AS 4485.1:2021

Australian STANDARD®

STANDARDS Australia

# Security for healthcare facilities

## Part 1: General requirements

AS 4485.1:2021

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 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
The Australian Council on Healthcare Standards

This Standard was issued in draft form for comment as DR AS 4485.1:2020.

**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 323 7

AS 4485.1:2021

# Security for healthcare facilities

## Part 1: General requirements

Originated as AS 4485.1—1997.
Revised and redesignated as AS 4485.1:2021.

# Preface

This Standard was prepared by Standards Australia Committee HT-008, Security for Health Care Facilities, to supersede AS 4485.1—1997.

The policies, principles, standards and common practices outlined in this Standard provide a framework 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.

(b) Content has been updated to reflect current security technologies and practices.

(c) Alignment with AS ISO 31000.

This Standard forms part of a series, as follows:

AS 4485.1, *Security for healthcare facilities, Part 1: General requirements* (this Standard)

AS 4485.2, *Security for healthcare facilities, Part 2: Procedures guide*

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

## Introduction

A high degree of consistency of approach to security throughout the healthcare industry is desirable to assist each facility to best fulfil its security responsibilities. This Standard aims to achieve this by encouraging facilities to adopt, wherever possible, a common approach to security issues.

The risks to be addressed vary from facility to facility. However, the following fundamental principles are applicable to most situations:

(a) Everyone has a right to be safe and secure at their place of work or residence. Patient safety and worker safety should not be addressed separately but in conjunction with one another.

(b) Organizations such as healthcare facilities have legal obligations to protect the personal and private information they hold about their workers and patients.

(c) It is necessary to protect other forms of information as well as valuable and attractive property for which the facility is responsible. It may also be important for insurance reasons to have a sound level of security.

(d) Often there will be contractual requirements for sound security practices to be in place.

(e) There may be a moral obligation to have sound security arrangements in place.

This Standard does not provide all the answers to the broad range of security issues which are faced by the wide variety of healthcare facilities that exist. There are likely to be occasions where specialist advice will be required from external agencies or organisations. In many cases it will be necessary to consider other legislation, policy, regulations, rules, or the like, when designing or applying security arrangements. Typically, these could be fire regulations, building codes, and work health and safety legislation.

The following are the most obvious and important outcomes for healthcare facilities:

(i) Provision of quality healthcare services to clients.

(ii) Maintenance of credibility with clients, boards of management and financial backers.

(iii) Financial viability.

(iv) Lower insurance costs.

(v) Lower lost work hours.

(vi) Administrative competency.

(vii) Reputation.

Factors contributing to an inability to realize outcomes include:

(A) Unsafe environment(s) for workers, patients and others at the facility.

(B) Poor safety culture and lack of security awareness.

(C) Unauthorized release, loss or misuse of —

  (1) sensitive information dealing with the administration of the facility; and

  (2) personal and private information about patients, workers and others for whom the facility holds personal details.

(D) Theft of vital and valuable assets, including drugs.

(E) Damage (e.g. vandalism) to property or equipment.

(F) Interruptions to operations due to protests, sit-ins and other acts creating a nuisance or safety concern.

(G) Unauthorized disruption to vital communications systems/links or utilities (e.g. computer systems/networks, power, gas and water) at the facility.

# NOTES

# Australian Standard®

# Security for healthcare facilities

## Part 1: General requirements

## Section 1 Scope and general

### 1.1 Scope

This Standard sets out the minimum requirements for healthcare facilities in developing policy, principles and procedures for the protection of —

(a) patients, workers and others required to attend such facilities;

(b) drugs and other controlled substances;

(c) information; and

(d) property owned or controlled by the facility, and the property of patients, workers and others at the facility.

Together, AS 4485.1 and AS 4485.2 provide requirements and guidance for the development and implementation of policy, principles and procedures for all public and private hospitals, facilities in remote locations, primary care facilities, community and residential aged-care facilities, and other locations where healthcare is delivered.

### 1.2 Application

This Standard is primarily for use by people who have direct responsibility for developing and managing security arrangements at a healthcare facility. It is designed to be used as a framework for developing security policy, systems and practices unique to individual facilities.

