measuring implementation


# Appendix 11

## Business impact levels for consequence of threat, (PSPF) (example)

Business impact level	1. Low impact	2. Low to medium impact	3. High impact	4. Extreme impact	5. Catastrophic impact
Consequence of threat	Insignificant damage to the national interest, organisations, or individuals	Limited damage to the national interest, organisations, or individuals	Damage to the national interest, organisations, or individuals	Serious damage to the national interest, organisations, or individuals	Exceptionally grave damage to the national interest, organisations, or individuals

## Appendix 12

**Risk appetite and risk tolerance levels, (based off PSPF) (example)**



<b>Extent of risk appetite</b>	<b>Risk tolerance level</b>	<b>Risk management approach</b>	<b>Management action</b>
<b>No Appetite</b>	<b>Zero tolerance</b>	<b>Highly cautious</b>	<b>Crisis Management</b>
<b>Low appetite</b>	<b>Low tolerance</b>	<b>Cautious</b>	<b>Executive approval</b>
<b>Moderate appetite</b>	<b>Moderate tolerance</b>	<b>Conservative</b>	
<b>High appetite</b>	<b>High tolerance</b>	<b>Confident</b>	<b>Business case</b>



## Appendix 13 **Special security considerations / not mandatory (for example of lower likelihood and higher consequence factors)**

Based off AS4485 Security in specific locations and HB188 Threat types, weapons and tactics, the following areas require special attention in applying risk mitigation strategies and although not applicable to every facility, may consider the following:

- Carparks and external environments
  - CPTED considerations applicable to shift workers
- Building entrance / exits, thoroughfares, lobby's, waiting areas etc.
- Plant rooms and critical infrastructure
- Helicopter landing sites / helipads
  - Access control and emergency retrieval
- Waste disposal / storage areas
  - Storage and disposal of hazardous substances, clinical waste, and drug diversion prevention
  - Storage and disposal of weapons and other illicit substances
- Mail rooms
- Loading and unloading bays
- Areas that host special events and high-profile visitors
- Inpatients, mortuary, worker accommodation, and isolated work areas
- Pharmacy and pharmaceuticals
  - Receiving pharmaceutical stock
  - Storing pharmaceuticals
  - Internal distribution of pharmaceutical
- Newborn and paediatric security
- Storage and transport of cash
- Emergency departments (ED)
  - Access control to ambulatory and ambulance entrance
  - Design of ED including waiting and reception / triage / nurses' stations
  - Duress alarms either mobile or wall mounted / fixed point duress alarms
  - Video surveillance, considering procedures, location, coverage, and type
- Mental health facilities
  - Physical security: maintenance and correct use of appropriate equipment, technology, and appropriate building design
  - Procedural security: application of se procedures, routines and audits that enable safe practices
  - Relational security: formation of a therapeutic relationship between workers and patients, centred in a continuing risk assessment

Typically linked to a relatively deescalated likelihood and escalated consequence the below are some examples and notes regarding potential threats and linked vulnerabilities.

Potential threat (examples only)	Potential vulnerability considerations (and contributing factors) (examples only and notes)
Theft occurs when physical security controls are ineffective at deterring and detecting criminal activity	<ul style="list-style-type: none"> <li>• lack of security personnel presence and patrols</li> <li>• surveillance monitoring capabilities</li> <li>• level of human activity in and areas (crowded places)</li> <li>• public access points</li> <li>• points of vulnerability in building</li> </ul>
Abduction of patients particularly newborn and paediatric patients can occur when offenders exploit weakness within physical security controls	<ul style="list-style-type: none"> <li>• staff / personnel identification</li> <li>• parent / carer / custodian identification</li> <li>• access control and visiting hours</li> <li>• adequacy of response</li> <li>• surveillance monitoring capabilities</li> </ul>
Assault and occupational violence (workplace aggression) may occur due to the nature of facilities and services provided	<ul style="list-style-type: none"> <li>• lack of security personnel presence and patrols</li> <li>• adequacy of response</li> <li>• staff training in security awareness</li> <li>• surveillance monitoring capabilities</li> </ul>
Violent protests may employ tactics that involve violence and destruction directed at property, infrastructure, and people.	<ul style="list-style-type: none"> <li>• adequacy of access control</li> <li>• public access points</li> <li>• points of vulnerability in building</li> <li>• location and accessibility of plant rooms</li> </ul>
Arson incidents can be motivated by a desire to cause large scale destruction or could be a result of recklessness with fire or deliberate use of fire to cause significant damage and threaten the safety of others potentially using accelerants.	<ul style="list-style-type: none"> <li>• facility and contents could be effectively damaged or destroyed by fire</li> <li>• combustible goods stored insecurely inside the facility buildings, or easily accessible</li> <li>• surrounding environment / climatic conditions</li> <li>• fire detection and prevention mechanisms</li> <li>• design allows for rapid escalation of fire / absence of compartmentation in building layout</li> </ul>

