Australian Government
Department of Defence

Australian Government Information Technology Security Manual

ACSI 33

Defence Signals Directorate

Release Date: 18 June 2004

May be announced to the public.

May be released to the public.

DSD authorises access to the SECURITY-IN-CONFIDENCE version to those with a need-to-know such as agency security staff and commercial organisations contracted to or seeking to support Australian Government agencies. Those individuals or organisations that do not deal with HIGHLY PROTECTED information or nationally classified information of CONFIDENTIAL and above are **not** considered to have a need-to-know. The document is not to be made available, directly or indirectly, to the public, or to persons not considered to have a need-to-know, unless approved by DSD.

ISBN 0 642 29598 0

Foreword

The *Commonwealth Protective Security Manual* sets out the policies, practices and procedures that provide a protective security environment that is not only fundamental to good business and management practice, but also essential for good government. This is complemented by the policies and guidance provided in this *Australian Government Information Technology Security Manual*, which are designed to enable government agencies to achieve an assured information technology security environment. The publication of such a manual ensures that there is a minimum standard for information and communication technology security that can be applied consistently across government agencies.

The move to greater sharing and exchange of information between and within agencies, and the greater electronic interaction with the public and industry, pose new risks to Australian Government information. These risks need to be managed carefully and in a consistent way across government. This manual provides guidance to government departments, agencies and commercial service providers for managing those risks.

I encourage the users of this manual to provide feedback to the Defence Signals Directorate on its utility and content to assist in its future development. In this way we can ensure that policies and guidance evolve to meet the new and emerging business requirements of government departments and agencies.

Stephen Merchant
Director
Defence Signals Directorate

February 2004

This page is intentionally blank.

Table of Contents

This page is intentionally blank.

Part 1
ACSI 33 and IT Security

Overview

Introduction

101. This part contains important information relating to the *ACSI 33* document and how it relates to the security of Australian Government Information Technology (IT) systems. These topics contain information about:

- using the *ACSI 33* document effectively,
- important definitions, and
- the authority by which the standards and requirements within *ACSI 33* are set.

Contents

102. This part contains the following topics:

Using ACSI 33

Introduction

103. The information in this topic will help you to use *ACSI 33* more effectively.

Classification of ACSI 33

104. *ACSI 33* comes in two versions as shown in the table below.

Version/classification	System classifications covered
UNCLASSIFIED	• PUBLIC DOMAIN, • UNCLASSIFIED, • IN-CONFIDENCE, • RESTRICTED, and • PROTECTED.
SECURITY-IN-CONFIDENCE	As per the UNCLASSIFIED version plus: • HIGHLY PROTECTED, • CONFIDENTIAL, • SECRET, and • TOP SECRET.

Colour coding of and within ACSI 33

105. The two versions of *ACSI 33* have been colour coded to enable easy identification. In addition to the colour coding of the manual itself, text that only appears in the SECURITY-IN-CONFIDENCE version is also coloured.

Version/classification	Colour
UNCLASSIFIED	Yellow
SECURITY-IN-CONFIDENCE	Blue

Paragraph classifications

106. Those paragraphs containing information that is not UNCLASSIFIED have been marked with the appropriate classification. Any unmarked paragraphs may be treated as UNCLASSIFIED.

Paragraph numbering

107. Readers of the UNCLASSIFIED version will notice that in places the numbering is non-sequential. This is intentional and indicates that the missing text relates to classifications outside the scope of the version of the document being read.

Paragraph applicability and system classifications

108. Readers will note that some paragraph titles include a system classification reference, shown within square brackets. Paragraph titles that do not include a classification reference indicate that the paragraph applies to all classifications.

Continued on next page

Updates

109. *ACSI 33* is a living document. It is therefore important that agencies ensure that they are using the latest version of *ACSI 33*.

The table below provides the websites from which the latest versions of *ACSI 33* will be available.

Version	Location
UNCLASSIFIED	• DSD's Internet website **URL:** http://www.dsd.gov.au/ • Onsecure members' area **URL:** http://www.onsecure.gov.au/ • Defence Restricted Network
SECURITY-IN-CONFIDENCE	• Onsecure members' area **URL:** http://www.onsecure.gov.au/ • Defence Restricted Network

Feedback

110. DSD welcomes feedback about *ACSI 33*. To suggest improvements, or advise of inaccuracies or ambiguities, please contact DSD.

See: 'Contacting DSD' on page 2-3.

Target audience

111. The target audience for *ACSI 33* is:

- IT Security Advisers (ITSAs),
- Agency Security Advisers (ASAs),
- agency IT security administrators, system administrators, and network administrators,
- agency security policy staff,
- Infosec Registered Assessors (under the Infosec-Registered Assessor Program (I-RAP)),
- technical personnel with some IT security responsibilities, and
- security personnel with some understanding of and responsibility for IT security.

Continued on next page

Classification terminology

112. This document is consistent with the terminology used in the *PSM*. In particular it adopts the following terms:

Term	Type of information
National Security	Information classified RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET.
Non-National Security	Information classified IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED.
Classified	Information that is classified as either National Security or Non-National Security. **Important:** "Classified" information **does not** include information deemed to be UNCLASSIFIED.
UNCLASSIFIED	Information that has been assessed as not containing any material that warrants a security classification. Australian Government employees must, however, have authorisation prior to releasing this information to members of the public.
PUBLIC DOMAIN	Information authorised for unlimited public access and circulation, such as agency publications and websites.
CABINET-IN-CONFIDENCE	Documents prepared for consideration by Cabinet, including those in preparation. **Important:** The *PSM* and *Cabinet Handbook* state that the **minimum** protection given to Cabinet documents is to be equivalent to information marked as PROTECTED. Unless otherwise noted, references in *ACSI 33* to IN-CONFIDENCE **do not** include CABINET-IN-CONFIDENCE.

Continued on next page

How to use ACSI 33

113. The table below contains suggestions for using *ACSI 33*.

If you…	Then read the…
are a new user of *ACSI 33*,	first Part of the document for an overall picture of IT security for Australian Government agencies.
need to complete a specific IT security administrative task, **Example:** Writing a System Security Plan.	high-level process of IT security table to determine the applicable stage and relevant topics or sections. **See:** 'The High-Level Process of IT Security' on page 1-8.
need to know a specific security standard, **Example:** What are the requirements for sanitising a RESTRICTED hard disk?	table of contents or index to identify the appropriate topic in Part 3, System Security Standards. **See:** • Table of Contents. • Index on page I-1.
are unfamiliar with a term or abbreviation,	list of abbreviations or the glossary. **See:** 'Abbreviations, Glossary and Index' on page A-1.

Reduction of "background" material

114. Readers of earlier versions of *ACSI 33* will note that the amount of background material in this version has been significantly reduced. This approach has been taken in recognition of the increased volume of information relating to IT security available from other sources.

Continued on next page

Keywords for requirements

115. The table below defines the keywords used within this document to indicate the level of requirements. All keywords are presented in bold, upper-case format.

Keyword	Interpretation
MUST	The item is mandatory. **See:** 'Waivers against "MUSTs" and "MUST NOTs"' on page 1-6.
MUST NOT	Non-use of the item is mandatory. **See:** 'Waivers against "MUSTs" and "MUST NOTs"' on page 1-6.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. **See:** 'Deviations from "SHOULDs" and "SHOULD NOTs"' on page 1-6.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course. **See:** 'Deviations from "SHOULDs" and "SHOULD NOTs"' on page 1-6.
RECOMMENDS **RECOMMENDED**	The specified body's recommendation or suggestion. **Note:** Agencies deviating from a **RECOMMENDS** or **RECOMMENDED** are encouraged to document the reason(s) for doing so.

Waivers against "MUSTs" and "MUST NOTs"

116. Agencies deviating from a "**MUST"** or **"MUST NOT"**, **MUST** provide a waiver in accordance with the requirements of the *PSM*.

Deviations from "SHOULDs" and "SHOULD NOTs"

116.1. Agencies deviating from a "**SHOULD"** or **"SHOULD NOT", MUST** document:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- a date by which to review the decision, and
- management's approval.

Continued on next page

Legislation and other Government policy	117. Compliance with the requirements of *ASCI 33* must be undertaken subject to any obligations imposed by relevant legislation or law (Commonwealth, State or local) and subject to any overriding Commonwealth Government policy instruction. While this document does contain examples of when some laws may be relevant for agencies, there is no comprehensive consideration of such issues. Accordingly, agencies should rely on their own inquiries in that regard.
Deleted block	118. <deleted>

The High-Level Process of IT Security

About the process

119. IT security is an ongoing process. Stages within the process are inter-related, with each stage building on the results of the previous stage.

Starting the process

120. The best outcome for IT security is achieved when security is considered to be an integral part of the system. Therefore, DSD **RECOMMENDS** that the high-level process of IT security be considered during the analysis and design of a system.

Process

121. The table below describes the stages that DSD **RECOMMENDS** agencies follow to implement the appropriate IT security measures for each system.

Stage	Major tasks	See
1. Policy development	• Identify any existing relevant policies • Develop new policies, as required, to cover the requirements of each system.	Chapter 3 - Identifying and Developing IT Security Policies on page 2-18
2. Conduct risk management	• Identify the scope of the system to be protected. • Develop an initial RMP.	Chapter 4 - Risk Management on page 2-23
3. Plan development	• Develop a high-level IT security plan for use across related systems. • Develop or amend an SSP, possibly based on the high-level IT security plan, to cover each system.	Chapter 5 - Developing an SSP on page 2-35
4. Implementation	• Implement the SSP(s), including the purchase of hardware and software. • Develop and document the SOPs.	Chapter 6 - Developing and Maintaining Security SOPs on page 2-38
5. Certification	• Determine what needs certifying. • Obtain certification from the relevant person or organisation.	Chapter 7 - Certifying and Accrediting the Security of IT Systems on page 2-45
6. Accreditation	Obtain accreditation from the relevant authority.	
7. Maintenance	• Implement change control procedures. • Perform integrity checks.	Chapter 8 - Maintaining IT Security and Managing Security on page 2-59
8. Review	Review and revisit each stage of this process annually.	Chapter 9 - Reviewing IT Security on page 2-72

About IT Systems

Definition: IT system

122. For the purposes of this document, an IT system is a related set of hardware and software used for the communication, processing or storage of information, and the administrative framework in which it operates.

This definition includes, but is not limited to:

- computers, including laptops and stand-alone PCs, and their peripherals,
- other communication equipment,
- communication networks and other telecommunication facilities used to link such equipment together,
- the software used on all such equipment,
- the procedures used in the maintenance and administration of the equipment,
- the information,
- the people, and
- the physical environment.

Continued on next page

System modes

123. For the purposes of this document, an IT system is considered to operate in any one of the modes described in the table below.

See: 'System Users' on page 2-10 for more detail about system users, and 'Chapter 6 - Logical Access Control' on page 3-58 for more detail about system access.

Mode	Description
System High	**All** users with access to the system **MUST**: • hold a security clearance at least equal to the system classification, • have received any necessary briefings, and • have a need-to-know some of the information processed by the system, with need-to-know access control enforced by the system.
Dedicated	System High applies except that **all** users have a need-to-know **all** of the information processed by the system.
Compartmented	**All** users hold a security clearance at least equal to the system classification **but** not all users are formally authorised to access all compartments of information processed by the system. Access to the compartmented information is enforced by the system.
Multilevel	Information at two or more security classifications is processed and **some** of the users with system access are **not** security cleared for **some** of the information processed by the system. Within each security level of the system, users **MUST**: • hold a security clearance at least equal to the classification of that level, and • have a need-to-know some of the information within that level.

Other References

Further information

124. The table below identifies the location of further information contained in other documents.

For further information on...	See...
CABINET-IN-CONFIDENCE information security	*Cabinet Handbook*, Chapter 7, Security and Handling of Cabinet Documents (The Department of Prime Minister and Cabinet)
classification labelling,	*PSM* 2000, Part C, Information Security.
clearances,	*PSM* 2000, Part D, Personnel Security.
information handling procedures,	*PSM* 2000, Part C, Information Security.
information security management,	• AS/NZS ISO/IEC 17799:2001 - *Information Technology - Code of Practice for Information Security Management.* • AS/NZS 7799.2:2003 - *Information Security Management* (Standards Australia).
information security responsibilities,	*PSM* 2000, Part A, Protective Security Policy.
information security risk management,	*HB 231:2004 Information Security Risk Management Guidelines* (Standards Australia).
information technology security management,	*AS 13335:2003 Information Technology – Guidelines for the Management of IT Security* (Standards Australia).
key management - commercial grade	*AS 11770.1-2003 Information technology – Security techniques – Key management* (Standards Australia).
management of electronic records that may be used as evidence,	*HB 171:2003 Guidelines for the Management of IT Evidence* (Standards Australia).
physical security requirements,	*PSM* 2000, Part E, Physical Security.
reporting of security incidents,	*PSM* 2000, Part G, Guidelines on Security Incidents and Investigations.
risk management,	*AS/NZS 4360:1999 Risk Management* (Standards Australia).
storage and archival of government information,	*Archives Act 1983* (National Archives of Australia).

This page is intentionally blank.

Part 2
IT Security Administration

Overview

Introduction

This part contains information about the way IT security is managed, implemented and documented.

Contents

This part contains the following chapters:

Chapter 1 - IT Security Roles and Responsibilities

Overview

Introduction

101. This chapter contains information relating to IT security roles and responsibilities.

System specific responsibilities

102. Information relating to the system specific roles and responsibilities of IT Security Advisers, system managers, system administrators and system users **SHOULD** be included in the documentation produced for each system.

Contents

103. This chapter contains the following topics:

DSD

DSD's role

104. The Defence Signals Directorate (DSD) is required under the Intelligence Services Act 2001 to provide:

- material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means, and
- assistance to Commonwealth and State authorities in relation to cryptography and communications technologies.

Within DSD, the Information Security Group performs these roles.

Contacting DSD

105. Agencies should contact DSD for advice and assistance through their ITSA or ASA.

ITSAs and ASAs should address IT security questions to Information Security Group's Client Services Team, which can be contacted via:

- Email infosechelp@dsd.gov.au
- Phone 02 6265 0197
- Fax 02 6265 0328
- URL http://www.dsd.gov.au/

Other Organisations

Other organisations

106. The table below contains a brief description of some of the other organisations that have a role in the security of Government systems.