Security controls should not be applied indiscriminately. They should harmonize with other operational requirements of the facility and, in some cases, be tailored to specific areas within the facility.

Security procedures shall not impinge on the quality or effectiveness of patient care services.

### 1.3 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document.

NOTE Documents for informative purposes are listed in the Bibliography.

AS 4811, *Employment screening*

AS 5182, *Vendor credentialing for healthcare facilities*

AS/NZS 1158.3.1, *Lighting for roads and public spaces, Part 3.1: Pedestrian area (Category P) lighting—Performance and design requirements*

AS/NZS 1680.2.1, *Interior and workplace lighting, Part 2.1: Specific applications — Circulation spaces and other general areas*

AS/NZS 1680.2.5, *Interior and workplace lighting, Part 2.5: Hospital and medical tasks*

AS/NZS 1680.3, *Interior and workplace lighting, Part 3: Measurement, calculation and presentation of photometric data*

AS/NZS 1680.4, *Interior and workplace lighting, Part 4: Maintenance of electric lighting systems*

AS/NZS 1680.5, *Interior and workplace lighting, Part 5: Outdoor workplace lighting*

AS/NZS 4421, *Guard and patrol security services*

AS ISO 31000, *Risk management — Guidelines*

AS/NZS ISO 45001, *Occupational health and safety management systems — Requirements with guidance for use*

AS ISO/IEC 27001, *Information technology—Security techniques—Information security management systems—Requirements*

## 1.4 Terms and definitions

For the purpose of this document, the following terms and definitions apply.

**1.4.1**
**healthcare facility**
hospital, residential aged-care facility or other facility where healthcare (including related core services) is delivered to patients

**1.4.2**
**may**
indicates the existence of an option

**1.4.3**
**patient**
person receiving healthcare

Note 1 to entry: Patients include in-patients, out-patients, day patients, and outreach service patients.

**1.4.4**
**property**
anything belonging to a person or an entity, including buildings and other physical structures, personal possessions, and commercial assets

**1.4.5**
**protective security**
measures employed to address security issues

**1.4.6**
**protective status**
status assigned to patients unable to care for or protect themselves against significant harm or exploitation

**1.4.7**
**risk**
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018(en), 3.1]

**1.4.8**
**secure areas**
spaces requiring special security precautions, equipment or structural reinforcement, monitoring or observation

**1.4.9**
**security risk**
factor or event, 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

**1.4.10**
**security risk assessment**
methodical process of identifying, analysing and evaluating security risks and of determining appropriate controls

Note 1 to entry: Refer to AS/NZS ISO 45001 and AS ISO 31000 for further information.

**1.4.11**
**sensitive information**
private or confidential data relating to personal or commercial interests of healthcare facilities

**1.4.12**
**shall**
indicates that a statement is mandatory

**1.4.13**
**should**
indicates a recommendation

**1.4.14**
**threat**
risk occurrence that would have a negative impact

[SOURCE: ISO/TR 21506:2018(en), 3.83]

**1.4.15**
**work health and safety**
DEPRECATED: occupational health and safety

assessment and mitigation of risks impacting the health, safety or welfare of workers and others in the facility

Note 1 to entry: Refer to relevant federal, state and territory legislation to determine any legal requirements.

[SOURCE: © Commonwealth of Australia 2019]

# Section 2 Policies and procedures

## 2.1 General

The aim of a healthcare facility's security function is to ensure that a vigorous security policy and plan is implemented throughout the facility. Where appropriate, security policies and procedures should be developed to address the specific needs of individual areas within the facility.

## 2.2 Security framework

### 2.2.1 Development

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.

The individual roles and responsibilities of those involved in the maintenance of safe conditions should be documented in position descriptions.

### 2.2.2 Management

Facilities shall designate appropriate personnel to be responsible for the day-to-day management of the security function. Ideally, such a person should have expertise and qualifications in, and understanding of, the application of security principles. This is particularly important for large healthcare facilities, such as major hospitals, where a coordinated approach to security throughout the facility is highly desirable.

