

AS 4485.2:2021



Security for healthcare facilities

Part 2: Procedures guide



AS 4485.2:2021

This Australian Standard® was prepared by HT-008, Security for Health Care Facilities. It was approved on behalf of the Council of Standards Australia on 07 May 2021.

This Standard was published on 28 May 2021.

The following are represented on Committee HT-008:

- Australian Association of Practice Management
- Australian Council of Trade Unions (ACTU)
- Australian Council on Healthcare Standards
- Australian Healthcare and Hospitals Association
- Australian Medical Association
- Australian Nursing and Midwifery Federation
- Australian Private Hospitals Association
- Australian Security Industry Association
- CRANaplus
- Justice Health and Forensic Mental Health Network
- NSW Ministry of Health
- Queensland Health
- SA Health
- Security Providers Association of Australia

This Standard was issued in draft form for comment as DR AS 4485.2:2020.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76113 335 0

Security for healthcare facilities

Part 2: Procedures guide

Originated as AS 4485.2—1997.
Revised and redesignated as AS 4485.2:2021.

© Standards Australia Limited 2021

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by Standards Australia Committee HT-008, Security for Health Care Facilities, to supersede AS 4485.2—1997.

The policies, principles, standards and common practices outlined in this Standard provide guidance for the development and implementation of effective security systems throughout all healthcare facilities.

The major changes in this edition are as follows:

- (a) Content has been restructured to reflect updates to AS 4485.1.
- (b) Content has been updated to reflect current security technologies and practices.
- (c) Alignment with AS ISO 31000.

This Standard is part of a series, as follows:

- (i) AS 4485.1, *Security for healthcare facilities, Part 1: General requirements*
- (ii) AS 4485.2, *Security for healthcare facilities, Part 2: Procedures guide* (this Standard)

Part 1 sets out the essential requirements needed to provide a safe and secure environment for workers, patients and visitors in healthcare facilities. Part 2 is a guide to the implementation of security services.

Contents

Preface	ii
Section 1 Scope and general	1
1.1 Scope	1
1.2 Normative references	1
1.3 Terms and definitions	1
Section 2 Policies and procedures	3
2.1 Governance	3
2.2 Security administrator	3
2.2.1 Formal delegation	3
2.2.2 Role and responsibilities	3
2.2.3 Policy coordination	3
2.2.4 Other sources of expert advice	3
2.3 Other organizations	4
Section 3 Security risk assessment	5
3.1 Risk management	5
3.2 Important assets and property	5
3.3 Information	5
3.4 Assessment of threats	6
3.4.1 Non-deliberate threats	6
3.4.2 Criminal risks	6
3.4.3 Sources of information	6
3.5 Risk assessment	7
3.6 Vulnerability analysis	8
3.6.1 Factors affecting vulnerability	8
3.6.2 Actions to reduce vulnerabilities	8
Section 4 Physical security	9
4.1 General	9
4.2 Design and construction	9
4.2.1 Introduction	9
4.2.2 Crime prevention through environmental design	9
4.2.3 Utilities and critical infrastructure	11
4.2.4 Barrier protection	11
4.2.5 Doors and windows	12
4.2.6 Restricted areas	12
4.2.7 Uninterrupted power supply (UPS)	13
4.2.8 Helicopter landing site (HLS)	13
4.2.9 Design of worker accommodation	13
4.3 Facility security	15
4.3.1 Security equipment	15
4.3.2 Engineering equipment	15
4.3.3 Equipment security and asset control	15
4.3.4 Car park security and control	16
4.3.5 Emergency and retrieval vehicle and aircraft security	17
4.3.6 Secure storage	17
4.3.7 Property	17
4.3.8 Intruder alarm systems	18
4.3.9 Video surveillance	19
4.3.10 Duress alarms	19
4.3.11 Access control	20
4.3.12 Locks	21
4.3.13 Combination locks	21
4.3.14 Keys	22
4.3.15 Passes or identity cards	23