Organisation	Services
Protective Security Coordination Centre - Attorney-General's Department	Risk management and general government security. The PSCC's Training Centre provides protective security training, including IT security and risk management training. **URL:** http://www.ag.gov.au/
T4 Protective Security Section - Australian Security Intelligence Organisation	Protective security risk reviews and advice, and equipment testing. **URL:** http://www.asio.gov.au/
National Archives	Advice and guidelines on archives legislation and its application to IT systems. **URL:** http://www.naa.gov.au/
National Office of the Information Economy	Development, coordination and oversight of Government policy on electronic commerce, online services and the Internet. **URL:** http://www.noie.gov.au/
The Office of the Federal Privacy Commissioner	Advice on how to comply with the Privacy Act and related legislation. **URL:** http://www.privacy.gov.au/
Department of Foreign Affairs and Trade	Policy and advice for security overseas. **URL:** http://www.dfat.gov.au/
Australian National Audit Office	Performance audits and "Better Practice" guides for areas including information security. **URL:** http://www.anao.gov.au/
High Tech Crime Centre - Australian Federal Police	Law enforcement in relation to e-crime and other high tech crimes. **URL:** http://www.ahtcc.gov.au/
Australian Computer Emergency Response Team	Computer incident prevention, response and mitigation strategies. **URL:** http://www.auscert.org.au/

Appointing an IT Security Adviser

Requirement for ITSA

107. Paragraph A4.9 of the *PSM* states that an "ITSA should be appointed to be responsible for the security of the agency's electronic communication networks."

Agencies **SHOULD** appoint a person to the role of ITSA.

Where the agency is spread across a number of geographical sites, DSD **RECOMMENDS** that a local ITSA be appointed at each site.

Appointing an ITSA

108. The ITSA **MUST** have:

a. ready access to and full support from line management,
b. familiarity with information and/or IT security, and
c. a general knowledge of and experience in information processing systems used by the agency.

The ITSA **SHOULD** have a detailed knowledge of and experience with the particular systems in use, especially the:

a. operating systems,
b. access control features, and
c. auditing facilities.

DSD **RECOMMENDS** that the ITSA have no other roles or duties.

Where an agency has outsourced its IT, the ITSA **MUST** be independent of the outsourcer.
Important: The agency retains ultimate responsibility for the security of its IT systems, regardless of what roles or functions are outsourced.

Clearance and briefing status

109. The ITSA **MUST** be**:**

a. cleared for access to the highest classification of information processed by the agency's IT systems, and
b. able to be briefed into any compartmented material on the agency's IT systems.

ITSAs and administrative staff may have unrestricted access to large volumes of classified information. DSD **RECOMMENDS** that agencies consider clearing these staff to a higher clearance that that of the system classification.

IT Security Adviser Responsibilities

Primary responsibility

110. The ITSA is responsible for overseeing IT security within an agency.

Allocation of ITSA functions

111. The ITSA role is assigned to an individual. However, the functions of the ITSA may be performed by several individuals or teams.

Regardless of how the functions are allocated, responsibility for their effective execution remains with the appointed ITSA.

Administrative responsibilities

112. The ITSA is responsible for:

- identifying and recommending security improvements to systems,
- ensuring security aspects are considered as part of the change management process, and
- coordinating the development, maintenance and implementation of all security-related system documents, in conjunction with the System Managers.
  See: 'System Manager' on page 2-8.

Technical security advice and training responsibilities

113. The ITSA is responsible for:

- providing technical security advice involved with information system:
  - development,
  - acquisition,
  - implementation,
  - modification,
  - operation,
  - support,
  - architecture, and
- managing the information system security training program.

Reviewing responsibilities

114. The ITSA is responsible for the regular review of:

- system security,
- system audit trails and logs, and
- the integrity of the system configuration.

Continued on next page

SOPs

115. The ITSA **SHOULD** be familiar with all SOPs relating to the operation of the system, including the:

- ITSA,
- System Manager,
- System Administrator, and
- System Users.

Certification and accreditation responsibilities

116. The ITSA is responsible for assisting System Managers to obtain and maintain security accreditation of their systems.

See: System Manager: 'Certification and accreditation responsibilities' on page 2-8 for more detail.

System Manager

System Manager, ITSA and ASA

117. The ITSA and ASA **SHOULD** assist the System Manager in the performance of the System Manager's security-related responsibilities.

***PSM* reference: protection of resources**

118. Paragraph C4.5 of the *PSM* states that the ASA and ITSA "must not…be responsible for making decisions about what requires protection and what type of protection is most appropriate. This is, and must remain, the responsibility of the manager with functional control of the resource."

Documentation responsibilities

119. The System Manager is responsible for the development, maintenance and implementation of the following system documentation:

- RMP, **See:** 'Chapter 4 - Risk Management' on page 2-23.
- SSP, **See:** 'Chapter 5 - Developing an SSP' on page 2-35.
- SOP, **See:** 'Chapter 6 - Developing and Maintaining Security SOPs' on page 2-38.

Certification and accreditation responsibilities

120. The System Manager is responsible for obtaining and maintaining security accreditation of the system by:

- ensuring that the system complies with the relevant ITSP and SSP,
- ensuring that the impact of system modifications or additions on security mechanisms is managed properly,
- identifying any system changes that may imply a need for recertification and re-accreditation,
- ensuring that documentation is complete, accurate and up to date, and
- obtaining all necessary certifications.

See: 'Chapter 7 - Certifying and Accrediting the Security of IT Systems' on page 2-45 for more detail.

SOPs

121. The System Manager **SHOULD** be familiar with all SOPs relating to the operation of the system, including the:

a. ITSA,
b. System Manager,
c. System Administrator, and
d. System Users.

Continued on next page

Ensuring adherence to procedures	122. The System Manager is responsible for ensuring that procedures recorded in security documentation are followed.

System Users

Types of system users

123. This topic explains responsibilities for:

- general users, including all users with general access to the information system, and
- users with administrative privileges.

Responsibilities of general users

124. Agencies **SHOULD** ensure that general users read and comply with the relevant policies, plans and procedures for the system they are using.

Requirements: privileged access

125. As a **minimum**, all privileged users **MUST**:

a. read and comply with the relevant policies, plans and procedures for the system they are using,
b. possess a security clearance at least equal to the highest classification of information processed on a system,
c. protect the authenticators for privileged accounts at the highest level of information it secures,
   Example: Passwords for root and administrator accounts.
d. not share authenticators for privileged accounts without approval,
e. be responsible for all actions under their privileged accounts,
f. use privileged access only to perform authorised tasks and functions, and
g. report all potentially security-related information system problems to the ITSA.

Management of privileged access

126. Agencies **SHOULD**:

a. restrict privileged access to a minimum, and
b. closely audit privileged access.

Chapter 2 - Security Documentation

Overview

Introduction

201. A documentation framework is essential for organising all the required IT security documentation in a manner that allows for easy creation, reference and maintenance of the information.

Contents

202. This chapter contains the following topics:

Not included

203. The following topics are not included in this chapter:

Requirements for IT Security Documentation

Derivation from the *PSM*

204. The *PSM* requires all agencies to have security risk assessments, policies and plans that cover their IT systems. These documents **SHOULD** be consistent with each agency's high-level security documents:

a. Agency Security Policy,
b. Agency Security Risk Assessment, and
c. Agency Security Plan.

Further information on these documents is contained in the *PSM*, Parts A, B and C.

Information Technology Security Policy

205. Agencies **MUST** have an IT Security Policy (ITSP) document. The ITSP may form part of the Agency Information Security Policy which, in turn, may form part of the overall Agency Security Policy.

See: 'Chapter 3 - Identifying and Developing IT Security Policies' on page 2-18.

Risk Management Plan for IT systems

206. Agencies **SHOULD** ensure that every system is covered by a Risk Management Plan (RMP). Depending on the documentation framework chosen, multiple systems may be able to refer to or build upon a single RMP.

See: 'Chapter 4 - Risk Management' on page 2-23.

System Security Plans

207. Agencies **SHOULD** ensure that every system is covered by a System Security Plan (SSP). Depending on the documentation framework chosen, some details common to multiple systems may be consolidated in a higher level SSP.

See: 'Chapter 5 - Developing an SSP' on page 2-35.

SOPs

208. Agencies **SHOULD** ensure that SOPs are developed for every system. Depending on the documentation framework chosen, some procedures common to multiple systems may be consolidated into a higher level SOP.

See: 'Chapter 6 - Developing and Maintaining Security SOPs' on page 2-38.

Continued on next page

Using higher level documents to avoid repetition

210. Where there is some commonality between systems, DSD **RECOMMENDS** that higher level documents describing the common aspects be created. System-specific documents may then refer to the higher level documents, rather than repeating the information.

Possible areas of commonality include:

- geographical location,
- security classification,
- system functionality,
- common technical platform, and
- management boundaries.

Using a documentation framework

211. DSD **RECOMMENDS** that an over-arching document describing the agency's documentation framework be created and maintained. This document should include a complete listing of all IT security documents, show the document hierarchy, and define how agency documentation is mapped to the requirements described here.

Where agencies lack an existing, well-defined documentation framework, DSD **RECOMMENDS** that agencies use the document names defined in this chapter.

Continued on next page

Documentation content: Summary

212. An ITSP contains high-level policy objective. An RMP identifies the risks and appropriate treatments. An SSP documents the means for implementing the treatments in accordance with the policies. SOPs document the means by which the ITSA, system manager, administrator and user will comply with the SSP.

The table below contains examples of statements that may be found in each of these document types.

	Purpose	Example
ITSP	Provides high-level policy objectives.	Malicious software/data must not be introduced into the agency.
RMP	Identifies controls needed to meet agency policy	• Implement gateways on all agency connections to the Internet. • Install anti-virus software on all agency systems. • Disable removable media drives on workstations.
SSP	Actions for implementing RMP controls.	• Configure the firewall to deny all unknown connections. • Scan email for viruses. • Install floppy locks on all floppy drives.
SOP	Instructions for complying with SSP.	Procedure: how to update virus signature files.

The Documentation Process

Need for new documents

213. New documents may be required for many reasons, including to:

- meet the documentation requirements for accrediting a new system,
- remove repetition from system-specific documents into a higher level document,
- address gaps in existing policy,
- develop new policy for new technologies or business requirements, and
- develop new SOPs in response to identified training requirements.

See: 'Requirements for IT Security Documentation' on page 2-12.

Develop the content

214. DSD **RECOMMENDS** that IT security documentation be developed by people with a good understanding of both the subject matter and the agency's business.

When documentation development is outsourced, agencies **SHOULD**:

a. review the documents for suitability,
b. retain control over the content, and
c. ensure that all policy requirements are met.

Depending on the agency's documentation framework, some new documentation requirements may be met by referencing or modifying existing documents.

Obtain formal signoff

215. All IT security documents **SHOULD** be formally approved and signed off by an appropriate person.

DSD **RECOMMENDS** that:

a. all high level IT security documents be approved by the security executive, senior executive manager or agency head, and
b. all system-specific documents be approved by the owner of the system, the senior executive manager, and/or the security executive.

Note: The roles of the agency head, senior executive manager, and security executive are defined in the *PSM*.

Continued on next page

Documentation maintenance

216. Agencies **SHOULD** develop a schedule for reviewing all IT security documents at regular intervals.

DSD **RECOMMENDS** that:

a. the interval between reviews be no greater than twelve months,
b. reviews be performed in response to significant changes in the environment, business or system, and
c. the date of the most recent review be recorded on each document.

Classifying IT Security Documents

Purpose

217. IT security documentation frequently contains information that could significantly increase the risk to the systems to which it relates, if someone with malicious intent accesses the information.

Agencies **MUST** classify their IT security documentation in accordance with Part C of the *PSM*.

General guidance

218. DSD **RECOMMENDS** that agencies, by default, classify system documentation at the same level as that of the system itself. However, an analysis of the applicable risks may determine a higher or lower classification is appropriate.

Examples: The following are two examples of when it may be appropriate to classify documents at a level other than the classification of the system to which they refer.

- Server configuration information for a web server hosting an agency's public website may be classified as SECURITY-IN-CONFIDENCE.
- A cabling diagram for a SECRET system may be classified as RESTRICTED.

Document classification

219. Agencies **SHOULD** apply the following classifications, as a minimum, to IT security documentation.

Exception: Agencies **SHOULD** classify security documentation that contains specific security configuration details at the level of the system to which it refers.

System classification	Documentation classification
• PUBLIC DOMAIN, • UNCLASSIFIED, • IN-CONFIDENCE, • PROTECTED	SECURITY-IN-CONFIDENCE
RESTRICTED	• SECURITY-IN-CONFIDENCE or • RESTRICTED

Templates

References

220.1. The table below provides references for templates that may assist agencies with the development of their security documentation.

Note: A reference for a template for SOPs has not been provided.

Type	Publication Title	Available from …	Notes
IT Security Policy (ITSP)	*AS/NZS 7799.2:2003 Information Security Management - Part 2*	Standards Australia **URL:** www.standards.com.au	Section 3 of Annex A contains the basis of an Information Security Policy which is slightly broader than an Information Technology Security Policy.
Risk Management Plan (RMP)	*HB 231:2004 Information Security Risk Management Guidelines*	Standards Australia **URL:** www.standards.com.au	Section 5 discusses documentation. **Note:** This document is based on *AS/NZS 4360:1999 Risk Management* which is also available from Standards Australia.
System Security Plan (SSP)	*NIST 800-18 Guide for Developing Security Plans for Information Technology Systems*	National Institute of Standards and Technology (US) **URL:** http://csrc.nist.gov/publications/nistpubs/index.html#sp800-18	This document is around 80 pages, however, Appendix C contains a template that could be used in isolation from the rest of the document. **Note:** This is a US document and it contains references to US agencies, legislation and policies.

Chapter 3 - Identifying and Developing IT Security Policies

Overview

Introduction

301. This chapter contains information about ITSPs.

ITSPs may also be known as Information System Security Policies (ISSPs).

Template

301.1 **See:** 'Templates' on page 2-18.

Contents

302. This chapter contains the following topics:

About ITSPs

Definition: ITSP

303. An Information Technology Security Policy is a high-level document that describes how an agency protects its IT resources. It allows management to provide direction and show commitment to IT security.

An ITSP is normally developed to cover all agency IT systems. It may exist as a single document or as a set of related documents.

See: 'Requirements for IT Security Documentation' on page 2-12.

ITSP contents

304. An ITSP should describe the IT security policies, standards and responsibilities of an agency, and set any specific minimum requirements, which will then feed into the development of RMPs.

National ITSP documents

305. The key national government ITSP documents to be considered when developing agency policy documents are the:

- *PSM*, and
- *ACSI 33*.

Inconsistencies between policies

306. Agencies **SHOULD** contact DSD if any apparent inconsistencies between the national ITSP documents require clarification.

Developing an ITSP

Process

307. The table below describes the process an ITSA follows to develop an ITSP for an agency.

Further details are supplied in the following paragraphs.

Stage	Description
1	Gain management support for the development of an ITSP.
2	Determine the overall scope, objectives and structure of the ITSP.
3	Identify all existing applicable policies and standards and record them in the ITSP.
4	Compare the identified objectives with the existing policies and standards to identify policy gaps.
5	Write policy statements to address each gap, and record them in the ITSP.
6	Identify general and specific responsibilities for IT security management.
7	Gain management approval and signoff.
8	Publish and communicate the ITSP to agency staff.