Potential threat (examples only)	Potential vulnerability considerations (and contributing factors) (examples only and notes)
<p>Hostile vehicle attack includes the use of a vehicle as a weapon to threaten life and damage property.</p>	<ul style="list-style-type: none"> <li>• level of human activity in and areas (crowded places)</li> <li>• ability for vehicles to approach the building</li> <li>• building proximity to traditional vehicle access routes</li> <li>• potential attack paths presented by non-traditional vehicle access routes</li> <li>• points of vulnerability in building</li> </ul>
<p>Improvised explosive devices (IEDs) have potential to be delivered or detonated in several ways including letters, parcels, and motor vehicles.</p>	<ul style="list-style-type: none"> <li>• critical assets within facility and location of facility</li> <li>• level of human activity in and areas (crowded places)</li> <li>• public access points</li> <li>• points of vulnerability in building</li> </ul>
<p>Chemical, biological, and radiological (CBR) agents have potential threaten life and damage property or contaminate buildings.</p>	<ul style="list-style-type: none"> <li>• accessibility of ventilation systems and air intakes</li> <li>• location and accessibility of plant rooms</li> <li>• storage of hazardous chemicals</li> <li>• areas and systems that by virtue of design allow distribution of airborne agents throughout the building</li> </ul>
<p>Sabotage includes the attack or compromise of infrastructure, systems, and assets resulting in operational disruption, loss of information financial loss and reputational impacts.</p>	<ul style="list-style-type: none"> <li>• adequacy of access control</li> <li>• number of staff with access to systems</li> <li>• criticality of infrastructure, assets, and information systems</li> </ul>
<p>Cyber-attacks / threats have potential to undermine the effectiveness of electronic (IT) and connected physical security controls.</p>	<ul style="list-style-type: none"> <li>• devices applications and networks components that allow organisations to digitally interact (internal / external)</li> <li>• building automation and computer-based controls systems</li> <li>• systems connected to the internet</li> </ul>
<p>Armed attacks include assaults that have potential to cause damage, injuries, and casualties using weapons.</p>	<ul style="list-style-type: none"> <li>• adequacy of access control</li> <li>• level of human activity in and areas (crowded places)</li> </ul>

## Appendix 14

### A guide for two-way / radios communications

Maintaining radio communication protocol preserves the security of the information being transmitted. Persons operating radios should avoid using names, instead opting for controlled and designated call signs. Call signs commonly include phonetic alphabet and associated number, such as: S1 / Sierra 1 (security officer no.1) or F2 / Foxtrot 2 (FSSO 2), and so on (as determined by each HHS).

The primary function of a call sign is to protect the identity of the parties involved in the radio transmission and serves to simplify matters when communicating between large groups of people. A call sign may be assigned to each position. Call signs are based on areas of responsibility. A call sign is not owned by an individual rather it is occupied by a position (shift dependant) or role when on duty.

When transmitting messages call signs used in conjunction with correct protocol ensures messages remain concise and easily understood. Consider the following:

- Start the message with your call sign and indicate to the call sign of intended contact
- Finish transmissions with the word OVER, informing the call sign you are communicating with, that you are waiting for their reply
- Use the word ROGER to let them know you have understood their transmission
- To end the conversation, use the word OUT. This informs the recipient that you are finished with the conversation

The below are commonly used phrases that should be used in conjunction with the phonetic alphabet:

- Affirmative / Affirm – Yes
- Negative – No
- Come in – requesting contact
- Go ahead— ready for you to send your message
- Copy— message has been heard and understood
- Over – I have finished talking and I am listening for your reply (over to you)
- Standby— pause for the next transmission or further instruction
- Out – I have finished talking to you and do not expect a reply

The phonetic alphabet reduces the chance of confusing transmissions or misunderstanding messages involving the spelling of words or letters (i.e. car registration letters).