4.3.16	Visitor identification.....	25
4.3.17	Weapons and other dangerous items	26
4.3.18	Storage and disposal of hazardous substances	26
4.3.19	Disposal of clinical waste.....	26
4.3.20	Drug theft and diversion prevention.....	26
4.3.21	Valuable collectables	26
4.3.22	Close of business.....	27
4.3.23	Protocols for after-hours safety.....	27
4.4	Patient security	27
4.4.1	Missing patients.....	27
4.4.2	Restrictive interventions.....	27
4.4.3	Special considerations for patients with protective status (other than persons in custody)	27
4.4.4	Security of persons in custody	28
Section 5	Security officers	29
5.1	General.....	29
5.2	Security services	29
5.3	Tasks and functions	29
5.4	Selection and vetting	30
5.5	Uniform, dress and bearing	30
5.6	Equipment	31
5.7	Proprietary versus contract services	31
5.8	Licensing.....	31
Section 6	Security and safety of people.....	32
6.1	Introduction	32
6.2	Application	32
6.3	Nature of risks.....	32
6.4	Risks to people.....	32
6.5	Responsibility of people	33
6.6	Special considerations	33
6.6.1	General.....	33
6.6.2	Wards.....	33
6.6.3	Emergency departments and urgent care.....	33
6.6.4	Mental healthcare facilities.....	34
6.6.5	Public interface areas.....	35
6.6.6	Operating room security.....	35
6.6.7	Home visits.....	36
6.6.8	Movement of workers and others at night	36
6.6.9	Isolated work areas	36
6.6.10	Worker accommodation.....	36
6.6.11	Mortuary.....	36
6.6.12	Research, pathology and radiology laboratories	37
6.6.13	Storage and transport of cash.....	37
6.6.14	Family planning facilities.....	37
6.6.15	Terrorism	37
6.7	Risk reduction	38
6.7.1	General.....	38
6.7.2	Personal security precautions in the workplace	38
6.7.3	Commuting.....	38
6.7.4	Social media	38
Section 7	Security screening of workers and vendors	39
7.1	Introduction	39
7.2	Worker probity	39
7.3	Responsibility.....	39
Section 8	Incident procedures	41
8.1	General.....	41

8.2	Preservation of crime scene evidence	42
8.3	Reporting and investigation	42
8.3.1	Reporting	42
8.3.2	Investigation	43
8.3.3	Criminal proceedings	43
8.4	Post-incident management	43
8.4.1	General	43
8.4.2	Choice of people to provide support	43
8.4.3	Post-incident management	43
8.4.4	Supervisor's role	44
8.4.5	Post-trauma	44
8.4.6	Critical incidents and psychological debriefing	44
8.4.7	Post-incident operational debriefing	44
8.4.8	Counselling and psychological support	44
8.5	Minimizing the possibility of recurrence	44
Section 9	Newborn and paediatric security	46
9.1	General	46
9.1.1	General	46
9.1.2	Healthcare facilities	46
9.1.3	Security for newborns and paediatrics	46
9.1.4	Physical security	47
9.1.5	Parents, family or guardians' involvement in security measures	47
9.2	Assumption of care	47
9.2.1	General	47
9.2.2	Response to a possible abduction	48
9.3	Media strategies	48
9.4	Paediatric security	49
9.5	Adolescent security	49
9.6	Country and stand-alone maternity services	49
9.7	Child-minding services	49
9.8	Delivery suite	49
Section 10	Pharmacy and pharmaceuticals security	50
10.1	General	50
10.2	Application	50
10.2.1	General	50
10.2.2	Responsibility	50
10.3	Policies and procedures	50
10.4	Facilities and equipment	51
10.4.1	General	51
10.4.2	Design of storage areas	51
10.4.3	Designated secure areas	51
10.4.4	Facilities and equipment	51
10.4.5	Holding areas	51
10.5	Pharmacy computer systems	51
10.6	Purchasing of pharmaceuticals	51
10.6.1	General	51
10.6.2	Valid orders	51
10.7	Receiving of pharmaceuticals (stock)	52
10.8	Storage of pharmaceuticals	52
10.9	Internal distribution of pharmaceuticals	52
10.9.1	General	52
10.9.2	Distribution	52
Section 11	Education, induction and training	53
11.1	Healthcare security officers	53
11.1.1	Training	53
11.1.2	Additional competencies for supervisors	53
11.1.3	Custodial and escort officers	53

11.2	Workers other than healthcare security officers.....	54
11.2.1	Training considerations.....	54
11.2.2	Evaluation of security-related education and training activities.....	56
Section 12	Security for services provided outside of the healthcare facility	57
12.1	Introduction.....	57
12.2	Application.....	57
12.3	General procedures for home visits.....	57
12.3.1	Risk assessment.....	57
12.3.2	Security risks to be considered.....	57
12.3.3	Potential risk controls.....	58
12.3.4	Alternative arrangements.....	58
12.3.5	Home visiting procedures.....	58
12.3.6	Vehicle breakdown.....	59
Section 13	Geographically remote or higher environmental risk healthcare facilities.....	60
13.1	General.....	60
13.2	Recruitment briefing.....	60
13.3	Security provisions.....	63
13.3.1	General.....	63
13.3.2	Remote area worker accommodation.....	63
13.3.3	Lighting.....	64
13.3.4	Doors and windows.....	64
13.3.5	Fencing.....	64
13.3.6	Suitable vehicle.....	64
13.3.7	Garaging and storage.....	64
13.3.8	Communications.....	64
13.3.9	Fire protection.....	65
13.3.10	Security awareness training.....	65
13.3.11	Emergency management plans.....	65
13.4	Security policies.....	65
Bibliography		66

Australian Standard®

Security for healthcare facilities

Part 2: Procedures guide

Section 1 Scope and general

1.1 Scope

This Standard provides guidance and explanatory material to assist with the implementation of the requirements of AS 4485.1.