Identifying existing policies and standards

308. Existing applicable policies and standards may include, but are not limited, to any or all of the following:

- PSM,
- ACSI 33,
- AS/NZS ISO/IEC 17799:2001,
- AS/NZS 7799.2:2003, and
- agency-specific policies.

Other applicable policies and standards are available from:

- ASIO T4 Protective Security Group,
- Commonwealth Law Enforcement Board,
- Information Security Group, DSD,
- National Archives of Australia,
- National Office for the Information Economy,
- The Office of the Federal Privacy Commissioner, and
- Attorney-General's Department.

Continued on next page

Policy questions

309. Policy may be structured to answer the following questions.

- What are the policy objectives?
- How will the policy objectives be achieved?
- What are the guidelines, legal framework and so on under which the policy will operate?
- Who are the stakeholders?
- What resourcing will be supplied to support the implementation of the policy?
- What performance measures will be established to ensure the policy is being implemented effectively?

Organising policy statements

310. Once the policy has been defined, the policy guidelines may be used to produce a more detailed policy framework. This framework may include:

- agency accreditation processes,
- responsibilities,
- configuration control
- access control,
- networking and connections with other systems,
- physical security and media control,
- emergency procedures and incident management,
- change management, and
- education and training.

Writing policy statements

311. Write appropriate policy statements, leaving the selection of controls to be addressed by the RMP, and implementation details to be addressed in SSPs and SOPs.

Example: Proposed changes to a system must go through a formal change control process prior to implementation.

Chapter 4 - Risk Management

Overview

Introduction

401. Risk management is a methodology for comprehensively and systematically managing risks in an organisation.

This chapter contains information about developing and using a RMP to manage risk affecting IT systems in compliance with the requirements of the ITSP.

IT security risk management

402. IT security risk management follows the same principles and procedures as general risk management but the threats and risks are specific to IT security.

Consistency with standards

403. The risk management process used in *ACSI 33* presents a risk assessment and treatment strategy that is consistent with the risk management guidelines in the:

- *PSM*, Part B - Guidelines on Managing Security Risk,
- Australian Standard AS/NZS 4360:1999 '*Risk Management*', and
- HB 231:2004 '*Information Security Risk Management Guidelines*'.

The material in this document does not duplicate these guidelines.

Development and maintenance

404. The System Manager is responsible for the development and maintenance of the RMP for that system.

Where higher level, multi-system or agency-wide RMPs are used, the ITSA is responsible for their development and maintenance.
See: 'Using higher level documents to avoid repetition' on page 2-13.

Outsourcing

405. An agency whose IT infrastructure is outsourced remains accountable for the security of the agency and its assets.

Template

406. **See:** 'Templates' on page 2-18.

Continued on next page

Contents

407. This chapter contains the following topics.

The Process of Developing a Risk Management Plan

Important

408. This topic contains practical assistance for developing an RMP. DSD **RECOMMENDS** it be used in conjunction with chapter 4 of HB 231:2004 '*Information Security Risk Management Guidelines*'.

Determining the scope

409. The scope of the RMP should be defined to meet a specific set of objectives, which may be strategic or operational in nature. An RMP may be developed for many reasons, including to:

- manage risks to a system,
- manage risks to a site,
- manage risks to a organisation,
- determine the impact of a proposed change, or
- focus on an identified high risk area.

See: 'Using higher level documents to avoid repetition' on page 2-13.

Appropriate level of detail

410. The level of detail provided in an RMP should be appropriate to the scope to be covered. In some cases, it may be sensible to omit some steps. Additional steps in accordance with chapter 4 of HB 231:2004 *'Information Security Risk Management Guidelines'* may be required for larger or more detailed plans, or where increased security requirements exist.

Process

411. The table below describes the process for developing an RMP.

Stage	Description
1	Establish the context of the RMP. **See:** 'Stage 1: Establishing the Context' on page 2-27.
2	Identify the risks for each asset. **See:** 'Stage 2: Identifying the Risks' on page 2-29.
3	Analyse the identified risks. **See:** 'Stage 3: Analysing the Risks' on page 2-30.
4	Assess and prioritise the risks. **See:** 'Stage 4: Assessing and Prioritising Risks' on page 2-33.
5	Determine appropriate controls for each risk. **See:** 'Stage 5: Developing a Risk Treatment Plan' on page 2-34.
6	Collate the information gathered in stages 1 - 5 to produce the RMP. **See: '**Producing an RMP' on page 2-26.

Continued on next page

Producing an RMP

412. Following a risk management process allows you to gather the information required to produce an RMP. This document comprises:

- an executive summary, derived from Stage 1,
- Risk Assessment (RA) documentation, derived from Stages 2, 3 and 4,
- a Risk Treatment Plan (RTP), derived from Stage 5, and
- risk worksheets, included as an annex.

Stage 1: Establishing the Context

Executive summary

413. The information documented as a result of completing this stage forms the executive summary for an RMP.

Further detail

414. See 'Establish the Context' in chapter 4 of HB 231:2004 '*Information Security Risk Management Guidelines'* for further detail regarding establishing the context.

Procedure

415. DSD **RECOMMENDS** that agencies follow the steps in the table below to establish the context for an RMP.

Step	Context	Answer these questions
1	Risk management	• Who is going to conduct the process? • What are the objectives of this risk management process? • What are the boundaries for this risk management process?
2	Strategic	• What are the strengths and weaknesses? • What are the priorities? • Who are the stakeholders? • What are the major threats and opportunities? • What are the external drivers?
3	Organisational	• What are the objectives of the IT system(s) concerned? • What are the internal drivers? • What is the key to the success of the IT system(s)? • Are there shared risks with other agencies? • What resources are available? • How does the IT system contribute to the agency's wider goals and priorities?
4	Evaluation criteria	• Are there legal requirements? • What are the financial, human resource, and/or operational implications? • What are the costs and benefits of actions? • What level of risk is acceptable?
5	Structure	• What are the assets involved? • How are the assets to be used? • What are the phases (time) or elements (structure) of any activities?

Continued on next page

Next stage

416. The next stage in the process of conducting an RMP is to perform an RA, starting by identifying the risks.

See: 'Stage 2: Identifying the Risks' on page 2-29.

Stage 2: Identifying the Risks

Prerequisite

417. Before commencing this stage, Stage 1 of the process of developing an RMP, 'Establishing the Context' needs to have been completed.

See: 'Stage 1: Establishing the Context' on page 2-27.

Further detail

418. See 'Risk Identification' in chapter 4 of HB 231:2004 '*Information Security Risk Management Guidelines*' for further detail regarding identifying risks.

Procedure

419. For each asset identified in step 5 of Stage 1: Establishing the Context, identify all possible risks and record on a separate worksheet for each risk:

- what the risk is,
- how it can occur, and
- the consequences of the risk occurring.

Next stage

420. The next stage in the process of conducting an RA is to analyse the risks.

See: 'Stage 3: Analysing the Risks' on page 2-30.

Stage 3: Analysing the Risks

Prerequisite

421. Before commencing this stage, Stage 2 of the process of developing an RMP, 'Identifying the Risks' needs to have been completed.

See: 'Stage 2: Identifying the Risks' on page 2-29.

Aim

422. The aim of analysing the risks is to:

- separate the acceptable risks from the unacceptable risks, and
- provide data for the evaluation and treatment of risks.

Further detail

423. See 'Risk Analysis' in chapter 4 of HB 231:2004 '*Information Security Risk Management Guidelines*' for further detail regarding analysing risks.

Procedure

424. Follow the steps in the table below for each risk worksheet created during Stage 2: Identifying the risks.

Note: Record these steps on the risk worksheet.

Additional information for each step is detailed in the following pages.

Step	Action
1	Determine the consequence of the risk.
2	Determine the likelihood of the risk and document the source of information or logical justification used to determine the likelihood. **Example:** Results of audit analysis.
3	Determine the overall level of risk using a risk matrix table.

Next stage

425. The next stage of the process for developing an RMP is 'Assessing and Prioritising Risks'.

See: 'Stage 4: Assessing and Prioritising Risks' on page 2-33.

Continued on next page

Consequence determination

426. The table below describes the consequence ratings used in the *PSM*. Agencies performing an RA may use this table, or develop their own agency-specific table.

If the consequences would…	Then an appropriate consequence rating is…
threaten the survival of not only the program but also the agency, possibly causing major problems for clients and for a large part of the Australian Public Service,	catastrophic.
threaten the survival or continued effective function of the program or project and require top level management or ministerial intervention,	major.
not threaten the program but would mean that the program could be subject to significant review or changed ways of operating,	moderate.
threaten the efficiency or effectiveness of some aspect of the program but would be dealt with internally,	minor.
be dealt with by routine operations,	insignificant.

Document Consequence Table

427. The Consequence Table applied in an RMP **SHOULD** be documented in the RMP.

Likelihood determination

428. The table below contains ratings that can be selected to show how likely it is that a risk will occur. Agencies performing an RA may use this table, or develop their own agency-specific table.

If a risk…	Then an appropriate likelihood rating is…
is expected to occur in most circumstances,	almost certain.
will probably occur in most circumstances,	likely.
might occur at some time and may be difficult to control due to some external influences,	possible.
could occur some time,	unlikely.
may occur only in exceptional circumstances,	rare.

Document Likelihood Table

429. The Likelihood Table applied in an RMP **SHOULD** be documented in the RMP.

Continued on next page

Risk matrix

430. A risk matrix uses the consequence and likelihood of a risk to determine an overall risk rating. Use the legend and risk matrix below to determine the risk level.

Legend

431. The table below identifies and explains the risk levels used in the matrix. Agencies performing an RA may use this table, or develop their own agency-specific table.

Level	Descriptor	Explanation
E	Extreme	Requires detailed research and management planning at an executive level.
H	High	Requires senior management attention.
M	Moderate	Can be managed by specific monitoring or response procedures.
L	Low	Can be managed through routine procedures.

Matrix

432. The matrix below, in conjunction with the legend, may be used to determine the risk level. Agencies performing an RA may use this matrix, or develop their own agency-specific matrix.

	Consequences				
Likelihood	**Cata-strophic**	**Major**	**Moderate**	**Minor**	**Insignifi-cant**
Almost certain	E	E	E	H	H
Likely	E	E	H	H	M
Possible	E	E	H	M	L
Unlikely	E	H	M	L	L
Rare	H	H	M	L	L

Documentation of risk matrix

433. The risk matrix and its associated legend **SHOULD** be documented in the RMP.

Stage 4: Assessing and Prioritising Risks

Prerequisite

434. Before commencing this stage, Stage 3 of the process of developing an RMP, 'Analysing the Risks', needs to have been completed.

See: 'Stage 3: Analysing the Risks' on page 2-30.

Aim

435. The aim of assessing and prioritising risks is to determine risk management priorities by comparing the level of risk against:

- predetermined standards,
- target risk levels, and/or
- other criteria.

Further detail

436. See 'Risk Evaluation' in chapter 4 of HB 231:2004 '*Information Security Risk Management Guidelines*' for further detail regarding assessing and prioritising risks.

Acceptable risks

437. The risks deemed acceptable will invariably differ amongst agencies and will generally be based on their corporate objectives.

Procedure

438. The table below describes the steps taken to assess and prioritise identified risks and create a risk register.

Step	Action
1	Document in a risk register the predetermined standards, target risk levels and/or other criteria that determine what is an acceptable or unacceptable risk.
2	Assess each worksheet against the criteria recorded in step 1 to determine whether the risk is acceptable or unacceptable. If the risk is **acceptable**, record the risk in the risk register as acceptable.
3	Use the criteria recorded in step 1 to prioritise the **unacceptable** risks and record them in the risk register.

Next stage

439. The next stage in the process of developing an RMP is to determine the appropriate controls.

See: 'Stage 5: Developing a Risk Treatment Plan' on page 2-34.

Stage 5: Developing a Risk Treatment Plan

Prerequisite

440. Before commencing this stage, Stage 4 of the process of developing an RMP, 'Assessing and Prioritising Risks', needs to have been completed.

See: 'Stage 4: Assessing and Prioritising Risks' on page 2-33.

Definition: Risk Treatment Plan

441. A Risk Treatment Plan (RTP) documents how risk treatment controls should be implemented.

A risk treatment control is a measure that is taken to minimise risks, by reducing the likelihood and/or the consequence of the risk occurring.

Aim

442. The aim of developing an RTP is to identify controls and implementation strategies that will reduce the residual risk for risks identified in the risk register as being unacceptable.

Further detail

443. See 'Risk Treatment' in chapter 4 of *HB 231:2004 'Information Security Risk Management Guidelines*' for further detail regarding determining appropriate controls and their implementation.

Procedure

444. The table below describes the steps taken to determine appropriate controls and develop an RTP.

Step	Action
1	Write the unacceptable identified risks from the risk register in priority order in a control register.
2	Record one or more appropriate controls for each risk on the risk worksheet.
3	Perform a cost/benefit analysis and write 'accept' or 'reject' against each control in the risk worksheet.
4	Calculate the residual risk rating taking into consideration the effect of the accepted control(s). **See:** 'Stage 3: Analysing the Risks' on page 2-30.
5	Assess the residual risk rating according to the criteria recorded on the risk register and update the risk register. **See:** 'Stage 4: Assessing and Prioritising Risks' on page 2-33.
6	Record the accepted controls in the control register. Develop the RTP by defining responsibilities, timetable and monitoring methods for the implementation of each accepted control.

Chapter 5 - Developing an SSP

Overview

Introduction

501. This chapter contains information about developing SSPs.

Template

502. **See:** ‘Templates’ on page 2-18.

Contents

503. This chapter contains the following topics.

About SSPs

Definition: System Security Plan

504. A System Security Plan (SSP) is a document that:

- is a means for implementing the ITSP and the outcomes of the RMP, and
- details the high-level security architecture and specific policies that are to be enforced:
  - within the system, and
  - for each interconnection.

Purpose

505. The purpose of an SSP is to indicate how all the relevant security requirements identified in the ITSP and RMP will be met in a given information systems context.

The SSP **MUST** provide the Accreditation Authority with sufficient information to assess the security of a computer system.
See: 'ITSP contents' on page 2-20.

Development and maintenance

506. The System Manager is responsible for the development and maintenance of the SSP for that system.

Where higher level, multi-system SSPs are used, the ITSA is responsible for their development and maintenance.
See: 'Using higher level documents to avoid repetition' on page 2-13.

Stakeholders

507. There may be many stakeholders involved in defining the SSP, including representatives from the:

- project, who must deliver the secure capability (including contractors),
- owners of the information to be handled by the system,
- users for whom the capability is being developed,
- management audit authority,
- information management planning areas,
- Accreditation Authority, and
- infrastructure management (building and/or communications infrastructure).