### Phonetic alphabet

<b>A</b> ALPHA	<b>B</b> BRAVO	<b>C</b> CHARLIE	<b>D</b> DELTA	<b>E</b> ECHO
<b>F</b>	<b>G</b>	<b>H</b>	<b>I</b>	<b>J</b>

Security guidelines

FOXTROT	GOLF	HOTEL	INDIA	JULIET
<b>K</b> KILO	<b>L</b> LIMA	<b>M</b> MIKE	<b>N</b> NOVEMBER	<b>O</b> OSCAR
<b>P</b> PAPA	<b>Q</b> QUEBEC	<b>R</b> ROMEO	<b>S</b> SIERRA	<b>T</b> TANGO
<b>U</b> UNIFORM	<b>V</b> VICTOR	<b>W</b> WHISKEY	<b>X</b> X-RAY	<b>Y</b> YANKEE
<b>Z</b> ZULU				

#### Two-Way Radio Etiquette (considerations)

- Don't interrupt transitions of others
- Avoid transmitting sensitive or confidential information
- Decide what you are going say and to whom it is meant for prior to sending message
- Ensure conversations are concise, precise, and clear as possible
- avoid long and complicated sentences. If your message is long, divide it into separate shorter messages

## Appendix 15A guide for BWC procedures

Procedures include, but may not be limited to the following:

- HSOs are to be advised of the specific purpose of the BWC, trained in use, and educated in the ethical use of the devices and any use of the device must be able to withstand later scrutiny
- Only BWCs supplied and managed through local arrangements should be used within the HHS's facilities
- BWCs may be activated prior to attending or during the below situations (depending on local arrangement). When recording cannot be commenced beforehand, the BWC is to be activated as soon as practicable:
  - When exercising a power under legislation
  - When applying a use of force or in response to incidents involving occupational violence or duress activation
  - To provide a record of evidence which assists in the investigation of an offence or suspected offence
- At the commencement of shift, HSOs are to ensure the BWC is fully charged, and all previous data collected has been uploaded prior to removing from the docking station
- HSOs performing operational duties are to wear and use a BWC during their shift, The BWC should be worn in a location where the lens will not be inadvertently obscured
- Where practicable, HSOs are to advise involved persons that they are recording their activities and conversation at the earliest possible opportunity by stating words to the effect of: *"I must advise you that events and conversations that take place between us are being video recorded for the purpose of accuracy when recalling this incident"*
- HSOs are to exercise reasonable care to ensure that the device remains functional and undamaged
- Initial statements at the time of the incident can be recorded on a BWC, and written statements should also be obtained from witnesses for presentation in court.
- BWC do not remove the necessity for HSOs to make written notes or obtain written statements from witnesses. BWCs are used to corroborate and not replace evidence from other sources
- At the conclusion of shift, the BWC device is to be returned to the docking station to charge and upload data
- A BWC register may be established to ensure:
  - The shift supervisor or equivalent position checks each BWC device when returned,
  - Details of the return are entered in the BWC register
  - Loss or damage is investigated to determine the cause
  - May be reviewed monthly along with an audit of the Evidence.com cloud storage system
  - The ability to review and share recorded footage is restricted to the management positions within the security service or staff delegated

Security guidelines

Queensland Occupational Violence Strategy Unit (QOVSU)  
Effective date: 9 December 2022

- Employees have a right to apply to review recorded images except in cases where authorised agencies or the HHS are exercising their legislative powers and review of images by staff would be deemed to affect the integrity of an investigation

### **Evidentiary integrity**

BWC data may be used as evidence in a court. The content of images shall be clear and contain the Evidence.com program, which complies with the criteria of this requirement and produces:

- Creation date
- Date and time stamp
- Proof of non-tamper
- Verification methodology

All captured footage is uploaded through the docking station and stored within the 'Evidence.com' program. Management positions (or equivalent) within the security service have the administration rights and work within Evidence.com program for compliance.

Delegated positions have the right to view and share any footage for the purpose of an investigation through the Evidence.com program. The Evidence.com program produces a log number for any access through the system and records any viewing of footage and shared footage for compliance. The Delegated positions right to the system does not allow them to tamper, delete or copy any footage.

Evidence.com program is a protected system with controlled rights and access. Officers have right to view only the camera they have assigned to themselves. The Evidence.com program produces a log number for any access through the system and records any viewing of footage for compliance.

## Appendix 16 AS 4485.1 Security lighting levels

Situation	Average lx	Minimum lx
Car parks (outdoor)	20	10
Car parks (in door)	40	20
General grounds adjacent to areas used at night	5	3
Walkways	20	10
Areas adjacent to entry / exit	5	30
General grounds used for night activity	20	10



Appendix 17 **Selecting commercial safes and vaults to protect physical assets, other than classified assets, PSPF**