1.2 Normative references

There are no normative references in this document.

NOTE Documents for informative purposes are listed in the Bibliography.

1.3 Terms and definitions

For the purpose of this Standard, the terms and definitions given in AS 4485.1 and the following definitions apply.

1.3.1

attractive asset

item which is vital to the operations of the facility, has a high monetary value or is of a particularly attractive nature (e.g. jewellery or drug holdings)

1.3.2

burglar resistant areas

areas which are secured in a manner suitable for the handling of money, drugs and other attractive assets to a level which will resist entry by an experienced criminal deliberately trying to force entry with suitable equipment

1.3.3

chief executive officer

CEO

position at that level of responsibility and authority immediately below the facility's governing body or authority, or proprietor

1.3.4

intruder resistant areas

areas which are secured in a manner suitable for the handling and storage of property of value to the facility and hazardous materials, to a level that will resist attempted entry, either unintentional or by a person without appropriate skills and equipment

1.3.5

may

indicates the existence of an option

1.3.6

outreach services

any service which visits clients, or potential clients, in their homes or at an external site

1.3.7

should

indicates a recommendation

1.3.8
video surveillance system
VSS

system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which may be necessary for the surveillance of a protected area

[SOURCE: AS/NZS IEC 62676.4:2020]

Section 2 Policies and procedures

2.1 Governance

Healthcare facilities should have a centralized governance mechanism in place for coordination and implementation of the security policy and procedures.

2.2 Security administrator

2.2.1 Formal delegation

The chief executive officer (CEO) should formally delegate a person to be responsible for the management of the security function for that facility (e.g. Security Administrator). Depending on the size and complexity of the facility this person could perform the role in a full or part-time capacity. Ideally, this person should be able to have direct access to the CEO, independent of any normal line management reporting mechanism.

2.2.2 Role and responsibilities

The facility security administrator should—

- (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 others about security matters; and
- (i) provide advice to planning groups on refurbishment and new construction projects.

NOTE Some jurisdictions may require that a person undertaking this role be licensed.

2.2.3 Policy coordination

The security administrator should establish a mechanism for developing, approving, disseminating and coordinating security policy, standards and procedures in an integrated manner throughout the facility.

2.2.4 Other sources of expert advice

While the security administrator should be capable of developing and managing the security programs, they should be aware of other sources of expert advice. Several avenues exist to provide security administrators with expert advice about physical security measures. These include the following:

- (a) External (independent) consultants who can assist facilities in conducting a security risk assessment and provide expert advice about security measures. The consultant selected should have a demonstrated knowledge and experience in security.

- (b) Private organizations and State and Federal government departments responsible for security design and construction can provide advice on equipment selection, installation and building structures related to physical security.
- (c) Agencies who provide advice on information technology (IT) security.
- (d) Police services which can provide advice about appropriate measures to minimize the possibility of criminal acts resulting in loss or harm.

2.3 Other organizations

It may be necessary to seek assistance from external organizations such as the Police, Fire Services, State Emergency Services and other similar bodies. Such organizations have particular responsibilities for dealing with certain emergencies. The executive management of each healthcare facility should consider establishing memoranda of understanding with some or all of these organizations, including sharing of relevant information.

Section 3 Security risk assessment

3.1 Risk management

AS ISO 31000 provides the general framework and processes that should be adapted and applied when developing security risk management for facilities. Insight and guidance on specific security risk management can be gained from HB 167. AS/NZS ISO 45001 should also be applied where appropriate in the development of security risk management.

3.2 Important assets and property

The following is a non-exhaustive list of items that should be considered as part of security risk management:

- (a) Workers, patients and visitors.
- (b) Facility's reputation.
- (c) Buildings and surrounds, including critical infrastructure.
- (d) Plant and machinery.
- (e) Radioactive sources.
- (f) Essential services cupboards, boxes, pits and risers.
- (g) Office equipment, particularly computers (software and hardware).
- (h) Medical and associated equipment.
- (i) Drugs and controlled substances and other dangerous items.
- (j) Patient property.
- (k) Currency.
- (l) Vehicles.
- (m) Supplies and consumables.
- (n) Intellectual property.
- (o) Security office and system infrastructure.
- (p) Security and emergency communications infrastructure.
- (q) Security keys and access cards.
- (r) Storage of contraband.
- (s) Storage of confidential waste.
- (t) Food preparation areas.