Developing an SSP

Procedure: developing an SSP

508. The System Manager follows the steps in the table below to develop an SSP.

Note: The contents of the SSP should be appropriate for the size and importance of the system. It may be appropriate to add or omit information.

Step	Action
1	Review the RMP, ITSP, and any higher level SSPs that may be relevant.
2	Develop the strategies required to implement the identified policies and controls. **Note:** Consult with stakeholders if necessary.
3	Record the strategies in the appropriate section of the SSP.
4	Obtain all necessary certifications and insert them in the appropriate section of the SSP.

Chapter 6 - Developing and Maintaining Security SOPs

Overview

Introduction

601. This chapter contains information about developing and using security-related SOPs.

Excluded material

602. This chapter contains information specifically about **Security** SOPs. Other IT system related SOPs are not covered in this chapter.

Example: The SOP for using Word Processing software is outside the scope of this chapter.

Template

603. **See:** 'Templates' on page 2-18.

Contents

604. This chapter contains the following topics.

Developing Security SOPs

Definition: SOPs

605. Security Standard Operating Procedures (SOPs) are instructions to all system users, administrators and managers on the procedures required to ensure the secure operation of a system.

SOP roles

606. Security SOPs **SHOULD** be developed for each of the following roles:

a. ITSA,
b. System Manager,
c. System Administrator and
d. System Users.

The ITSA, System Manager and System Administrator roles may have some overlap.

The ITSA and System Manager **SHOULD** be familiar with all SOPs.

Relationship between SSP and SOPs

607. The primary function of SOPs is to ensure the implementation of and compliance with the SSP.

See: 'Chapter 5 - Developing an SSP' on page 2-35.

Maintenance

608. The System Manager **SHOULD** ensure that SOPs are maintained and updated. This may be done as:

a. a response to changes to the system, and
   See: 'Managing Change' on page 2-61.
b. part of a regular review of documentation.
   See: 'Chapter 9 - Reviewing IT Security' on page 2-72.

Continued on next page

Procedure

609. The table below describes the procedure a System Manager follows to develop SOPs for a system.

Where higher level, multi-system SOPs are used, the ITSA is responsible for their development and maintenance.
See: 'Using higher level documents to avoid repetition' on page 2-13.

Step	Action
1	Locate the SSP.
2	Working with one strategy in the SSP at a time, allocate the responsibility for adhering to that rule to: • the ITSA, • the System Manager, • the System Administrator, and/or • System Users.
3	Write each rule or procedure in full in the appropriate section of the SOP.

SOP Contents

Introduction

610. Use the information in this topic as a checklist for the contents for the SOPs written for each role.

Depending on the size and structure of the agency, there may be some overlap or shifting of procedures between roles defined here.

ITSA SOPs

611. The table below describes the minimum procedures that **SHOULD** be documented in the ITSA's SOPs.

Topic	Procedures SHOULD be included for…
User education	instructing new users to comply with IT security requirements.
Audit logs	reviewing system audit trails and manual logs, particularly for privileged users.
System integrity audit	• reviewing user accounts, system parameters and access controls to ensure that the system is secure, • checking the integrity of system software, • testing access controls, and • inspecting equipment and cabling.
Data transfers	• managing the review of removable media containing data that is to be transferred offsite, and • managing the review of incoming media for viruses or unapproved software.
Asset musters	labelling, registering and mustering assets, including removable media.
Security incidents	reporting and managing security incidents.

Continued on next page

System Manager SOPs

612. The System Manager is responsible for the technical and operational effectiveness of the system.

The table below describes the minimum procedures that **SHOULD** be documented in the System Manager's SOPs.

Topic	Procedures that SHOULD be included
System maintenance and hardware destruction	• Managing the maintenance of system software and hardware. • Managing the destruction of unserviceable equipment and media.
User account management	Authorising new system users.
Configuration control	Approving and releasing changes to the system software or configuration.
Access control	Authorising access rights to applications and data.
System backup and recovery	Recovering from system failures.

System Administrator SOPs

613. The System Administrator is responsible for the day-to-day operation of the system.

The table below describes the minimum procedures that **SHOULD** be documented in the System Administrator's SOPs.

Topic	Procedures that SHOULD be included
System closedown	Securing the system out-of-hours.
Access control	Implementing access rights to applications and data.
User account management	• Adding and removing users. • Setting user privileges. • Cleaning up directories and files when a user departs or changes roles.
System backup and recovery	• Backing up data, including audit logs. • Securing backup tapes. • Recovering from system failures.

System Users

614. System Users **SHOULD** sign a statement that they have read and agree to abide by the System Users' SOP.

Continued on next page

System Users - background information

615. System Users' SOPs **SHOULD** contain:

a. an instruction on the security roles and responsibilities at the site, and
b. a warning that:
   1) users' actions may be audited, and
   2) users will be held accountable for their actions.

System Users - SOPs

616. The table below describes the **minimum** information that **SHOULD** be documented in the System Users' SOPs.

Topic	Information that SHOULD be included
Passwords	Guidelines on choosing and protecting passwords.
Need-to-know	Guidelines on enforcing need-to-know on the system.
Security incidents	What to do in the case of a suspected or actual security incident.
Security classification	The highest level of classified material that can be processed on the system.
Temporary absence	How to secure the workstation when temporarily absent.
End of day	How to secure the workstation at the end of the day.
Media control	Procedures for controlling and sanitising media, including requirements for the ITSA or delegate to vet all incoming and outgoing media.
Hardcopy	Procedures for labelling, handling and disposing of hardcopy.
Visitors	Preventing overview of data by visitors.
Maintenance	What to do for hardware and software maintenance.

Continued on next page

User guidance

617. Agencies **MUST** provide guidance to users on their responsibilities relating to IT security, and the consequences of non-compliance.

DSD **RECOMMENDS** that agency guidance to users include the following:

a. only access data, control information, and software to which they have authorised access and a need-to-know,
b. immediately report all security incidents and potential threats and vulnerabilities involving information systems to the ITSA,
c. protect their authenticators and report any compromise or suspected compromise of an authenticator to the appropriate ITSA,
d. ensure that system media and system output is properly classified, marked, controlled, stored, and sanitised,
e. protect terminals from unauthorised access,
f. inform the ITSA when access to a particular information system is no longer required, and
   Example: User completes a project, transfers, retires, or resigns.
g. observe rules and regulations governing the secure operation and authorised use of information systems.

Improper use of general access rights

618. Agencies **SHOULD** advise users not to attempt to:

a. introduce malicious code into any information system,
b. physically damage the system,
c. bypass, strain, or test security mechanisms,
   Exception: If security mechanisms must be bypassed for any reason, users **MUST** first receive approval from the ITSA.
d. introduce or use unauthorised software, firmware, or hardware on an information system,
e. assume the roles and privileges of others,
f. attempt to gain access to information for which they have no authorisation, or
g. relocate information system equipment without proper authorisation.

Chapter 7 - Certifying and Accrediting the Security of IT Systems

Overview

Introduction

701. This chapter contains information about certifying and accrediting the security of IT systems. Certification and accreditation provides management and data owners with an assurance that the information system has been secured in accordance with the SSP and other relevant documents.

Contents

702. This chapter contains the following sections:

Not included in this chapter

703. This chapter does **not** include the standards on which the certification and accreditation processes are based.

See: 'Part 3 - IT Security Standards' on page 3-1.

About Certification and Accreditation

Definition: certification

704. Certification is the assertion by an approved entity that compliance with a standard has been achieved, based on a comprehensive evaluation. It may involve:

- a formal and detailed documentation review,
- a physical review, and/or
- testing.

Certification is a prerequisite for accreditation. Accreditation Authorities **SHOULD NOT** accredit a system until all relevant certifications have been provided.

Continued on next page

What is certified?

705. The table below describes what may be certified and the certifying entity for areas related to IT security.

Note: The degree of assurance provided by a certification may vary depending on who performs the certification; self-certification of gateways and IT Systems by an agency ITSA is not the same as independent third-party certification by DSD or an I-RAP assessor. Policy for some interagency systems (e.g. Fedlink) may mandate independent certification.

Certification of…	Is undertaken by…
the physical security of sites,	• the Department of Foreign Affairs and Trade (DFAT) for systems located at overseas posts, • ASIO T4 for TOP SECRET systems, and • the ASA for all other systems. **See:** • 'Chapter 1 - Physical Security' on page 3-2 for physical security standards, and • 'Guidance on the physical protection of security classified information and other official resources' on page E35 of the *PSM*.
Gateways,	• DSD, • an I-RAP Assessor, or • the ITSA. **See:** 'Gateway Certification' on page 2-50 for more detail.
products approved for government use listed on the Evaluated Products List (EPL),	DSD. **See:** 'DSD Approved Products' on page 3-22 for more detail.
IT systems,	• DSD, • an I-RAP Assessor, or • the ITSA.
Comsec,	• the Comsec Custodian, or • the ITSA.

Continued on next page

Definition: accreditation

706. Accreditation is the formal acknowledgement of the Accreditation Authority's decision to approve the operation of a particular IT system:

- processing classified information,
- in a particular security environment, and
- using a particular set of controls.

Accreditation of a specific computer system is defined in terms of:

- a particular configuration,
- operation in a defined site,
- a particular range or type of data, and
- operation in a specific mode.

Accreditation Authority

707. The *PSM* states that "The accreditation is given by the owner of the system who, in doing so, accepts the residual risk, that is, the risk remaining after the protective measures are implemented." (*PSM* C7.29)

The Accreditation Authority is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

For…	The Accreditation Authority is…
Australian Government agencies,	the head of the agency or their authorised delegate.
organisations supporting Australian Government agencies,	the head of the supported agency or their authorised delegate.
multinational and multi-agency systems,	determined by the formal agreement between the parties.

Accreditation certificate

708. The Accreditation Authority may issue a certificate once accreditation has been achieved.

Requirement for accreditation

709. Agencies **SHOULD** ensure that systems are accredited before they are used operationally.

Continued on next page

RESTRICTED information on non-national security systems

710. Agencies with a system accredited for PROTECTED or HIGHLY PROTECTED information may choose to also accredit the system for RESTRICTED information. In this case, the system would be accredited for "[HIGHLY] PROTECTED and RESTRICTED".

Note: The requirements for CONFIDENTIAL and above include some measures that are not required for HIGHLY PROTECTED systems. A system designed to meet HIGHLY PROTECTED standards will not usually be suitable for accreditation to CONFIDENTIAL.

Accreditation is not transferable

711. Accreditation is not transferable, although the process may be simplified in cases where similar or identical systems are the subject of multiple accreditation requests.

Gateway Certification

Purpose of certification

712. Gateways, which provide secured connections between networks, perform an important role in the protection of agency systems.

The combination of high availability requirements and high threat environment frequently leads to a need for a high level of assurance that the gateway is securely managed.

Gateway certification is a process that aims to provide Australian Government agencies, or service providers to Australian Government agencies, with assurance that their gateway has:

- been configured and managed to industry best practice, and
- appropriate controls implemented and operating effectively.

This assurance will provide clients using the gateway services with a level of trust in the service provided.

Types of gateway certification

713. Gateways, as with all IT systems, may be certified by the agency ITSA, however the security status of an agency-certified gateway may not be accepted outside the scope of that agency.

Gateways may also receive an independent third-party certification by DSD or I-RAP that a gateway environment meets Australian Government best practice standards. This form of certification offers a higher level of assurance.

Agencies connecting to other agencies **SHOULD** ensure that the gateway has received DSD or I-RAP certification prior to establishing the connection.

Connections to certain interagency systems (e.g. Fedlink) may require independent certification from DSD or an I-RAP assessor as a prerequisite to system specific accreditation. Such requirements need to be obtained from the interagency system managers prior to determining the type of certification a gateway will undergo.

Continued on next page

Gateways eligible for certification

714. All gateways **SHOULD** undergo certification.

DSD **RECOMMENDS** that independent DSD or I-RAP assessors perform the gateway certifications for:

a. agencies developing gateways that:
   1) will connect to public networks, or
   2) will not connect to public networks, but where the level of risk warrants a certified gateway.
b. companies wishing to provide gateway services to the Government, and
c. companies who, via outsourcing contracts, are required to provide gateway services to their clients. In these cases:
   1) the agency contract controller becomes the customer for the gateway certification, and
   2) any problems with the certification or issue of the certification will be passed to the contract controller.
   Note: This type of certification does **not** enable an outsourcing partner to claim that they have a certified gateway when offering services to other agencies/clients, unless specific agreement has been obtained from the contract controller.

Note: Gateways to public networks, provided by commercial gateway service providers, will normally be certified by DSD. Commercial organisations wishing to provide such services should contact DSD to discuss the proposal and to confirm certification arrangements.

Continued on next page

Stages of the certification process

715. The table below describes the five stages of the gateway certification process.

Stage	Review the…	To verify…
1	ITSP,	that policies have been developed or identified by the agency to protect their information assets.
2	RMP,	• that the RMP is in accordance with the security requirements, and • the comprehensiveness and appropriateness of the identified controls. **See:** 'Chapter 4 - Risk Management' on page 2-23.
3	design documentation,	that the documents have been developed and meet the standards required. Design documents required for certification may include the: • Gateway Logical/Infrastructure Diagram, • Concept of Operations, • List of Mandatory Requirements, • Risk Based Requirements, and • List of Critical Configurations.
4	SSP and SOPs,	that they meet the required standards and include: • security administrative tasks, • proactive security checking tasks, • proactive security auditing tasks, and • a contingency plan. **See:** • 'Chapter 5 - Developing an SSP', on page 2-35, and • 'Chapter 6 - Developing and Maintaining Security SOPs' on page 2-38.
5	current system configuration,	• the configuration checking of critical components, and • that the tools in use meet the requirements and are usable.

Continued on next page

What is looked for in a review?

716. As part of the review of the above documents, the reviewer will specifically look for:

- inconsistencies,
- indications that minimum standards have been met,
- mapping of the results of the RMP to the design and operation of the gateway, and
- realistic and achievable plans and procedures.

Provisional certification

717. Provisional Gateway Certification:

- can be awarded to:
  - agencies or companies whose gateway is lacking compliance in some non-critical aspect(s) of the design, policy or management, or
  - companies whose gateway is assessed as meeting the relevant requirements, but who have yet to connect any Government customers,
- is issued to indicate that full certification can be expected, subject to successful completion of a number of stated provisions, and
- does not preclude the gateway from operating, but does mandate that the provisions be corrected within a specified timeframe.

The timeframe for the completion of the provisions **SHOULD** be advised in a certification report. Failure to meet the provisions within the specified timeframe may result in certification being withdrawn.