Business impact level	1. Low business impact	2. Low to medium business impact	3. High business impact	4. Extreme business impact	5. Catastrophic business impact
Zone One	Determined by an entity risk assessment, locked commercial container recommended.	Determined by an entity risk assessment, commercial safe or vault recommended.	AS 3809 commercial safe or vault.	AS 3809 high security safe or vault.	Not to be held unless unavoidable.
Zone Two	Determined by an entity risk assessment, locked commercial container recommended.	Determined by an entity risk assessment,	Determined by an entity risk assessment, commercial safe or vault recommended.	AS 3809 medium security safe or vault recommended.	Not to be held unless unavoidable.
Zone Three	Determined by an entity risk assessment.	Determined by an entity risk assessment,	Determined by an entity risk assessment,	AS 3809 commercial safe or vault recommended.	AS 3809 high or very high security safe or vault recommended.
Zone Four	Determined by an entity risk assessment.	Determined by an entity risk assessment,	Determined by an entity risk assessment,	commercial safe or vault recommended.	AS 3809 medium or high security safe or vault recommended.
Zone Five	Determined by an entity risk assessment.	Determined by an entity risk assessment,	Determined by an entity risk assessment,	commercial safe or vault recommended.	AS 3809 medium or high security safe or vault recommended.
<ul style="list-style-type: none"> <li>• <b>Security planning and risk management – Guideline, Appendix 3. Assessing sensitive and security classified information, PSPF</b></li> <li>• <b>Security planning and risk management – Guideline, Appendix 7. Business impact levels for consequence of threat, PSPF (example)</b></li> </ul>					

Appendix 18 **AS 4083: 2010, s2 Emergency codes**, states: “Colour codes for emergencies in a facility, other than those listed, shall not be used as they may lead to confusion.”

**a) Fire / smoke code red** typical initial actions may include (but are not limited to):

- Ensuring the immediate safety of anyone within the affected or impacted vicinity
- Taking measures to ensure fire authorities are notified: Queensland Fire and Emergency Services (QFES) (Fire Communications Centre), in emergency call 000, in non-emergency call 13 QGOV (13 74 68). [Contact Us | Queensland Fire and Emergency Services \(qfes.qld.gov.au\)](https://www.qfes.qld.gov.au)
- Contacting appropriate emergency officer (s), this may include: HSOs, IRTs, ERTs (or equivalent response teams) which may be contacted through internal mechanisms such a switchboard operator (if personnel have not responded to activated alarms)

**Corporate services - fire warden roles and responsibilities**, states: “Ensure you know the R.A.C.E. procedure in the event of a fire:

*R = remove people from immediate danger*

*A = alert: call emergency number 000 / break glass / notify nearby staff*

*C = confine fire and smoke (if possible, close windows and doors)*

*E = extinguish (control fire if safe to do so) or evacuate (through nearest fire exit or smoke door)”*

**Note.** The above information is guidance only and does not supersede existing policies, procedure and plans utilised by HHSs.

Dependant on the HHS or facility expectations or roles and responsibilities delegated to HSOs may include that of the: Chief Fire Warden or Area / Floor Warden during times of code red activations and duties may include liaising with and escorting QFES, controlling the Fire Indicator Panel (FIP), and other fire systems.

Please refer to: AS4083: 2010, for a general action plan in response to fire or smoke and refer to local procedures and plans for specific instructions for local processes to be followed in the event of fire / smoke: code red.

**Building Fire Safety Regulation 2008 (Qld)**, defines: first-response evacuation instructions and evacuation coordination procedures.

**b) Evacuation code orange** typically involves the rapid and safe removal of persons (patients, visitors, staff, and others) from a facility or area within the facility.

AS 4083:2010 describes the authority to evacuate. For best results this standard should be referenced when developing evacuation (code orange) instructions.

**AS 4083:2010 s5.8.2 Assessing the situation**, states: “The situation should be assessed by a senior staff member, present in the area at the time, before the decision to evacuate is made, having regard to the:

- (a) Seriousness and relevance of the threat to human safety
- (b) Proximity of hazards which may be relevant to the situation, and
- (c) Nature and type of patient in the area”

The following summarised evacuation stages may be worth considering dependant on the severity of the situation:

- **Stage 1** removal of people from the immediate danger area
- **Stage 2** removal to a safe area
- **Stage 3** complete evacuation of building

**Note.** The above information is guidance only and does not supersede existing policies, procedure and plans utilised by HHSs.

Dependant on the HHS or facility duties delegated to HSOs may include that to assist in evacuation processes during and outside code red activations. This may include, assisting through maintaining communications with involved parties, providing clear direction, escorting persons from one area to another, and assisting with head counts or roll calls to verify occupant attendance, as determined necessary by the HHS.

Please refer to: AS4083: 2010, for further information and refer to local practices for evacuation (code orange). Local evacuations instructions should align **with Building Fire Safety Regulation 2008 (Qld)**, which sets out evacuation instruction, evacuation signs and diagrams, and evacuation practice and plan requirements.