3.3 Information

The following is a non-exhaustive list of information that needs to be considered as part of security risk management:

- (a) Information relating to plans, policies, finances and other matters associated with operating a healthcare facility.

- (b) Any personal and official records.
- (c) Building floor plans, especially showing security features and essential services details.
- (d) Details of drug holdings and locations.
- (e) Valuable or significant intellectual property.
- (f) Data from security systems, e.g. video surveillance footage, identification (ID) photo images, personal data.

Many facilities process and store information on computers, or computer systems, as well as in hard copy form. When identifying information to be protected, it is important to look at both electronic (locally and remotely stored) and hard copy holdings.

3.4 Assessment of threats

3.4.1 Non-deliberate threats

Not all risks which could impact on security will be deliberate or have a criminal connection. Human error, natural hazards outside of the facility's control and equipment failure are some examples of non-deliberate risks which could impact on the security of a facility. Such matters need to be considered during the risk assessment process.

Particular consideration should be given to patients who are a risk to themselves and/or others.

Security risk management and related business continuity planning (BCP) should fully consider the possible impact on security operations and the control of security risks during major natural disruptions, e.g. flooding from heavy storms. The BCP should consider the relevant risks, e.g. the loss of technical service support from contractors during such circumstances.

3.4.2 Criminal risks

Many threats will involve some form of criminal or illegal activity, such as burglary, theft, vandalism, molestation, violence or misuse of assets or information. The source of such risks could be from within ("insider threat") or external to the facility. The reasons for such individuals or groups posing a threat will be varied, but could include:

- (a) Theft (facility or personal property).
- (b) Targeted assault.
- (c) Abduction.
- (d) Arson.
- (e) Any person who targets a healthcare facility or individual with criminal intent.
- (f) People looking to illegally acquire personal information about patients or workers, or information concerning the management or operations of a facility.

3.4.3 Sources of information

Information relevant to assessing risks can be gathered from a wide variety of sources including, for example, incident reports, the facility's workers, contractors providing security services.

Police services are usually able to advise on the nature and level of criminal activity occurring in a particular location. The healthcare facility should establish and maintain a working relationship with local police, preferably requesting a liaison officer from police to the facility.

Past experience, liaison with similar facilities and security-related issues raised in safety committee meetings are other examples of information sources.

Sharing of information between departments within the facility is important to ensure important information is received in a timely manner to allow for appropriate management from a security perspective.

Care should be taken to ensure that potential threats are not dismissed without proper inquiries, or any risk underestimated.

3.5 Risk assessment

AS ISO 31000 is the essential source to develop an accurate and comprehensive picture of security risks at a facility, and to identify and implement strategies and measures to ensure reasoned and sustainable risk management. To complete an accurate risk assessment at a facility, the potential consequences or outcomes and the likelihood of security risk events occurring needs to be determined in consultation with all key stakeholders.

Security risks that relate to the potential consequences or adverse outcomes to a range of risk groups include the following:

- (a) People — workers, patients, visitors and vendors.
- (b) Property and assets.
- (c) Provision of services.
- (d) Essential services (e.g. electricity, communications, water).
- (e) Information.
- (f) Pharmaceuticals.
- (g) Food.
- (h) Public confidence and facility reputation.

The likelihood of security risk events occurring may be affected by a variety of internal and external facility specific factors including the following:

- (i) Facility design.
- (ii) Security operations implemented i.e. security officer resourcing, security patrols, response to alarm activations and security incidents.
- (iii) Level of competency and knowledge of workers regarding security management.
- (iv) Policies and procedures implemented i.e. safe work methods statement (SWMS), or equivalent, which provides full appreciation of hazards and risks associated with the roles and duties of the workers under the engagement.
- (v) Services provided and the manner by which these are provided i.e. patients under escort, for example by corrective services officers, immigration officers.
- (vi) Aggression by patients and relatives.
- (vii) Assault of workers outside of buildings (e.g. leaving work at night).
- (viii) Robbery of drugs and/or cash (e.g. facility café, automated teller machine (ATM) located on-site) etc.

Consideration should also be given to identifying and addressing vulnerabilities.