Recertification

718. Recertification **SHOULD** be undertaken on all certified gateways at least every 12 months or at initiation of a major change. A major change can include:

- change of ownership,
- significant redesign of gateway architecture,
- significant change in access policy,
- significant upgrade of hardware or software,
- installation of additional services,
- change of service providers, and
- addition of clients.

Depending on the nature of the change, a change may be able to occur without recertification, but may require a review. The gateway certifier **SHOULD** review change management procedures as part of the certification process.

Note: Policy for some interagency systems (e.g. Fedlink) may mandate regular recertification.

Continued on next page

Minimum policy standards

719. The table below contains a summary of the **minimum** policy standards for Gateway certification.

Item	Policy MUST…
Access policy	be derived from the results of the RMP and the customer requirements, if any.
Security policy	have a clear link to the RMP to ensure the security policy objectives and associated countermeasures are appropriate to the level of identified risk.
Physical security of gateway premises	meet the standards detailed in 'Chapter 1 - Physical Security' on page 3-2.
Cryptography	be in accordance with the standards detailed in 'Cryptography' on page 3-77.
Contingency policy	have a clear link to the risk assessment to ensure the contingency policy objectives are appropriate to the level of identified risk.
Reporting of incidents to DSD	include DSD notification as soon as practicable of all Grade 3 and greater incidents.
Storage of logs	require agencies to securely store logs off-site for no less than 12 months.

Comsec Certification

Definition: Comsec certification

720. Comsec certification:

- is a process undertaken in support of the accreditation process, and
- specifically targets the Comsec environment, including:
  - the overall cabling installation,
  - TEMPEST, and
  - keying material management issues.

Granting Comsec certification

721. Comsec certification **SHOULD** only be granted if/when all requirements, including those given under provisional Comsec certification, have been finalised and certified by the relevant authority.

Site/Floor cabling diagram

722. A site/floor cabling diagram or equivalent specifications **SHOULD** be provided for Comsec certification. The diagram **SHOULD**:

a. be updated on a regular basis as cabling/conduit configuration changes are made and approved, and
b. contain a "Current as at .....(date)" on each page to indicate the status of the document.

Accreditation Process

Prerequisites

724. Essential steps that need to be taken prior to accreditation include:

- an RMP,
- a clear definition of the controls that need to be put in place, and
- certification that these controls have been implemented correctly and are effective.

The selected controls **MUST** comply with all approved security documents.

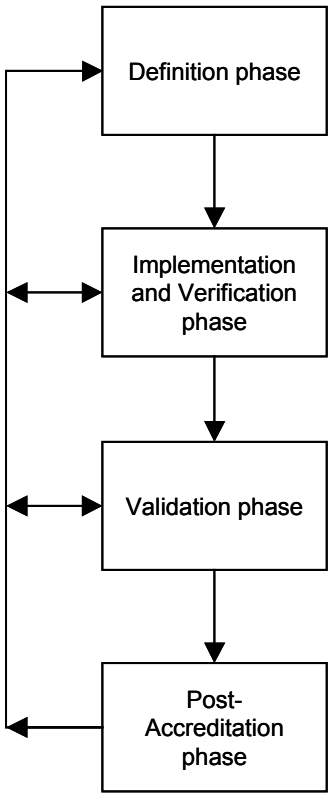
Clarification of policies and standards

725. From the start of the accreditation process, it is advisable to have ongoing discussions with the Accreditation Authority for clarification of, and guidance concerning, the accreditation policies and standards.

This liaison should also continue throughout the life of the accredited system.

The accreditation process

726. The diagram below shows the four phases of the accreditation process.



Continued on next page

Definition phase

727. During this phase, all relevant stakeholders work together to develop an SSP for the system for which accreditation will be sought.

Note: The need for a waiver is best identified and considered during this phase. Where a waiver is deemed necessary for an already existing system, a review of the accreditation of that system is initiated and the implications of the request assessed during this phase.

See: 'Chapter 5 - Developing an SSP', on page 2-35.

Implementation and verification phase

728. During this phase the SSP is implemented.

The quality assurance procedures to be applied during this phase are left to the discretion of the System Manager, who must maintain close contact with all stakeholders, particularly the Accreditation Authority representative.

Where technical or other issues related to implementing the SSP arise, the SSP will need to be reviewed as per the Definition phase.

Validation phase

729. During Validation, the implemented security is thoroughly tested and checked by Accreditation Authority staff to confirm that it is effective. Other security staff will be asked to confirm the physical and personnel security aspects of the implementation.

If discrepancies are revealed during this phase, the SSP and/or its implementation need to be revisited.

The result of the Validation phase is an accreditation decision.

Provisional accreditation

730. Provisional accreditation may be granted as an interim measure if one or more requirements for full accreditation have not been met.

The Accreditation Authority **SHOULD** ensure that:

a. the provisional accreditation has an expiry date,
b. a clear and realistic process to achieve all accreditation requirements has been developed and agreed to, and
c. the risk of operating without all required security measures in place is acceptable.

Continued on next page

Waivers

731. The Accreditation Authority **SHOULD** ensure that all mandatory requirements have either been met or waived prior to granting accreditation.

See: 'Waivers against "MUSTs" and "MUST NOTs"' on page 1-6.

Post-accreditation phase

732. The ITSA, in liaison with the System Manager/Administrator and users, promotes and maintains security in the operational environment. The key activities to be undertaken include:

- ongoing security awareness and training,
- change management, configuration control and asset management,
- audit trail monitoring and management,
- ongoing testing for vulnerabilities,
- user account management,
- security management of media, and
- incident handling.

The Accreditation Authority **SHOULD** conduct reviews of the security of the accredited systems. This may be:

- as a result of some specific incident,
- due to a change to the system that significantly impacts on the agreed and implemented security architecture and policy, or
- as part of a scheduled review of the system.

See: 'Chapter 8 - Maintaining IT Security and Managing Security ' on page 2-59.

Chapter 8 - Maintaining IT Security and Managing Security Incidents

Overview

Introduction

801. Maintaining IT security is an ongoing task. It involves putting into place mechanisms to protect information and system resources. The IT areas requiring security maintenance include:

- confidentiality - ensuring that information is not accessed by unauthorised persons,
- integrity - ensuring that information is not altered by unauthorised persons in a way that is not detectable by authorised users,
- availability - ensuring that information is accessible when required by authorised users,
- authentication - ensuring that users are the persons they claim to be, and
- access control - ensuring that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive.

Why maintain IT security?

802. Information Technology is continually changing. Methods used to breach IT security are also continually changing. Once IT security measures are in place, it is important to maintain them to continue protecting the data being processed.

This involves:

- keeping track of changing technology and security requirements in order to implement changes required to IT security,
- performing regular integrity checks,
- auditing security and implementing any changes required, and
- identifying breaches of security, responding to them and documenting lessons learnt for future reference.

Compliance with security policy

803. Effective security management also involves a regular review of compliance with the ITSP, RMP and SSP.

Staff who maintain security

804. It is imperative that the appropriate staff are:

- tasked with maintaining IT security, and
- given the necessary resources to successfully complete such tasks.

Continued on next page

Contents

805. This chapter contains the following sections.

Managing Change

Identifying the need for change

806. The need for change may be identified in various ways, including:

- users identifying problems or enhancements,
- vendors notifying of upgrades to software or hardware,
- advances in technology in general,
- implementing new systems that require changes to existing systems, and
- identifying new tasks requiring updates or new systems.

Principles of change management

807. Consider the impact of change on system security. Change may have a positive or negative impact on system security.

All changes **SHOULD** be:

a. appropriately approved,
b. documented in all associated system documentation, and
c. properly managed.

This policy applies equally to urgent changes. The change management process should define appropriate actions to be followed before and after urgent changes are implemented.

Change Process

Types of system changes

809. A proposed change to a system environment could involve:

- an upgrade to system hardware,
- an upgrade to system or application software,
- the addition of an extra terminal, or
- major changes to system access controls.

A change may be a one-off or something that occurs periodically.

Change process

810. The table below describes DSD's **RECOMMENDED** change process.

Stage	Who	Description
1	System User, System Manager or ITSA	Produce a written change request. **Note:** The change request should be in accordance with the requirements listed in the SSP and may require a formal change request form.
2		Submit the change request for approval. **Note:** All changes that may impact the security of the IT system must be submitted to the Accreditation Authority for approval before they can be implemented.
3		Document the changes to be implemented. **Note:** Up-to-date documentation must be maintained and detail the correct configuration of the hardware and its operation, and identify the significance of the security-related features.
4		Implement and test the approved changes.
5	System Manager, ITSA	Update the relevant security documentation, including the: • RMP, • SSP, and • SOPs.
6	System Manager, ITSA	Notify and educate users of the changes that have been implemented as close as possible to the time the change is applied.
7		Continually educate users in regards to IT changes. **Example:** Regular security bulletins via electronic mail.

Managing Security Incidents

Procedures

811. Maintaining security includes having procedures for managing security incidents, including:

- detecting potential security breaches,
- identifying and responding to breaches in security, and
- documenting breaches for future reference.

Documentation

812. Security incident responsibilities and procedures **MUST** be detailed in the SSP and in SOPs.

See:

- 'Chapter 5 - Developing an SSP' on page 2-35.
- 'Chapter 6 - Developing and Maintaining Security SOPs' on page 2-38.

Detecting Security Incidents

What constitutes a breach of security?

813. The table below gives examples of types of security incidents and user activities that may result in a security breach.

Type of security incident	A person is in breach of security if they…
Unauthorised access	• attempt to access information and/or resources without: – obtaining the required authorisation, clearance or briefing, or – being able to justify their need for access, • extract information from the system and pass it to a person who: – does not have an established need-to-know, or – is not authorised to access that information, • attempt to circumvent the access mechanisms that have been applied to protect information and/or resources, • use another person's password and user id, including security tokens or smartcards, for **any** purpose, • permit another person to use their own user id and password for **any** purpose, or • attempt to deny functionality of the system to any other person without first being authorised to do so.
Modification of information	• attempt to corrupt information that may be of value to another person, • attempt to modify information and/or resources without authority, or • process information that is classified above the system's classification.

Continued on next page

Tools used

814. The table below describes the tools that may be used to detect a breach of security.

Tools	Description
Network and Host Intrusion Detection Systems	Monitor and analyse network and host activity, usually relying on a list of known attack signatures to recognise potential security incidents.
System Integrity Verification	Used to detect changes to critical system components, such as files, directories or services. These changes may alert an administrator to: • unauthorised changes that may signify an attack on the system, and • inadvertent system changes that render the system open to attack.
Log Analysis	Involves collecting and analysing audit logs using pattern recognition to detect anomalous activities. Used to monitor critical assets.
Intrusion Repulsion	Some intrusion detection systems are combined with functionality to repel detected attacks. Caution and assessment of the potential impact should be exercised if this capability is to be used.

Effectiveness of tools

815. Automated tools are only as good as the level of analysis that they perform. If tools are not configured to assess the areas of high risk in a system configuration, then it will not be evident when a weakness emerges.

If the software is not regularly updated to include knowledge of new vulnerabilities, the effectiveness of the tools will be reduced.

Implement-ation of tools

816. Implementation of intrusion detection tools should always flow from the goals laid out in the security policy or plan, which are derived from a risk management process.

It is difficult for a security administrator to keep pace with all current and potential threats to information systems. An appropriately configured and managed intrusion detection system will present a security administrator with more options to mitigate identified risks.

Continued on next page

Vulnerability analysis

817. An intrusion detection strategy should be complemented by a vulnerability analysis strategy. Vulnerability analysis is used to detect changes in the level of system vulnerabilities from an established security baseline.

Vulnerability analysis strategy

818. Agencies **SHOULD** implement a vulnerability analysis strategy combining the following three techniques of:

a. monitoring public domain information about new vulnerabilities in operating systems and application software.
b. running tools to assess vulnerabilities.
c. running manual checks against system configurations to ensure disallowed services are prevented, and
   Example: "Netstat" commands to check the status of open sessions against the configuration parameters.

A vulnerability analysis strategy also needs to identify when the analysis needs to occur.
Example: Vulnerability analysis strategy could occur as part of the change control process.

The timing of the analysis should be based on a risk assessment focusing on the areas of highest risk.

Managing Incidents

Guidelines

819. Agencies **SHOULD**:

a. encourage staff to report security incidents through the appropriate management channels as soon as possible after the incident is discovered,
b. encourage staff to note and report any observed or suspected security weaknesses in, or threats to, systems or services,
c. establish and follow procedures for reporting software malfunctions,
d. put mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored, and
e. deal with the violation of organisational security policies and procedures by employees through a formal disciplinary process.

Development of incident handling and response procedures

820. Agencies **SHOULD** develop and maintain procedures based on the guidelines to:

a. establish the cause of any security incident, whether accidental or deliberate,
b. detail the action to be taken to recover and minimise the exposure to a system compromise, and
c. document any recommendations on preventing a recurrence.

Recording incidents

821. Agencies **SHOULD** ensure that all security incidents are recorded in a register. The purpose of the register is to highlight the nature and frequency of the incidents and breaches so that corrective action may be taken.

By recording all IT security incidents and breaches, the register may then be used as a reference for future risk assessments.

The recorded information **SHOULD** include, at a minimum:

a. the date the incident was discovered,
b. the date the incident occurred,
c. a description of the incident, including the people and locations involved,
d. the action taken,
e. to whom the incident was reported, and
f. the file reference.

Continued on next page

Handling data spillages

822. Data spillage occurs when, by faulty labelling, incorrect transfer, system failure, or similar process, data actually or potentially becomes accessible to persons not cleared or briefed for access to it.

In all cases of spillage, agencies **SHOULD** assume that the information has or will be compromised.

Standard procedures for all personnel with access to the system or its products **SHOULD** include the requirement to notify the ITSA of:

a. any data spillage, or
b. access to any data classified above that for which they are authorised.

Agencies **SHOULD**:

a. treat any such incident as a compromise,
b. investigate the incident,
c. take all necessary steps to minimise the likelihood of a repetition, and
d. notify DSD via ISIDRAS.

Handling malicious code infection

823. The table below describes the steps to be taken when malicious code is detected.

Step	Action
1	Isolate the infected computer or network.
2	Scan all connected systems, and any media used within the past six months (or longer, if the need is indicated), for malicious code. **Result:** Infected systems and media are identified.
3	Isolate all infected systems and/or media to prevent reinfection.
4	Use current anti-virus software to remove the infection from the systems and/or media. If this fails, seek advice from the vendor.
5	Report the incident in accordance with the incident response plan. **See:** 'Incident Response Plan' on page 2-69.

Incident Response Plan

Developing the plan

824. Each agency **MUST** develop and document an Incident Response Plan which, as a minimum, details:

a. broad guidelines on what constitutes an incident,
b. the minimum level of training for users and system administrators,
c. the authority who is responsible for initiating investigations of an incident,
d. the steps necessary to ensure the integrity of information supporting a compromise,
e. the steps necessary to ensure that critical systems remain operational, and
f. how to formally report incidents.