### 2.2.3 Employees

Facilities shall assign specific responsibilities to personnel for the application of security arrangements within their areas of operation and/or authority in accordance with the facility's security policy and procedures. This will include a specific duty of care for themselves, other workers and other persons, such as patients, for whom they are responsible.

## 2.3 Security instructions

Instructions on security policy, procedures and practices shall be provided to all relevant personnel upon commencement and when a change in policy and/or procedures occurs.

Security and safety related information for patients and visitors using the healthcare facilities should be provided as appropriate. This information may be distributed in a written form (e.g. brochures or signage) or communicated verbally by workers responsible for providing such instructions, e.g. fire, safety and/or security officer/s.

Documented security instructions shall be complemented by regular security education sessions (see Clause 11.1) for workers and others as appropriate.

# Section 3 Security risk assessment

## 3.1 General

To implement an effective security program, a facility shall make an assessment of the potential threats, vulnerabilities and risks it will need to manage, including the appropriateness and effectiveness of current controls.

The security risks to each healthcare facility will vary depending on its operations, location, perceived or known value of information and assets, and the image portrayed by the facility from a security perspective (e.g. it may be seen as an easy target because it has little or no security). It would be impossible for any organization to operate in a zero-risk environment.

The risk management process involving identification, analysis, assessment, control and continuous risk monitoring shall be undertaken in accordance with AS/NZS ISO 45001 and AS ISO 31000.

A healthcare facility shall be able to produce evidence that the findings of the security risk assessment have been implemented.

## 3.2 Asset identification

Before being able to manage its risks, a facility shall identify critical infrastructure, other important assets and information to be assessed.

NOTE Refer to AS 4485.2 for more information on asset identification.

## 3.3 Assessment of threats

The next step is to assess the risks that may be directed against persons, information or property which belong to, or which are located at, a facility/workplace, resulting in a negative impact. The assessment of these threats can only be usefully coordinated by a person in each facility who has a good understanding of the operations of the facility and who can obtain, analyse and assess potential threat information from a variety of sources.

NOTE Refer to AS 4485.2 for further information on threat assessment.

## 3.4 Frequency of risk assessments

Every healthcare facility shall take a systematic and coordinated approach, including an initial security risk assessment, to reduce potential security risk.

After an initial security risk assessment each healthcare facility shall conduct regular assessments in response to any significant change in the facility's —

(a) internal and/or external risk context;

(b) role, responsibilities and functions;

(c) property and buildings; and

(d) volume or severity of security incidents.

NOTE Frequency and intervals between risk assessments may be subject to additional regulatory and/or jurisdictional requirements.

A healthcare facility shall be able to produce evidence that it has conducted a comprehensive security risk assessment within the past three years.

## 3.5 Performance of risk assessments

Security risk assessments shall be conducted by qualified and experienced personnel in consultation with relevant workers and other stakeholders as part of —

(a) the decommissioning process to secure vacated premises; and

(b) the commissioning and planning processes for new and redeveloped facilities.

Security risk assessments shall be documented and plans developed.

Risk assessments and control plans shall be retained by the facility for a period of at least seven years.

NOTE There may be additional regulatory requirements affecting how long risk assessment and control plan documentation is to be retained.

## 3.6 Outcomes of risk assessment

Each risk assessment shall result in a plan to manage identified risks.

Policy, procedures, controls and training shall be reviewed, revised and updated in accordance with the security risk management plan.

The facility shall be able to produce evidence that the recommendations of the security risk management plan have been implemented. Each security risk management plan shall address the following:

(a) Identification of priority areas.

(b) Security governance.

(c) Security overview.

(d) Physical security.

(e) Security technology.

(f) Administrative and procedural security.

(g) Worker, patient and visitor safety.

(h) Security personnel.

(i) Information security management (in accordance with AS ISO/IEC 27001).

(j) Strategies to address vulnerabilities.

(k) Training and development.

(l) Traffic and vehicle management.

(m) Security activities.

(n) Incident management and response.

(o) Personal protective equipment.

(p) Emergency preparedness and business continuity.

NOTE Refer to AS 4485.2 for further information on the security risk management plan.

# Section 4 General security requirements

## 4.1 General

The policies and procedures applicable to general security requirements shall take into account the following topics:

(a) Provision for security features relevant to identified security threats in new buildings or major renovations.