3.6 Vulnerability analysis

3.6.1 Factors affecting vulnerability

Factors which can contribute to the degree of vulnerability of an asset, information or person will most likely include:

- (a) Attractiveness as a target.
- (b) Suitability of facility design, including access and egress.
- (c) Effectiveness of security work practices.
- (d) The level of security in place for the protection of assets, information and person.
- (e) The ability to react to and recover from a security incident.
- (f) The safety culture and applications of security arrangements.

3.6.2 Actions to reduce vulnerabilities

The documented risk assessment should identify vulnerabilities and assist with determining the appropriate actions to effectively manage the risks. The actions for reducing vulnerabilities may include:

- (a) Hardening the physical perimeter of a facility, or the perimeters of areas within a facility.
- (b) Introducing, or improving, access control arrangements.
- (c) Employing security officers, both static and mobile.
- (d) Improving physical storage measures for drugs, money, information, etc.
- (e) Utilizing security technology and monitoring devices.
- (f) Improving perimeter lighting (e.g. in car parks and storage areas).
- (g) Improving computer and communications security.
- (h) Providing better security instructions, briefings and training for all workers.
- (i) Having adequate response mechanisms to deal quickly with security incidents, particularly the sounding of alarms.
- (j) Security training and security awareness programs.
- (k) Performance and compliance audits on security systems (e.g. duress alarms, emergency power back-up on systems) and contracted security services (e.g. patrols and system maintainers).
- (l) Police patrols.
- (m) Knowledge of expected incoming high (security) risk patient.
- (n) Credible engagement with non-security workers.

Section 4 Physical security

4.1 General

Physical security comprises the measures taken to protect workers, patients and visitors from deliberate harm and to protect equipment and property from loss or damage. Such measures include the control of the movement of people, the utilization of physical design features and structures and monitoring arrangements to manage security risks, including those risks that arise where equipment storing facility information is lost.

Measures should include the following:

- (a) Workplace design, including physical barriers designed to deter and minimize the possibility, or show evidence, of unauthorized entry/exit.
- (b) Entry/exit control measures designed to minimize the possibility of unauthorized access.
- (c) Monitoring systems designed to detect unauthorized entry/exit or other emergency situations.
- (d) Adequate responses to deal with security contingencies.

4.2 Design and construction

4.2.1 Introduction

Physical security measures for new buildings and refurbishment projects should be considered as early as possible, preferably during the concept and design stages. Engaging with architects, other disciplines, security management and administrators at concept, master planning and design development will ensure that physical security principles can be applied cost-effectively.

4.2.2 Crime prevention through environmental design

4.2.2.1 Overview

One area of security risk mitigation strategy is the application of crime prevention through environmental design (CPTED) principles. CPTED should inform the design of many elements, for example perimeter protection, landscaping, lighting, security technology, structural requirements, design of patient service areas, pharmacies and perimeter doors.

The location of some departments will warrant special consideration in the furniture design and access/exit requirements. Placements 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.

CPTED may support perceived safety by legitimate users of the facilities and may reduce the over reliance on security technology.

The environmental design should be fully appreciated and applied from the concept stages of any facility development. CPTED may be a requirement of the local planning authority.

4.2.2.2 Other considerations

Consideration should be given to the location and securing of areas in which classified information, drugs, currency, and attractive assets are stored or handled so that these areas are given appropriate protection. Particular care should also be taken when electronic information systems are to be installed.

Other factors that should be considered at the concept/design development stages include—

- (a) engineering requirements for security and associated equipment;

- (b) space for secure storage;
- (c) space for security officers;
- (d) special features for worker protection such as heavy barriers, safe havens;
- (e) power and cabling needs for security equipment;
- (f) server, communications and plant rooms;
- (g) secure storage facilities;
- (h) lockdown procedures;
- (i) loading docks and food services;
- (j) location and design of parking areas and related facilities; and
- (k) security of fire systems and other essential services.

4.2.2.3 Landscaping

Landscaping affects the ability of intruders to gain access and carry out their intended actions. Canopy (e.g. trees) and ground cover planting should be utilized in preference to screening planting (e.g. hedges). Trees and shrubs should be trimmed away from doors and windows, around car parks and pathways and not allowed to overhang buildings thereby reducing the opportunity for intruders to conceal themselves and gain access to roofs, windows and balconies.

4.2.2.4 Lighting

Lighting types, levels and plotting should be consistent around the facility's service environment including between buildings, car parks and at entries.

Healthcare facilities should establish and maintain an effective internal and external protective security and safety lighting system that allows for the following:

- (a) Sufficient lighting and continuity of illumination to all areas of access/egress, parking and any other service or activities provided by the facility in their normal business.
- (b) Lighting that has a deterrent effect on potential intruders and enhances the potential of detection.
- (c) External lighting design and installations to enhance detection, including clothing and other features of persons.
- (d) Movement through illuminated spaces.
- (e) High efficiency with low energy consumption where reasonably practicable.