Guidelines

825. It is critical that security incidents be addressed in a timely and thorough manner. Thorough consideration should be given to how best to deal with security incidents in the organisation.

The Incident Response Plan **SHOULD** contain:

a. clear definitions of the types of incidents that are likely to be encountered, and
b. a documented plan with the expected response to each incident type.

DSD **RECOMMENDS** that the definition of what constitutes an incident:

a. be based on the intrusion detection objectives of the organisation, and
b. include examples of how the incidents may be detected.

Training

826. The minimum level of training to be provided to users and system administrators **SHOULD** include:

a. how to detect possible system compromises, and
b. to whom a suspected event should be reported.

System administrators **SHOULD** be specifically instructed by ITSAs not to reconfigure or access any systems until:

a. management have authorised such changes, and
b. all events are recorded.

Continued on next page

Investigations of incidents

827. The following list describes the information that **SHOULD** be included in the Investigation of Incidents section of the Incident Response Plan:

a. The authority within the agency who is responsible for initiating a:
   1) formal (administrative) investigation, and
   2) police investigation of an incident.
b. The criteria by which the responsible authority would initiate a formal or police investigation of an incident.
c. References to other related agency policies.
   Example: Fraud Control Plan.
d. Which other agencies or authorities should be informed in the event of an investigation being undertaken.
e. The location of system contingency measures.

Allowing continued attacks

828. The authority may decide to allow an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence. Agencies considering this approach **SHOULD** seek legal advice.

Integrity of evidence

829. Although in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected.

Agencies **SHOULD**:

a. transfer a copy of raw audit trails onto media such as CD-ROM or DVD-ROM for secure archiving, as well as securing manual log records for retention, and
b. ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

Further information relating to the management of IT evidence is contained in *HB 171:2003 Guidelines for the Management of IT Evidence*.

ISIDRAS

830. The Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) has been established by DSD to collect information on security incidents that affect the security or functionality of Australian Government computer and communications systems.

Continued on next page

Reporting of incidents

831. Paragraph G6.23 of the *PSM* states that ASAs and ITSAs **MUST** report significant computer security incidents to DSD.

DSD may then be able to assist in the:

- analysis of the incident,
- identification of remedial measures to remove the exploited vulnerability,
- minimisation of the likelihood of compromise, and
- overall assessment of the organisation's system security safeguards.

Formal reporting of incidents **SHOULD** be undertaken using ISIDRAS. Further details, including reporting requirements, are located on the DSD website.
URL: http://www.dsd.gov.au/infosec/assistance_services/incident.html

Documentation

832. Agencies **MUST**:

a. develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering the:
   1) detection of any intrusions, incorporating:
      i) intrusion detection systems,
      ii) audit analysis
      iii) system integrity checking, and
      iv) vulnerability assessments.
   2) incident response, and
      See: 'Incident Response Plan' on page 2-69.
b. make their users aware of the agency's policies, plans and procedures in relation to intrusion detection and incident response.

Chapter 9 - Reviewing IT Security

Overview

Introduction

901. A security review:

- identifies any changes to the risks faced by the subject of the review,
- assesses the effectiveness of the existing countermeasures, and
- reports on any changes necessary to maintain the required level of security.

Note: A security review may be scoped to cover anything from a single system to an entire agency.

Contents

902. This chapter contains the following sections:

About IT Security Reviews

When to conduct a review

903. A review of IT security may be required:

- as a result of some specific incident,
- due to a change to a system or its environment that significantly impacts on the agreed and implemented security architecture and policy, or
- as part of a regular or scheduled review.

Reviews **SHOULD** be undertaken and documented for any systems used for the storage, handling or processing of security classified information.

How frequently to review

904. Agencies **MUST** review the security of their IT systems.

DSD **RECOMMENDS** that agencies review all aspects of IT security at least annually. In addition, some aspects may need to be reviewed more frequently. The table below covers some specific components in more detail.

Component	Review…
Security documentation	the following documents and update as necessary: • ITSP, • RMP, • SSP, and • SOP.
Operating environment	when: • an identified threat emerges or changes, • an agency gains or loses a function, or • the operation of functions is moved to a new physical environment.
Procedures	after an incident or test exercise.
System security	items that may have an effect on the security of the system on a regular basis.
Waivers	prior to the identified expiry date. **See:** 'Waivers' on page 2-58.

Who can perform a review?

905. IT Security reviews may be performed by internal staff, or by independent third parties such as:

- an I-RAP assessor, or
- DSD.

Continued on next page

Audits after reviews

906. DSD **RECOMMENDS** that agencies undertake audits to ensure that agreed security measures identified during security reviews have been implemented and are working effectively.

Process for Reviewing IT Security

Basis of a review

907. Security reviews **SHOULD** be based on information that is:

a. comprehensive,
b. current, and
c. reliable**.**

Elements of a review

908. In security risk management, the structure under review can be broken down into a set of elements.

Examples:
a. A whole-of-agency review might best be approached by a review of each program.
b. A review of one particular program could be approached at the division or branch level.
c. A review of a particular building or installation could be approached by reviewing different groups or types of users separately.

Gathering information for a review

909. As part of the review, DSD **RECOMMENDS** that the ITSA gather relevant information from a range of sources. These may include:

- the police,
- DSD,
- ITSAs of other similar or related agencies, and
- system administrators and users.

Rigour of a review

910. DSD **RECOMMENDS** that the rigour of a review be commensurate with the risk environment and the highest level of security classified information that is involved.

Process

911. An IT Security Review follows the core IT Security Process with reference to the existing documentation.

See: 'The High-Level Process of IT Security' on page 2-8.

This page is intentionally blank.

Part 3
IT Security Standards

Overview

Introduction

This part contains IT security standards, principles and advice relating to specific aspects of IT systems, such as hardware, software and access control.

Contents

This part contains the following chapters:

Chapter 1 - Physical Security

Overview

Introduction

101. Table 7.62 in Part E of the *PSM* sets out the minimum standard of security container or secure room required for the handling and storage of security classified information within Australia. This table is directed towards the storage of hardcopy material, and is not directly applicable to IT systems.

The purpose of this chapter is to:

- define physical security standards for IT systems, including servers and workstations, and
- assist Agencies in developing an appropriate security environment for their IT systems that would meet the guidelines and established minimum standards of the *PSM*.

Physical security for Australian sites overseas

102. These standards are **only** applicable to sites located within Australia.

Agencies **MUST** consult DFAT for advice on the protection of classified information outside of Australia.

Contents

103. This chapter contains the following sections:

Continued on next page

Not included

104. This chapter does not contain information on the following topics:

Topic	See
Clearances and Briefings	‘Clearances and Briefings’ on page 3-19.
Media Security	‘Chapter 4 - Security of Hardware’ on page 3-29.
Logical Access Controls	‘Chapter 6 - Logical Access Control’ on page 3-58.
Comsec Standards	‘Chapter 8 - Communications Security (Comsec)’ on page 3-72.
Cabling	‘Cabling' on page 3-74.
Telephones	‘Telephones and Pagers’ on page 3-92.
Personal Electronic Devices (PEDs)	‘Portable Computers and Personal Electronic Devices’ on page 3-43.

Additional references

105. High-level information relating to area security is also contained in the:

- *PSM*, Part E - Physical Security, and
- *AS/NZS ISO/IEC 17799:2001*, 7 Physical and environmental security.

ASIO T4 Protective Security

Introduction

106. ASIO-T4 Protective Security (T4) provides the following services to the government on a cost-recovery basis:

- protective security advice,
- protective security risk reviews,
- security equipment testing,
- technical surveillance countermeasures, and
- physical security certification of sites.

Contact details

107. T4 can be contacted via:

- Phone: (02) 6234 1217
- Fax: (02) 6234 1218
- Email: t4ps@ozemail.com.au

T4 Protective Security
GPO Box 2176
Canberra ACT 2601

Contacting T4

108. T4 **RECOMMENDS** that agencies contact it for advice:

- if any of the measures in this chapter are not possible for site-specific reasons, and
- prior to the design and construction of a secure room/facility.

Security Construction and Equipment Committee

109. The Security Construction and Equipment Committee (SCEC) is a standing interdepartmental committee responsible for the evaluation and endorsement of security equipment for use by Australian Government departments and agencies. The SCEC is chaired by ASIO and reports directly to the Protective Security Policy Committee (PSPC).

Security Equipment Catalogue

110. The SCEC produces the *Security Equipment Catalogue (SEC)*, which lists equipment that has been tested and endorsed as meeting relevant SCEC standards.

Copies of the catalogue can be obtained from T4.

Fundamentals

Risk review

111. Dependent upon the risk environment in which an agency is operating, there may be circumstances in which there is a requirement for additional physical security measures that exceed these minimum standards.

In accordance with the requirements of Part B of the *PSM*, agencies **SHOULD** conduct a formal Threat Assessment and Risk Review process, incorporating the strategic and operational requirements of the facility to identify and assess the site-specific risks associated with its operation.

Once an agency has a clear picture of its risk environment, it can then determine whether the minimum measures address unacceptable risks, or whether additional measures will be required to provide an appropriate protective security environment.

The basics

112. The basics of the physical security for an IT facility consist of:

- a perimeter enclosing the entire user network,
- a more restrictive area separated from general user areas containing the servers and communications equipment, and
- the protection of the facility by appropriate physical security measures.

The measures applied to the server room are designed to limit access to those with the authorisation and requirement to enter and to detect those attempting to gain unauthorised access.

Protecting PUBLIC DOMAIN and UN-CLASSIFIED systems

113. The unintentional or unauthorised release of PUBLIC DOMAIN and UNCLASSIFIED information, by definition, should have little or no consequence. However, if equipment containing PUBLIC DOMAIN or UNCLASSIFIED information is stolen or damaged then a “Denial of Service” situation may arise while the equipment is being replaced or repaired. In some cases, the information contained on the equipment may be unique and therefore either irreplaceable or replaceable but only at great expense.

Agencies **SHOULD** implement measures to protect such equipment from theft and damage.

Removable Media

Definition: removable media

114. Removable media is storage media that can be easily removed from an IT system and is designed for removal.

Examples:

- Hard disks,
- DVDs,
- CDs,
- floppy disks,
- tapes,
- smartcards, and
- flashcards.

Storage authority

115. Removable media **MUST** be stored in accordance with the *PSM* requirements for the storage of hardcopy material.

Storage requirements

116. The table below is an extract from Table E7.62 of the *PSM*. It sets out the **minimum** standard of security container or secure room required for the storage of removable media containing classified information within Australia.
Note: The standard is determined by the classification of the media and the physical security standard of the area where the security container or room is located.

Classification	Secure	Partially Secure	Intruder Resistant
PROTECTED	C	C	B
• RESTRICTED • IN-CONFIDENCE	Agency discretion	Lockable commercial grade cabinet	Lockable commercial grade cabinet

Servers and Communication Equipment

Definition: Server

116.1 A server is a computer used to run programs that provide services to multiple users.

Examples:
- file server,
- mail server, and
- database server.

Separating servers and communication equipment from users

117. Spaces containing servers and communication equipment **MUST** be separated from general user areas by a clearly defined perimeter. This separation can be achieved by the use of either:

- a purpose-built server room, or
- appropriate cabinets or racks.

Access to the spaces **MUST** be limited to authorised staff.

No-Lone-Zones

118. DSD **RECOMMENDS** that areas containing sensitive materials and/or equipment be designated and operated as a No-Lone-Zone (NLZ) area.

A No-Lone-Zone area is an area in which people are not permitted to enter alone. The aim of this is to enforce "two person integrity".

Areas designated as an NLZ area **MUST**:

a. be suitably sign-posted, and
b. have all entry and exit points appropriately secured.

Equipment cabinets and racks

119. Where the perimeter is achieved by means of a cabinet or rack, the equipment **MUST** be secured in a SCEC endorsed cabinet or rack, in accordance with the *PSM* requirements for the storage for hardcopy material.

Determining the required class of rack

120. The required class of rack is determined by the classification of the system and the physical security standard of the area in which the cabinet or rack is located.

Continued on next page

Compartmentalisation

121. Compartmentalisation within a server room—due to cohabitation, multiple classifications, need-to-know, or other issues—can be achieved by means of cabinets and/or racks.

The equipment **MUST** be secured in a SCEC endorsed cabinet in accordance with the *PSM* requirements for the storage of hardcopy material.

Mass storage devices

122. Information stored on media that is not permanently fastened in equipment **MUST** be contained in a container or cabinet in accordance with the *PSM* requirements for the storage for hardcopy material.

Examples: Examples of media not permanently fastened in equipment are CD and DVD towers, backup tapes, and RAID arrays.

Securing media in server rooms

123. The fixed media **MUST** be secured in the equipment, which **MUST** be secured in a locked, commercial grade rack or cabinet in the server room.

Server Rooms

Standards

124. The following table sets out the minimum standard of server room required for the storage of equipment containing classified information within Australia.

Classification	Room standard
PROTECTED	SR1
• RESTRICTED • IN-CONFIDENCE	SR2
• UNCLASSIFIED • PUBLIC DOMAIN	**See:** 'Protecting PUBLIC DOMAIN and UNCLASSIFIED systems' on page 3-5.

SR1 and SR2 standards

125. T4 has developed guides detailing the physical security standards for Server Rooms (SR). Agencies may obtain these guides from T4.
Note: Comments and questions on the material in the guides should be directed to T4.

Administrative Measures

126. A Site Security Plan and Standard Operating Procedures (SOPs) **MUST** be developed for the room.

Subjects to be identified and covered include, but are not limited to:

- a summary of the protective security threat and risk assessment,
- roles and responsibilities of Facility or IT Security Officer, and individual staff,
- the administration, operation and maintenance of the Electronic Access Control System (EACS) and/or Security Alarm System (SAS),
- key management, the enrolment and culling of users and issuing of pin codes,
- staff clearances, security awareness training, and regular briefings,
- inspection of the generated audit trails and logs,
- end of day checks and lockup, and
- reporting of security incidents and breaches.

DSD **RECOMMENDS** that agencies contact T4 for advice on the content of these documents.

Workstations

Area type

127. Workstations and network infrastructure **MUST** be wholly contained within an area of the appropriate rating as shown in the table below.

Classification	Minimum area type
• PROTECTED • RESTRICTED • IN-CONFIDENCE • UNCLASSIFIED • PUBLIC DOMAIN	Intruder Resistant

Removable hard disks

128. If removable hard disks are utilised they **MUST** be:

- removed for after-hours storage, and
- stored in a container appropriate for the classification of the material on the hard disk.