**c) Bomb threat code purple** AS 4083:2010 outlines:

- Types of specific and non-specific threats (written, telephone, and suspect objects including mail)
- Identification of suspect objects and actions to be taken, such as mnemonic (HOT UP) questioning as per below:
  - *Is the item:*
    - Hidden?**
    - Obviously, a bomb?**
    - Typical of its environment?**
  - Has there been:
    - Unauthorised access?**
    - Perimeter breach?**

- Processes to evaluate (threats and actions), notification responses (involving emergency services), search activities (with or without evacuation) and evacuation options (including partial evacuations)

**AS 4083:2010 s5.4**, states: *“Bomb threat is a serious public nuisance of modern times. Each bomb threat could be a prank or a warning of an impending bomb attack. Usually, they are committed by individuals seeking to create a state of alarm and confusion. The problem may be minimised by proper site-specific planning and nomination of appropriate decision – making authorities.”*

**Note.** The above information is guidance only and does not supersede existing policies, procedure and plans utilised by HHSs.

Dependant on the HHS or facility duties delegated to HSOs may include that to assist in evacuation processes and other tasks as necessary in response to threats made against the HHS or facility.

**d) Infrastructure and other internal emergencies:** **code yellow** AS 4083:2010 identifies the following as code yellow events:

- Electrical failure
- Medical gases (oxygen, air and other gases and suction) failures
- Water supply failure
- ICT (information communication technology) failures
- Incidents involving hazardous substances
- Structural damage

The above-mentioned events and any other event that has potential to adversely impact service delivery and the or the safety of persons may require frontline support from HSOs to effectively manage. Actions may include access control (restricting or providing access to areas), wayfinding, escorting contractors / service providers and so on. Please refer to local plans, practices, and functions for information.

**e) External emergency:** **code brown** AS 4083:2010 identifies the following non-exhaustive list of events that may cause a code brown:

- Aircraft, train, or bus crash
- Structural collapse
- Explosions
- Natural disaster
- Emergencies at another facility

A code brown may be declared if resources from the facility are required as part of a health response to an external emergency. Again, this may require frontline support from HSOs to effectively manage with actions that may see an increased presence requested (such as within ED) and actions like the supports mentioned for code yellow. Please refer to local emergency plans and sub plans (or equivalent).

f) **Personal threat** (armed or unarmed persons threatening injury to others or themselves, or illegal occupancy): **code black** AS 4083:2010 defines responses to code black events in following three key sections:

- 1) **Unarmed confrontation**, arising from threats of violence, threats made in a violent manner and threats of suicide, where these threats are made by an unarmed person

**AS 4083:2010 s5.6.2 Unarmed confrontation**, states: “...The proper evaluation and management of the aggressive, agitated, violent or threatening patient can decrease assault... The planning process should involve appropriate medical, nursing, administrative and security staff. Staff specialised in mental health are important in such planning, with the aim of minimising the risk of injury to staff, patients and others.”

- 2) **Armed confrontation**, in which AS 4083:2010 provides a procedure to follow, which includes (but are not limited to) the following summarised instructions to obey offenders’ instructions, stay out of danger, raise the alarm, follow notification and escalation processes, observe activity, and follow procedures to preserve the crime scene.

**AS 4083:2010 s5.6.3 Armed confrontation**, states: “...The following warning is suggested ‘UNDER NO CIRCUMSTANCES SHOULD STAFF, PATIENTS OR VISITORS PLACE THEMSELVES IN FURTHER JEOPARDY.’”

- 3) **Illegal occupancy**, AS 4083:2010, requires facilities to have appropriate emergency plans in place to address events including illegal occupancy, and provides appropriate actions to such event.

**Note.** The above does not supersede existing policies, procedure and plans utilised by HHSs. Please refer to local instructions.

The standard requires the planning process of these emergencies to be developed in consultation with local police (QPS) and other specialists for consistency with facility standard operating procedures. Dependant on local HHS arrangements HSOs may form part of a response team (ERT, IRT, or equivalent) that may be engaged to safely respond to local code black events with appropriate supports and coordination.

g) **Medical emergency:** **code blue** AS 4083:2010 requires facilities to be able to effectively respond to a medical emergency through, an action plan, staff training requirements in BLS (basic life support) and ALS (advanced life support) and recommends appropriate pharmaceuticals and equipment.

Please refer to local arrangements for specifics on response to medical emergencies. HSOs in and out of response teams (ERT, IRT, or equivalent) engaged to safely respond to local code black events and other security procedures, should be aware of how to activate a code blue response or notify appropriate persons to enable a code blue (if required).