Sufficient safety and security lighting should be connected to an uninterruptable power supply.

There are four main issues regarding external lighting:

- (i) Fit-for-purpose colour temperature consistency for pathways and gathering spaces.
- (ii) Avoidance of up-lighting.
- (iii) The use of luminaires that minimize glare.
- (iv) Complementing street and roadway lighting, particularly in terms of colour coordination and luminosity.

4.2.2.5 Signage

Signage is critical to the CPTED principles of territorial definition, access control and activity support. Refer to AS 1319 for information on sign classification and use.

Signage comprises the following:

- (a) Signs — displaying visual and/or audio text information.
- (b) Symbols — displaying illustrated representations of text information.
- (c) Notices — displaying warnings or messages using signs or international pictorial symbols.

The following five types of signage should be applied:

- (i) Way-finding or directional signs are for welcoming and reassuring “guidance systems”. They invite safe destination access. They are critical to ensuring that public access through and around the facility will reduce levels of destination and access uncertainty, refer to AS 1428.4.2.
- (ii) Destination signs (e.g. pre-determined emergency evacuation assembly points) through and around the facility will complement way-finding signage. They are points of identification when there is any sense (perception) of danger or emergency. Destination signage should be part of a way-finding continuum.
- (iii) Access limiting or controlling signage is appropriate to indicate public and private space separation. They also indicate restricted access to plant and utilities infrastructure.
- (iv) International “pictogram” warning signage should be used.
- (v) Emergency (including fire and exit) signage is subject to codified compliance. In addition to codified signs, consideration should be given to locating a series of “help” or assistance signs in more distant and/or vulnerable spaces.

4.2.3 Utilities and critical infrastructure

The security and protection of utilities and critical infrastructure, e.g. plant and communications rooms, fire hydrant boosters, energy supply, is critical. Highly restricted access should be maintained at all times. Access should be under video surveillance and doors alarmed and monitored.

Arrangements should be set out that clarify the monitoring responsibilities (including by video surveillance) for essential service facilities owned and controlled by external operators but that are located on facility property.

Alarms for security critical doors should not have the audible function of the alarm in the security control room/security office disabled, an example being emergency stair perimeter doors.

Some locations may require “tamper-evident” products, in particular coloured, durable security seals with unique numbers. Examples may be ceiling and air conditioning access hatches.

Barriers to prevent impact and damage of infrastructure by vehicles should be installed. Barriers should be certified by a qualified engineer to ensure fit for (risk) purpose.

4.2.4 Barrier protection

Purposely designed barrier protection such as fences, walls, gates, and ditches, should be considered to meet identified threats. Barriers may need to be used in conjunction with other measures where identified, such as hostile vehicle mitigation applications, lighting and IP network cameras, to provide maximum benefit.

Barriers may be required to mitigate the security risks associated with people (e.g. pedestrians and front doors), window panelled perimeter walls and infrastructure such as fuel and gas tanks, boom gates, bus and taxi waiting areas, water mains, fire suppression systems etc.

Suitable barrier protection should be considered for vulnerable areas. Examples that may require the installation of barrier protection may include the security office, human resource department, cash and drug holding areas, public enquiry/reception desks etc.

4.2.5 Doors and windows

Doors and windows to secure areas and rooms should be designed and constructed to resist forced entry. Timber door frames should not be used in these areas. Hinge pins should be such that they resist easy removal, e.g. fixed pins, security butt hinges, or dog bolts installed to prevent removal of the pins.

Doors to restricted access areas should have a viewing panel to allow workers inside to visually vet people requesting admission. The panel should provide a view of the external side of the door. A video surveillance camera located in the public area that views the door locality with a monitor within the secure area should be considered.

Security screen doors can be used as auxiliary protection and to allow additional ventilation in warm weather. Security screen doors should conform to AS 5039 and AS 5040.

Where perimeter doors are locked for security reasons during hours of darkness, consideration should be given to providing an intercom device to allow workers to be alerted by people seeking entry. It may be necessary to provide video surveillance coverage of such doors and allow the caller to be recognized before being allowed entry.

Windows should be reinforced. Where light but not ventilation is needed, windows can be replaced with heavy gauge glass bricks or glass panels secured within a metal frame. Windows not used for ventilation should be fixed to prevent them being opened. Windows used for ventilation should be fitted with keyed window locks. Where the risk assessment identifies that additional resistance is needed, consideration should also be given to applying shatter resistant film to glass, having glass replaced with laminated glass or installing security screen mesh or grilles in accordance with AS 5039 and AS 5040.