Laptops

129. Even if hard disks have been encrypted with DSD approved cryptography, the laptops **SHOULD** be stored securely after-hours. The level of security required will depend on the particular product that is used but, at a minimum, they **SHOULD** be stored in a locked commercial grade cabinet.

Protecting against theft of workstation equipment

130. Agencies **SHOULD** implement measures to protect workstation equipment and internal components against theft.

Area Security Standards

Area security requirements

131. Part E of the *PSM* contains the requirements for the different types of area security.

Preventing observation by unauthorised people

132. Agencies **SHOULD** prevent unauthorised people from observing IT equipment, and in particular displays and keyboards.

DSD and T4 **RECOMMEND** that agencies:

a. position screens and keyboards so that they cannot be seen by unauthorised people, and/or
b. fix blinds or drapes to the inside of windows.

See:

- 'Curtains and Overlooking' in the *SEC*.
- 'Security Equipment Catalogue' on page 3-4.

Tamper Evident Seals

Approved seals

138. The SCEC endorses seals to be used for various sealing requirements.

Recording seal usage

139. Agencies **SHOULD** record the usage of seals in a register that is appropriately secured. The register **SHOULD** contain information on the:

a. issue and usage details of the seals and any associated tools,
b. serial numbers of all seals purchased,
c. the location or system each seal is used on.

Reviewing seal usage

141. Agencies **SHOULD** review the seals for differences with the register.

DSD **RECOMMENDS** that the review be done at least annually.

Purchasing seals

143. Where possible, agencies **SHOULD** purchase seals and/or associated tools with a unique identifier appropriate to the purchasing department.
Example: DFA for DFAT.

Agencies **SHOULD NOT** allow contractors to purchase seals and/or associated tools on behalf of the Australian Government.

Physical Security Incidents

Physical security incidents

144. Agencies **MUST:**

a. have policies, plans and procedures that address the management of physical security incidents, and
b. advise staff to report all physical security incidents, actual or suspected, to the ITSA and/or the ASA.

Incidents include, but are not limited to:

a. unauthorised access to equipment and cabling,
b. detection of any unauthorised equipment both covert and overt, and
c. failures in security mechanisms, which may have allowed unauthorised access.

Emergency Procedures

Emergency situations

146. DSD **RECOMMENDS** that agencies develop a set of policies, plans and procedures for when staff are required to evacuate a site which covers the:

a. securing of classified material and equipment, and
b. sanitisation, which may be achieved by destruction, of classified material and equipment.

Important: Health and safety must, at all times, be the first priority.

Chapter 2 - Personnel

Overview

Introduction

201. This chapter contains information on user education, personnel clearance and briefing requirements.

Contents

202. This chapter contains the following topics:

Not included

203. The following topics are not included in this chapter:

Topic	See
IT Security Roles and Responsibilities	'Chapter 1 - IT Security Roles and Responsibilities' on page 2-2.
Physical Security	'Chapter 1 - Physical Security' on page 3-2.
Access Control	'Chapter 6 - Logical Access Control' on page 3-58.

Additional references

204. Additional information relating to personnel training is also contained in the:

- *PSM*, Part D - Personnel Security, 4.1 - 4.3 Security Awareness,
- *AS/NZS ISO/IEC 17799:2001*
  - 6.1 Security in job definition and resourcing, and
  - 6.2 User training.

User Training and Awareness

Why have user education programs?

205. User training and awareness programs are designed to help users:

- become familiar with their roles and responsibilities,
- understand and support security requirements, and
- learn how to fulfil their security responsibilities.

See: 'Chapter 1 - IT Security Roles and Responsibilities' on page 2-2.

Training responsibility

206. Agency management is responsible for ensuring that an appropriate information system security training program is provided to staff.

Security education

207. Agencies **MUST**:

a. ensure that all personnel who have access to the agency's IT systems have sufficient training, and
b. provide ongoing IT security training and awareness for the staff on topics such as responsibilities, potential security risks and countermeasures.

Degree and content of security training

209. The exact degree and content of security training will depend on the security policy objectives of the organisation and **SHOULD** be aligned to user responsibilities.

DSD **RECOMMENDS** that the security training includes, at a minimum, information on:

a. the purpose of training or awareness program,
b. agency security appointments and contacts,
c. contacts in the event of a real or suspected security incident,
d. the legitimate use of system accounts,
e. configuration control,
f. access and control of system media,
g. the security of accounts, including sharing passwords,
h. authorisation requirements for applications, databases and data, and
i. the destruction and sanitisation of media and hardcopy output.

Continued on next page

Promoting user awareness

210. DSD **RECOMMENDS** that agencies promote user awareness of IT security. Some possible methods include:

- logon banners,
- system access forms, and
- departmental bulletins or memoranda.
  Example: The ITSA could distribute security bulletins via electronic mail to remind users of password responsibilities.

Training Resources

Training requirements and resources

211. The table below identifies potential topics and resources for training.

For…	DSD RECOMMENDS that training cover…	And possible training providers and resources are…
senior management,	• appreciation of computer security issues, and • security problems and solutions,	• the Attorney-General's Department, and • DSD-sponsored seminars for SES officers. **Note:** These can be tailored to meet specific requirements.
system administrators and security administrators,	• specialist training in implementing and monitoring systems, and • security features of the systems,	• formal in-house courses, • third party vendor programs, • security courses conducted by the Attorney-General's Department in collaboration with DSD, • self paced tuition manuals, and • user groups.
IT users,	• general and specific security requirements, • potential risks and countermeasures, and • system implementation,	• formal in-house courses, • customised training programs, and • external training organisations.
IT security trainers,	general and specific security information,	• security courses conducted by the Attorney-General's Department in collaboration with DSD, and • customised training programs.

Disclosure of information while on courses

212. Agencies **SHOULD** advise personnel attending courses along with non-agency personnel not to disclose any details that could be used to compromise agency security.

Clearances and Briefings

Policy

213. Agencies **MUST** specify the level of security clearance and any briefings required for each type of user in the SSP.

Note: The policy for granting and maintaining security clearances is set out in Part D of the *PSM*.

Clearances and briefings requirements

214. The SSP contains the requirements for clearances and briefings for:

- access/accounts granted to all staff, including contractors, and
- general, and privileged access.

Responsibilities

215. Agencies **MUST** ensure users have the appropriate clearance and need-to-know as determined by the *PSM* before they are permitted to access a system. **See:** *PSM* D2.4.

Agencies **SHOULD** ensure that user accounts are:

a. correctly maintained, and
b. disabled when the user ceases to have access rights to the system either because they have:
   1) left the agency, or
   2) changed to a new role within the agency which does not require access to the system.

Continued on next page

Definition: privileged access

216. Privileged access is defined as access which may give the user:

- the ability to change key system configurations,
- the ability to change control parameters,
  Examples: Routing tables, path priorities, addresses on routers, multiplexers, and other key system equipment.
- access to audit and security monitoring information,
- the ability to circumvent security measures,
- access to data, files and accounts used by other users, including backups and media, and
- special access for troubleshooting the information system.

Note: Users with privileged access are called privileged users.

Example: Users with "superuser", "root" or system administrator access are privileged users.

See: 'Chapter 1 - IT Security Roles and Responsibilities' on page 2-2.

Clearances for privileged users

217. DSD **RECOMMENDS** clearing privileged users to a level one classification above the classification of the system to which they have privileged access.
Example: A system administrator on a PROTECTED system could be cleared to HIGHLY PROTECTED.

If there are frequent transfers of data from a more highly classified system on to the system, then DSD **RECOMMENDS** that at least one system administrator on the lower system be cleared to the classification of the higher system.
Example: If a CONFIDENTIAL system frequently has CONFIDENTIAL data transferred to it from a SECRET system then one of the system administrators on the CONFIDENTIAL system could be cleared to SECRET.

Chapter 3 - IT Product Lifecycle

Overview

Introduction

301. This chapter contains information on selection, acquisition, installation, use and disposal of IT products.

Contents

302. This chapter contains the following topics:

DSD Approved Products

Definition: DSD Approved Product

303. A DSD Approved Product (DAP) is a product that:

- has been evaluated and certified within the Australasian Information Security Evaluation Program (AISEP),
  URL: http://www.dsd.gov.au/infosec/evaluation_services/aisep.html
- is being evaluated within the AISEP,
- has been evaluated and certified within a scheme with which Australia has a mutual recognition arrangement in place and the certification result has been formally recognised by DSD, or
- has been evaluated by some other DSD approved process, and has been certified and approved by DSD.

Definition: AISEP

304. The Australasian Information Security Evaluation Program (AISEP) exists to ensure that a range of evaluated IT products is available to meet the needs of Australian and New Zealand Government agencies.

The AISEP performs the following functions:

- evaluation and certification of IT products using the Common Criteria (CC) and Information Technology Security Evaluation Criteria (ITSEC),
- continued maintenance of the assurance of evaluated products, and
- recognition of products evaluated by a foreign scheme with which AISEP has an agreement.

Evaluation level mapping

305. The ITSEC and CC assurance levels are similar but not identical in their relationship. The table below shows the relationship between the two evaluation criteria.

ACSI 33 refers only to CC assurance levels. The table maps ITSEC levels to CC levels.

Common Criteria	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	-	E1	E2	E3	E4	E5	E6

Benefits of selecting a DAP

306. DAPs provide a level of assurance to agencies that the specified security functionality of the product will operate:

- as claimed by the developer in the Security Target (ST) or a similar document, and
- satisfies Australian Government policy requirements.

Continued on next page

Finding DAPs

307. DAPs are listed on DSD's Evaluated Products List (EPL).

The EPL is maintained by DSD and located on the DSD website on the Internet.
URL: http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html

Product Selection

Policy

308. Agencies **SHOULD** use a DAP when they are relying on the product to enforce security functionality for the protection of classified Australian Government information and systems.

However, agencies **MUST** use either a DAP or a product that correctly implements a DSD Approved Cryptographic Protocol if the product contains cryptography that is used to enforce security functionality for the protection of classified Australian Government information and systems.
See: DSD approval of cryptographic products on page 3-77

Order of preference

309. Agencies **SHOULD** select products that meet their needs in the following order of preference:

a. products that are listed on DSD's EPL and whose developer has made a commitment to the on-going maintenance of the assurance of the product,
   Note: These products will be indicated as such within the EPL.
b. products that are listed on DSD's EPL and have completed evaluation, and
c. products that are listed on DSD's EPL as being in evaluation.
   Important: Agencies must accept the risk that products listed as in-evaluation may not eventually complete evaluation.

Note: Products under these categories are considered to be DAPs.

However, if agencies cannot find an approved product that meets their needs, agencies **SHOULD** select products in the following order of preference:

a. products that have been evaluated by a foreign scheme with which the AISEP has a recognition agreement,
b. products that are in evaluation by a foreign scheme with which the AISEP has a recognition agreement, and
c. products that have had no formally recognised evaluation.

Note: Products under these categories are **not** considered to be DAPs.

Continued on next page

Options if selected product isn't on DSD's EPL

310. The table below identifies some options available to agencies that identify a suitable product that is not listed on DSD's EPL.

If the product…	DSD RECOMMENDS that the agency…
has completed evaluation through a foreign scheme with which DSD has a recognition agreement,	discuss with DSD the options for sponsoring the product for inclusion on DSD's EPL. **Note:** Before a product is listed on DSD's EPL, DSD will review it to ensure it is suitable for the protection of Australian Government classified information and systems.
is in evaluation within a foreign scheme with which DSD has a recognition agreement,	discuss with DSD the options for sponsoring the product for inclusion on DSD's EPL once the evaluation has been completed.
is not currently listed as being evaluated under any schemes or is being evaluated within a foreign scheme with which DSD does not have a recognition agreement,	contact the developer/vendor to discuss having the product evaluated within the AISEP or a scheme recognised by DSD.

Assessing the suitability of DAPs

311. In assessing a DAP for its suitability to meet the security objectives of the agency, the agency **SHOULD** review the product's Security Target (ST) and Certification Report (CR) or similar documents for the following:

a. its applicability to the intended environment,
b. that the version and configuration of the product matches that of the evaluated product,
c. that the required functionality was evaluated and certified,
d. that the level of assurance is adequate for its needs, and
e. for any constraints or caveats DSD may have placed on the product's implementation and use.

Note: Products that are in evaluation will not have a CR and may not have a published ST.

High Grade Equipment

311.1 Agencies intending to use High Grade Equipment **SHOULD** contact DSD.

Acquiring Products

Delivery of non-DAPs

312. DSD **RECOMMENDS** that agencies ensure that non-DAP products are delivered in a manner that provides confidence that they receive the product they expect to receive.

Delivery of DAPs

313. Agencies **SHOULD** ensure that DAPs are delivered in a manner that is consistent with the certified delivery procedures.

Note: For products evaluated under the CC at EAL2 or higher, or ITSEC, delivery information is available from the developer in the delivery procedures document.

Leasing arrangements

314. Agencies **SHOULD** ensure that leasing agreements for IT equipment take into consideration the:

a. difficulties that may be encountered when the equipment requires maintenance,
b. sanitisation of the equipment prior to its return, and
c. possible requirement for destruction of the equipment if sanitisation cannot be performed.

Installing and Using Products

Introduction

315. This section discusses the installation, configuration, administration and use of IT products.

Installing and configuring DAPs

316. Agencies **SHOULD** ensure that products are installed and configured in a manner consistent with the evaluated and/or approved configuration of the product.

Note: For products evaluated under the CC and ITSEC, this information is available from the developer in the installation, generation and start-up documentation. Further information is also available in the ST and CR.

Use of DAPs in unevaluated configurations

317. A DAP is outside of its evaluated configuration if:

- functionality is used that was not within the scope of the evaluation,
- functionality is used that was within the scope of evaluation but is not implemented in the specified manner,
- patches are applied to resolve "bugs", and/or
- the environment does not comply with assumptions and/or Organisational Security Policies (OSPs) stated in the product's ST or similar document.

Products that have a High Grade level of assurance **MUST NOT** be used in unevaluated configurations.

If an agency intends to use a DAP in an unevaluated configuration the agency **MUST** undertake a risk assessment. To be effective, the risk assessment **MUST,** at a minimum, be based on the following considerations:

a. the necessity of the functionality or patch,
b. the testing of the functionality or patch, and
c. the environment in which the product is to be used.

Operation of DAPs

318. Agencies **SHOULD** ensure that products are operated and administered in accordance with the user and administrator guidance.

Note: This guidance is generally available from the developer.

Disposing of Products

Secure disposal

319. Agencies **SHOULD** ensure that equipment and media are disposed of in a manner that does not compromise classified Australian Government information or capabilities.

High Grade Equipment

320. Agencies **MUST** contact DSD for advice on the disposal of High Grade Equipment.

Sanitising equipment and media

321. It is generally possible to sanitise equipment and media to a level acceptable for release however in some cases the destruction of the equipment may be justified.