(b) Emergency response procedures.

(c) Police response protocols.

(d) Special accommodation for patients with protective status.

(e) Security of patients in custody or detained under a mental health schedule.

(f) Safe assessment room for patients displaying aggressive behaviour.

(g) Designated secure areas.

(h) Patient surveillance and security equipment.

(i) Secure and restricted areas.

(j) Secure storage:

  (i) Weapons.

  (ii) Personal effects.

  (iii) Valuables.

(k) Alarm systems:

  (i) Duress.

  (ii) Intruder.

(l) Alarm testing and maintenance.

(m) Access control.

(n) Video surveillance systems.

(o) Use of passes or identity cards:

  (i) Workers.

  (ii) Visitors.

  (iii) Media.

  (iv) Contractors.

(p) Doors and windows.

(q) Keys and locks.

(r) Key control.

(s) Security lighting.

(t) Signage:

(i) Security.

(ii) Way-finding.

(iii) Destination.

(iv) Access limiting.

(v) Warning.

(vi) Emergency.

(u) Lockdown.

(v) Patient security; general and special cases, e.g. visiting very important persons (VIPs), patients in custody or patients admitted under a mental health schedule being treated in the facility who may impose special considerations on the facility.

(w) Medication security.

(x) Security of medical records and other confidential information.

(y) Allied health security arrangements.

(z) Security for non-medical departments.

(aa) Secure accommodation for workers and visitors.

(bb) Security awareness training.

## 4.2 Lighting

Healthcare facilities shall establish and maintain an internal and external protective security and safety lighting system to enhance safety and crime prevention.

All lighting shall meet the requirements of the following Standards:

(a) AS/NZS 1680.2.1.

(b) AS/NZS 1680.2.5.

(c) AS/NZS 1680.3.

(d) AS/NZS 1680.4.

(e) AS/NZS 1680.5.

(f) AS/NZS 1158.3.1.

After a security risk assessment, a specialist lighting organization shall be engaged to provide a lighting plan based on the security risk assessment.

NOTE 1 While these Standards provide minimum requirements, each context may also have additional considerations in the crime prevention context including increasing and/or varying beam angles, lumens output, colour, temperature, lux levels, video surveillance and emergency egress.

NOTE 2 The effects the lighting on the surrounding environment should be limited (refer to AS/NZS 4282).

Lighting assessment based on crime prevention principles shall be conducted as part of the commissioning process for all new developments or redevelopments.

NOTE 3 AS 4485.2 provides further information on lighting.

Security lighting levels shall be as indicated in Table 1.

**Table 1 — Security lighting levels**

| Situation | Average, lx | Minimum, lx |
|---|---|---|
| Car parks (outdoor) | 20 | 10 |
| Car parks (indoor) | 40 | 20 |
| General grounds adjacent to areas used at night | 5 | 3 |
| Walkways | 20 | 10 |
| Areas adjacent to entry/exit | 50 | 30 |
| General grounds used for night activity | 20 | 10 |

## 4.3 Design and construction

Relevant aspects of architecture, including engineering and technology, can be applied to a facility's security through Crime Prevention Through Environmental Design (CPTED). AS 4485.2 provides guidance on the application of CPTED principles as a crime prevention strategy. These principles can also be applied to existing facilities.

## 4.4 Procurement

Specific security provisions shall be included in tender documents, purchase agreements and service contracts where deemed necessary.

## 4.5 Security personnel

The policy and procedures applicable to security services shall take into account the following topics:

(a) Vetting of potential workers (see Section 6).

(b) Specialized training for security officers (see Clause 11.2).

(c) Performance requirements and contractual provisions for contracted services.

NOTE Further guidance on strategies that should be considered for the implementation and operation security services is given in AS 4485.2.

## Section 5 Security and safety of people

Healthcare facilities have a responsibility and duty of care to provide for the safety and security of patients, workers and visitors.

The policies and procedures shall take into account the following:

(a) Incident prevention.

(b) Incident control.

(c) Incident evaluation.

(d) Incident reporting.

(e) Post-incident support for workers.

(f) Public interface areas.

(g) People working in isolation.