Safety glass, laminated glass or impact resistant transparent panels (i.e. plastics) should be used to glaze all windows and glass panel doors in high-risk traffic areas. Where float glass is installed, shatter resistant film should be applied to at least one surface (i.e. the surface facing the occupied side of the glass barrier).

A range of vandal resistant and bullet resistant materials are available to counter various threat scenarios. Expert advice should be sought when such threats are identified.

4.2.6 Restricted areas

4.2.6.1 General

Restricted areas, which may be a single room, a building, or a complex consisting of a number of buildings, are areas with measures in place for the secure handling and storage of classified matter and attractive assets. They are described in [Clause 4.2.6](#), to assist with the selection of appropriate security measures, to determine appropriate security procedures and to determine appropriate clearances and access privileges, where necessary, for people authorized to enter such areas.

Burglar resistant areas and intruder resistant areas, whether restricted areas or not, together with other measures, are used to protect people, information, and property.

Facilities with large holdings of classified material could seek specialist advice on the most cost-effective measures to adequately secure them.

4.2.6.2 Features of restricted areas

Restricted areas are those areas which have specific controls to restrict access to authorized persons only. A restricted area may be part or all of a burglar resistant or an intruder resistant area.

A restricted area should have the following features:

- (a) A means of preventing entry by unauthorized persons.
- (b) A means of identifying authorized persons, e.g. electronic access control requiring an authorized programmed proximity card.
- (c) Video surveillance options.
- (d) A means of logging entry and where required exit of authorized persons.
- (e) A means of logging people, information or property that has been removed from the restricted area.
- (f) A means of alerting the appropriate authorities in the event of a forced entry or a door opened too long based on the set down criteria.
- (g) Signage indicating restricted access.

4.2.6.3 Intruder and burglar resistant areas

The physical security features of an intruder and burglar resistant area should include the following:

- (a) Tamper-evident barriers, highly resistant to unauthorized entry/exit, with no unsecured openings.
- (b) A security alarm system with a reliable communications link to an effective response providing after-hours coverage of all areas where classified and attractive assets are handled or stored. On-site security officers, conducting after-hours internal patrols, physically checking all key points at random intervals not exceeding two hours, may be employed in lieu of a security alarm system, provided there are sufficient security officers to respond effectively to security-related incidents.
- (c) Video surveillance of the entry(s).

4.2.7 Uninterrupted power supply (UPS)

A suitable UPS system that supports critical infrastructure should be considered and, where installed, located in a secure environment.

4.2.8 Helicopter landing site (HLS)

If a helicopter landing site is incorporated into the design, refer to the Civil Aviation Authority (CASA) CAAP 92-2(2) and any state or territory health design and operational requirements.

4.2.9 Design of worker accommodation

Accommodation should be built to appropriate codes and standards for the locality, e.g. cyclone and earthquake resistant, including physical security such as solid core doors, locks, security rated screen doors and security rated screen mesh over windows, intruder alarms (refer to AS/NZS 2201), smoke alarms (refer to AS 3786) and be fully maintained. Environmental aspects such as heating, ventilation, air conditioning and emergency power should also be considered. Where possible, the location and construction of the external building or structure should facilitate safe and secure access to accommodation and to comply with the principles of CPTED (see [Clause 4.2.2](#)).

Properties should be securable with the following elements:

- (a) Where practicable, electronic access control should be installed. Otherwise, physical keys can be used with the following:
 - (i) Deadlocks to be provided and fully operational to all external doors, except designated fire exits.
 - (ii) External doors should be on their own master restricted key system. Master keys should be held by the manager of the residence and individual keys can be held by the tenant. Internal doors should be keyed alike if necessary. Refer to master keying schedule at each facility.
 - (iii) Keys should be on a registered system separate from the district master system to prevent the unauthorized access and copying of the keys.
 - (iv) External doors should have a mortice lock on both swinging and sliding doors. The locks should have a deadlock function except for designated fire exits.
 - (v) Internal doors should have a mortice lock. Bathroom and bedroom doors should have individual keys.
- (b) Security rated screens should be securely installed to the following:
 - (i) Screens should be installed to all openable parts of windows and to all windows below 3 m from ground level or accessible point i.e. awning, downpipe, fence, veranda.
 - (ii) Screen doors should be installed at all external doors and doors on external walls (except to fire doors). Construction and installation should be in accordance with AS 5039.
 - (iii) Suitable and functional catches and fittings should be provided to all windows.
- (c) Where a security risk assessment determines a higher potential for security risk—
 - (i) all glass areas of doors and windows should have security rated screens fitted;
 - (ii) consideration should be given to emergency egress capabilities; and
 - (iii) a (monitored) alarm system or duress alarm system may need to be installed and should be regularly tested.
- (d) Additional internal security and safety applications include the following:
 - (i) Fire detection and suppression equipment should be installed as well as available fire blankets.
 - (ii) Security and emergency procedures should be accessible within the accommodation.
- (e) External security applications include the following:
 - (i) Fencing and gates should be in good repair, catches provided and functional and all gates and security doors should have protection shields fitted at locks.
 - (ii) Pathway pole style lighting should be installed at and between accommodation, car parking, health facility (if on site), clothes drying and laundry areas (if external). Lighting at all external entry doors should be installed.
 - (iii) Liquid petroleum gas (LPG) bottles should be secured in a lockable cage.

4.3 Facility security

4.3.1 Security equipment

Where possible, a facility should adopt an integrated approach to security, ensuring compatibility of related equipment. The security equipment and its installation should comply with all relevant Australian Standards.

A facility should consider the following criteria in selecting a reputable supplier or security installer:

- (a) Evidence of conformance with industry licensing and insurance requirements.
- (b) Evidence of corporate or individual membership of industry or professional associations.
- (c) The company's trading history.
- (d) The opinions of the company's past and current clients.
- (e) Evidence of conformance with the requirements of quality assurance Standards.

4.3.2 Engineering equipment

The following matters relating to the maintenance, biomedical and utilities facilities should be addressed:

- (a) Security of tools and equipment that could be used as break-and-enter implements.
- (b) Security of vital services such as the supply of—
 - (i) electricity including emergency standby power equipment;
 - (ii) fuel gas;
 - (iii) medical gases;
 - (iv) water; and
 - (v) telephone.
- (c) Security of vital plant such as—
 - (i) hot water;
 - (ii) air conditioning (heating/cooling); and
 - (iii) refrigeration.
- (d) Security of maintenance documentation including—
 - (i) site and building plans;
 - (ii) maintenance schedule; and
 - (iii) contracts.
- (e) Valuable equipment being repaired or awaiting return.

4.3.3 Equipment security and asset control

Facilities should secure goods receiving areas, verify correct receipt of goods and maintain access control to the receiving and storage areas.

Storage areas should be theft resistant and have restricted access. A stringent equipment and goods accountability program should be operating in each facility department, featuring a clear audit trail of goods that passes from one area to another. Documentation should receive frequent spot checks for accuracy. Procedures for periodic and unscheduled internal audits should be put in place. Primary and secondary stores should operate under the same level of accountability.

Equipment and stores should be security and inventory marked with either engraving, non-lift labels or ultraviolet fluorescent marker pen. For items of high value, micro-dots or heavy metal spot identification may be warranted. Some security technology available allows the facility to tag/label equipment and trace movement of the items throughout the facility.

Condemned or damaged stock should be struck from the facility's asset register and removed promptly from the user's department and taken to a secure area, from where the supplies department should arrange disposal or repair.

Every facility should have a written policy on borrowing of equipment and tools by workers. Items officially on loan should be authorized in writing by a manager and accounted for by a loan card/documentation system.

It should be made clear to workers that unauthorized borrowing or misuse of equipment may be a criminal offence.

4.3.4 Car park security and control

A vehicle control and space allocation program should be developed and maintained by the security administrator. Access control and authorized vehicle identification measures should be implemented; a label, decal or access card system may be used.

All facilities should investigate through State and municipal council legislation the options available in the event that vehicles are illegally parked or abandoned on facility property.

Traffic flow and numbers should be investigated and road usage should be optimized with directional movement restrictions, thereby encouraging separate entry and exit points where possible.

Car park layout and allocations should consider the following—

- (a) shift work;
- (b) designated parking spaces for emergency services vehicles;
- (c) workers with priority;
- (d) accessible parking; and
- (e) visitors and patients.

Parking areas should be regularly patrolled by security and a security escort should be offered between the workplace and parking areas. Parking space in most facilities is at a premium and many vehicles are likely to be parked on the public streets surrounding the facility. Negotiations with local councils and a neighbourhood group may contribute to easing the vehicle and pedestrian traffic concerns as well as fostering good community relations.

See [Clause 4.2.2.4](#) for further information on car park lighting. Refer to AS 4485.1 for minimum lighting requirements.

Security measures such as video surveillance, lighting (refer to requirements in AS 4485.1), duress points and intrusion detection equipment should be used to improve safety. Worker and visitor parking should be separate.