(h) Worker accommodation.

(i) People working after normal business hours.

(j) Response to duress alarms and calls for assistance.

(k) Health services for high risk patients.

(l) Health services provided in high risk environments.

NOTE Further guidance on strategies that should be considered for the protection people for whom the organization has a duty of care is given in AS 4485.2.

## Section 6 Security screening of workers and vendors

Healthcare facilities shall develop and implement security policies and procedures appropriate to the facility's need for a practicable and effective workforce recruitment and promotion system.

The policies and procedures applicable to workforce recruitment requirements shall include an appropriate system for screening/vetting workers in accordance with AS 4811 and vendors in accordance with AS 5182.

## Section 7 Incident procedures

The policies and procedures for dealing with incidents shall take into account the following:

(a) Safety and security procedures during an incident.

(b) Preservation of a crime scene.

(c) Reporting and recording of incidents.

(d) Incident investigation.

(e) Post-incident management including psychological and physical first aid and debriefing of workers involved in incidents.

(f) Damage control and minimization of a potential re-occurrence.

NOTE A guide to strategies to be considered is given in AS 4485.2.

## Section 8 Neonatal and paediatric security

The policies and procedures for the security of newborn and paediatric patients shall take into account the following:

(a) Effective system for identifying newborn and paediatric patients.

(b) Identification and access authorization systems for workers, family, guardians and visitors.

(c) Physical security.

(d) Access control.

(e) Video surveillance.

(f) Involvement of parents, family or guardians in security measures.

(g) Protocols and procedures for community services.

NOTE Further guidance on strategies that should be considered for the protection newborn and paediatric patients and workers is given in AS 4485.2.

## Section 9 Security of pharmacy and pharmaceuticals

The policies and procedures for the security of pharmacies and pharmaceuticals shall take into account the following:

(a) Prescribing, dispensing, supply, transportation and storage of all pharmaceuticals within the facility.

(b) Dispensing of drugs in accordance with facility policy.

(c) Ordering, delivery and stock control of drugs.

(d) Handling of all investigational drugs and drugs used in clinical trials.

(e) Control of sample drugs brought into the facility and medications used in the facility by patients.

(f) Arrangements for controlled service outside normal pharmacy hours.

(g) Control of expired stock and disposal of pharmaceutical waste.

(h) Handling of cytotoxic drugs and other hazardous substances.

(i) Security of the pharmacy service and drug storage.

(j) Measures to prevent drug diversion and theft by workers.

(k) Clinical pharmacy services and drug administration.

(l) S8/S4 drug storage.

(m) Access control.

(n) Video surveillance.

NOTE 1 Refer to relevant federal, state and territory legislation to determine any legal requirements relating to security of pharmacy and pharmaceuticals.

NOTE 2 Further guidance on strategies that should be considered for the protection pharmacy and pharmaceuticals is given in AS 4485.2.

## Section 10 Data security

Healthcare facilities shall develop, implement and maintain policy and procedures designed to protect information and safeguard confidential and sensitive information from unauthorized use or disclosure.

Policy and procedure shall not be used or misused to prevent a worker from raising concerns or making public interest disclosures.

NOTE 1 Refer to relevant federal, state or territory "whistle-blowing" legislation to determine any legal requirements.

The policy and procedures applicable to sensitive information shall take into account the following:

(a) Types of information to be protected.

(b) An information classification structure that aligns with the facility's activities.

(c) Reproduction limitations.

(d) Limitations on access, use and disclosure.

NOTE 2 Refer to relevant federal, state and territory legislation to determine any legal requirements.

NOTE 3 Reference should be made to the ISO/IEC 27000 series for cybersecurity considerations.

# Section 11 Education, induction and training

## 11.1 All workers

Healthcare facilities shall ensure all workers have access to the required induction, education, instruction, supervision and training to maintain worker awareness of essential security issues. Risk assessment of roles and responsibilities of all workers shall be undertaken. This risk assessment shall identify the level of risk for the services being delivered and the relevant training needs. Examples of specific training include dementia specific training, mental health training, early intervention and physical intervention options.

The training strategy in place shall take into account the following:

(a) Security orientation for all workers, including security awareness, how to summon assistance and the requirements of a safety culture.

(b) Ongoing training, supervision and instruction for all workers to ensure that procedural knowledge is up to date. Training needs shall be identified as per risk assessment for identified risks.

(c) Collective training, such as exercises and practice responses.

(d) Manager-specific training to ensure they can effectively undertake their role in identifying, assessing and eliminating, or controlling security risks in their workplace. Training shall also equip managers to identify the training needs of their workers.

(e) Patient and visitor awareness programs.

NOTE Further guidance on training for non-security workers is given in AS 4485.2.

## 11.2 Security officers

Healthcare facilities shall ensure that all security officers have appropriate knowledge and competency relevant to their role and responsibilities. The roles and responsibilities are determined by the healthcare facility and will be subject to a risk assessment to ensure controls are in place so security officers remain safe.

All security officers shall meet the requirements of AS/NZS 4421.

NOTE 1 Training to the level specified in AS 4421 would not be sufficient for security officers who have regular contact with seriously ill, disabled or aggressive patients.

NOTE 2 An example training syllabus is outlined in AS 4485.2.

# Section 12 Special considerations

## 12.1 Security for external and community healthcare settings

In addition to general security measures outlined in Clause 4.1, the policy and procedures applicable to external services and community settings shall take into account the following topics:

(a) Procedures for home visits.

(b) Security of drugs and other goods carried by the service.

(c) Security for patient records carried by the service.

(d) Legal standing of workers providing the service.

(e) Appropriate vehicle allocation.

(f) Worker training specific to home visits and/or working in community settings.

(g) Appropriate means of communication in emergencies and the policies and procedures relevant to them.

(h) Continuity of telecommunication coverage and connection.

(i) Assessment of need for GPS tracking, satellite phones or personal locator beacon.

NOTE Further guidance on strategies and equipment that should be considered for the protection workers and property is given in AS 4485.2.

## 12.2 Security for geographically remote areas

The policies and procedures for services in geographically remote areas shall take into account the following:

(a) Appropriate worker numbers.

(b) Accommodation.

(c) Lighting (including path of travel between worker accommodation and health facility, if on campus).

(d) Doors and windows.

(e) Intruder detection.

(f) Duress alarms.

(g) Safe (safety) rooms.

(h) Fencing.

(i) Suitable vehicles.

(j) Vehicle parking including lighting.

(k) Garaging and storage.

(l) Communications protocols.

(m) Fire protection.

(n) Emergency management plans.

(o) Training specific to the special requirements of geographically remote areas.

(p) Worker pre-posting brief.

(q) Worker posting debrief.

(r) Continuity of telecommunication coverage and connection.

(s) Assessment of need for GPS tracking or personal locator beacon.

(t) Uninterrupted power supply (UPS).

(u) Helicopter and/or fixed wing landing site.

NOTE Further guidance on strategies that should be considered for the protection workers and property is given in AS 4485.2.

# Bibliography

AS 4485.2, *Security for healthcare facilities, Part 2: Procedures guide*

AS/NZS 4282, *Control of the obtrusive effects of outdoor lighting*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

# NOTES

**Standards Australia**
Standards Australia develops Australian Standards® and other documents of public benefit and national interest. These Standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth Government, Standards Australia is recognized as Australia's peak non-government national standards body.

For further information visit www.standards.org.au

**Australian Standards®**
Committees of experts from industry, governments, consumers and other relevant sectors prepare Australian Standards. The requirements or recommendations contained in published Standards are a consensus of the views of representative interests and also take account of comments received from other sources. They reflect the latest scientific and industry experience. Australian Standards are kept under continuous review after publication and are updated regularly to take account of changing technology.

**International Involvement**
Standards Australia is responsible for ensuring the Australian viewpoint is considered in the formulation of International Standards and that the latest international experience is incorporated in national Standards. This role is vital in assisting local industry to compete in international markets. Standards Australia represents Australia at both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

STANDARDS
Australia

GPO Box 476 Sydney NSW 2001
Phone (02) 9237 6000
mail@standards.org.au
www.standards.org.au

Printed in Australia

ISBN 978 1 76113 323 7