See: 'Disposing of Hardware' on page 3-34.

Chapter 4 - Security of Hardware

Overview

Introduction

401. This chapter contains information on the handling, maintenance and disposal of hardware.

Definition: hardware

402. Hardware is a generic term for the physical components of computer equipment, including peripheral equipment.

Definition: media

403. Media is a generic term for the components of hardware that are used to store information. The information storage may be short or long term.

Media may be:

- fixed or removable, and
- volatile, which loses its information when power is removed, or non-volatile, which retains its information when power is removed.

Contents

404. This chapter contains the following sections:

Not included in this chapter

405. This chapter does **not** include information on the following topics:

Topic	See
Physical security and server rooms	‘Chapter 1 - Physical Security’ on page 3-2.
Cabling	‘Cabling’ on page 3-74.

Deleted block

406. <deleted>

Continued on next page

Additional references

407. Additional information relating to handling hardware is also contained in the:

- *PSM*, Part C - Information Security:
  - 6.69 Applying protective markings,
  - 6.87 Electronic storage media,
  - 7.53 Photocopiers, facsimile machines and electronic media,
  - 7.62 Removal of information on electronic media from agency premises,
  - 7.64 IT storage equipment and media,
  - 7.159 Electronic media and equipment, and
- *AS/NZS ISO/IEC 17799:2001*, 8.6 Media handling and security.

Definition: media reclassification

407.1. Reclassification is an administrative decision to **change** the classification of the media, based on an assessment of relevant issues including:

- the consequences of damage from unauthorised disclosure or misuse,
- the effectiveness of any sanitisation procedure used, and
- the intended destination of the media.

Definition: media declassification

407.2. Declassification is an administrative decision to **remove** all classifications from the media, based on an assessment of relevant issues including:

- the consequences of damage from disclosure or misuse,
- the effectiveness of any sanitisation procedure used, and
- the intended destination of the media.

Classifying hardware

407.3. Hardware containing media **MUST** be classified at or above the classification of the media until the media is either removed or declassified.

Classifying non-volatile media

408. Non-volatile media **MUST** be classified to the highest classification stored on the media since any previous reclassification.

Classifying volatile media with continuous power supply

410. Volatile media that has a continuous power supply **MUST** be classified to the highest classification stored on the media while the power is on.

Classifying volatile media [IC, R, P]

411. Volatile media that contains information classified IN-CONFIDENCE, RESTRICTED or PROTECTED may be treated as UNCLASSIFIED once the power is removed from the media.

Continued on next page

Labelling hardware and media

413. All classified media **MUST** be labelled with the appropriate classification in accordance with paragraphs C6.69-75 of the *PSM*.
Exception: Internally mounted media do not need a label. However, the hardware containing the media **MUST** be labelled instead.

DSD **RECOMMENDS** that, where possible, media be labelled so that the classification is visible when the media is mounted in the unit in which it is used **and** when it has been removed.

Registering media

414. All removable media **SHOULD** be registered with a unique identifier in an appropriate register.

Repairing and Maintaining Hardware

On-site repairs

417. Repairs and maintenance for hardware containing classified media **SHOULD** be carried out on-site by appropriately cleared and briefed personnel.

Using an uncleared technician

418. If hardware is to be repaired or maintained by a technician without an appropriate security clearance, the technician **MUST** be escorted by someone who:

a. is appropriately cleared and briefed, and
b. understands both the item(s) being repaired or maintained **and** the function the technician is undertaking.

Agencies **SHOULD** ensure that the ratio of supervising escorts to technicians allows for an appropriate oversight of all activities.

Off-site repairs [U, IC, R, P]

419. The table below describes options for off-site repairs to hardware.

Note: If the media contained within the hardware cannot be removed or declassified then the hardware **MUST** be escorted or repaired at a facility rated to at least the classification of the media.

DSD **RECOMMENDS** that agencies conceal the origin and nature of the system.

Hardware that is…	May be repaired off-site…
UNCLASSIFIED	at the agency's discretion provided due care is taken to protect official information.
IN-CONFIDENCE, RESTRICTED, or PROTECTED	by: • a repair company approved for that purpose by the agency, or • any other company if the hardware is escorted at all times by an appropriately cleared and briefed escort and due care is taken to ensure that official information is not compromised.

Disposing of Hardware

PSM reference: disposal

420.1. Paragraph C7.149 of the *PSM* states that "only information which is PUBLIC DOMAIN or has already undergone a SCEC-endorsed destruction process…should be discarded in the agency's general garbage."

Faulty media and hardware

421. Where the media cannot effectively be accessed due to faults in the hardware or the media itself, agencies **MUST**:

a. repair the equipment before sanitisation,
b. maintain the media at its highest classification, or
c. destroy the media.
See: 'Media Destruction' on page 3-41.

Continued on next page

Disposal Process

422. Agencies **MUST** have a documented process for the disposal of hardware.

The process **RECOMMENDED** by DSD is described in the table below.

Step	Action
1	Does the hardware contain any classified media? • If yes, then go to step 2. • If not, then go to step 7.
2	Determine whether the media should be either sanitised or destroyed, and the most appropriate method of doing so. Factors to be considered include: • Does an approved sanitisation procedure exist for the specific media involved? • What are the relative costs of sanitising versus destroying (and replacing where necessary) the media? • What is the classification and sensitivity of the data? • What level of control, if any, will the agency have over the hardware after disposal? • What is the acceptable level of risk associated with the recovery of data from the media?
3	Seek approval for the chosen sanitisation or destruction process from the ITSA. **Note:** For frequently used processes, this approval may be in the form of an authorised SOP.
4	Apply the agreed sanitisation or destruction process to the media.
5	Determine if the media has been satisfactorily sanitised or destroyed. • If yes, go to step 6. • If no, return to step 2.
6	Seek approval for declassification from the information owner. **Note:** For frequently used processes, this approval may be in the form of an authorised SOP.
7	Remove or obliterate all labels indicating the higher classification, codewords, caveats and owner.
8	Update any relevant documentation and registers.
9	Dispose of the hardware.

Media Sanitisation

Definition: media sanitisation

423. Media sanitisation is the process of erasing or overwriting data stored on media.

Note: The process of sanitisation **does not** automatically change the classification of the media, nor does sanitisation involve the destruction of the media.

Requirements for sanitising media

423.1. DSD **RECOMMENDS** that agencies sanitise all media prior to reuse in a new environment.

Agencies **MUST** use an approved method, as described within this Media Sanitisation section, whenever the media is moving **from**:

a. a higher classification **to** a lower classification, or
b. a CONFIDENTIAL or SECRET environment **to** a non-national security environment.

Where the new classification of the media will be equal to or higher than the previous classification, DSD **RECOMMENDS** that the media undergoes at least a basic form of sanitisation.

Examples: Basic forms of sanitisation include formatting magnetic media and clearing Erasable Programmable ROM.

Media that cannot be sanitised

424. The following media types **cannot** be sanitised and **MUST** be destroyed prior to disposal if they contain or may have contained classified information:

a. microfiche,
b. microfilm,
c. optical disks, including CDs and DVDs and all variations,
d. printer ribbons and the impact surface facing the platen,
e. Programmable Read-Only Memory (PROM), and
f. Read-Only Memory (ROM).

Continued on next page

Approved media sanitisation methods [IC, R, P]

425. The table below describes the approved methods for sanitising media classified as IN-CONFIDENCE, RESTRICTED and PROTECTED.

Media type	Sanitisation method
Magnetic media	Overwrite, or use a degausser of sufficient field strength for the coercivity level of the media to be sanitised. **See:** • 'Magnetic media sanitisation products' on page 3-38, and • 'Procedure: overwriting magnetic media' on page 3-39.
Erasable non-volatile semi-conductor memory. **Examples:** • Erasable Programmable ROM (EPROM), • Electrically Erasable PROM (EEPROM), • Flash cards, • Memory sticks.	Erase as per the manufacturer's specification **but** repeat the process three times.
Electrostatic memory devices within printers and photocopiers. **Examples:** • Laser printer cartridges, • Photocopier drums.	Print at least three pages of UNCLASSIFIED text on each colour cartridge within the device. **Note:** The text **SHOULD NOT** include any blank spaces or solid coloured areas and the print **SHOULD** cover the page.
Video screens	Visually inspect the screen by turning up the brightness to the maximum to determine that no classified information has been etched into the surface. If information is present, destroy the screen in accordance with OH&S standards.

Continued on next page

Approved media sanitisation methods
[IC, R, P] (continued)

Magnetic media sanitisation products

428. Agencies **SHOULD** use a DAP for the sanitisation of magnetic media.

See: 'DSD Approved Products' on page 3-22.

Continued on next page

Procedure: overwriting magnetic media

429. The table below describes the approved procedure for overwriting classified magnetic media.

Legend:

- ***X*** = a value determined from the table in 'Overwriting procedure: determining *X*' on page 3-40
- ***C*** = a character/bit pattern
- ***-C*** = the bit-wise complement/inverse of ***C***

Example: If ***C*** = 00101101 then ***-C*** = 11010010

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Determine the appropriate value of X using the table in 'Overwriting procedure: determining X' on page 3-40.

<table><tr><th>If X is…</th><th>Then…</th></tr><tr><td>a number</td><td>go to step 2.</td></tr><tr><td>'F'</td><td>format the media. End of procedure.
Important: Do not use a 'quick' format method.</td></tr></table></td></tr>
<tr><td>2</td><td>• Overwrite the entire media with C.
• Verify that all areas of the media have been overwritten with C.
• Overwrite the entire media with -C.
• Verify that all areas of the media have been overwritten with -C.

Important: If there are any errors, such as defective sectors, do not proceed with overwriting as it will be ineffective. In these cases the media SHOULD be destroyed.

If X equals '0' (zero), go to step 4, otherwise go to step 3.</td></tr>
<tr><td>3</td><td>• Overwrite the entire media with C.
• Overwrite the entire media with -C.

Repeat this step X times.</td></tr>
<tr><td>4</td><td>Overwrite the entire media with random data.</td></tr>
</table>

Continued on next page

Overwriting procedure: determining *X*

430. The value of ***X*** reflects the degree of rigour required when sanitising media in preparation for reclassification. Use the table below to determine the value of ***X*** to be used in the 'Procedure: overwriting magnetic media' on page 3-39.

Note: The value of ***X*** as shown below **does not** equal the total number of passes required. Using ***X*** in the overwriting procedure results in 3 + 2(***X***) passes in total.

		To			
		U	**IC**	**R**	**P**
From	**U**	F	F	F	F
	IC	0	F	F	F
	R	0	0	F	F
	P	1	0	0	F

Deleted block

432. <deleted>

Media Destruction

Definition: media destruction

434.1. Media destruction is the process of physically damaging the media with the objective of making the data stored on it inaccessible.

Requirement for media destruction

434.2. Agencies **MUST** destroy all **unsanitised** classified media prior to disposal using an approved method, as described within this Media Destruction section.

Reasons for not sanitising media include:

a. no approved sanitisation method exists,
b. a risk assessment identifies destruction as the preferred treatment,
c. the sanitisation method cannot be applied due to defective hardware, or
d. the cost of sanitising the media outweighs the benefits.

See: 'Disposal Process' on 3-35.

Media destruction equipment

434.3. DSD **RECOMMENDS** that agencies use the SEC as a guide for suitable equipment.

See: 'Security Equipment Catalogue' on 3-4.

Further advice

434.4. Agencies are encouraged to contact T4 for further information on the selection of protective security equipment used to destroy media.

See: 'Contact details' on 3-4.

Continued on next page

Approved media destruction methods [IC, R, P]

434.5. The table below describes the minimum approved methods for destruction of media classified IN-CONFIDENCE, RESTRICTED, and PROTECTED.

Media type	Destruction method
Volatile semi-conductor memory.	No destruction required once all power supplies, including batteries, are removed.
Non-volatile semi-conductor memory.	Smash.
Electrostatic memory devices within printers and photocopiers. **Examples:** • laser printer cartridges, • photocopier drums.	Not required.
Magnetic and optical media. **Examples:** • floppy disks, • hard disks, • tapes, • CDs.	Cut or smash

Portable Computers and Personal Electronic Devices

Introduction

435. This section contains information about security requirements for portable computers (e.g. laptops) and Personal Electronic Devices (PEDs).

Definition: PED

436. For the purposes of this document, PEDs are defined as portable devices that can store, process and/or transmit data electronically.

A PED is generally differentiated from a portable computer by its lack of comprehensive security features including user identification, authentication, and auditing.

Examples of PEDs

437. PEDs include, but are not limited to:

- Personal Digital Assistants (PDAs),
- mobile telephones,
- two-way pagers,
- digital cameras, and
- audio recorders.

Related topics

438. The table below describes the location of related information.

Topic	See
Telephones and pagers	'Telephones and Pagers' on page 3-92.
Physical security standards	'Chapter 1 - Physical Security' on page 3-2.
Cryptography	'Cryptography' on page 3-77.

Policy

439. In accordance with Part E of the *PSM*, portable computers and PEDs storing classified information **MUST** be protected in the same way as classified hardcopy material.

Operation and storage

440. Portable computers and PEDs containing classified information **SHOULD** be operated **only** in intruder resistant areas under continual, direct supervision, and stored in areas secured for that classification.

Portable computers and PEDs **SHOULD NOT** be operated in areas where the confidentiality and integrity of material cannot be assured.

Continued on next page

Configuration considerations

441. Agencies **SHOULD** configure portable computers and PEDs with:

a. encryption software, and
b. a lock that requires the user to authenticate before the system can be used.

See: 'Product Selection**'** on page 3-24 for information on selecting products.

Transit security

442. Portable computers and PEDs containing security classified information **MUST** be transported in accordance with the requirements for hardcopy material in the *PSM*.

See: *PSM* C7.68-7.104.

Labelling portable computers and PEDs

443. Agencies **MUST** put a classification label on all portable computers and PEDs.

Agencies **SHOULD** put a label warning against unauthorised use on all portable computers and PEDs.

An additional label **SHOULD** be affixed asking the finders of a lost portable computer or PED to hand the equipment in to any Australian police station or, if overseas, an Australian Embassy, Consulate or High Commission.

Emergency destruction

444. Agencies **SHOULD** develop an emergency destruction plan for any portable computer or PED used in high risk situations.

Chapter 5 - Security for Software

Overview

Introduction

501. This chapter contains information about handling malicious code and anti-virus software, using software applications and software development.

Types of software

502. Software includes:

- operating systems,
- data,
- programs and applications,
- utilities,
- email, and
- the Internet and web applications.

Contents

503. This chapter contains the following sections:

Not included in this chapter

504. This chapter does not include information on the following topics:

Topic	See
Physical Security	‘Chapter 1 - Physical Security’ on page 3-2.
Access Control	‘Chapter 6 - Logical Access Control’ on page 3-58.
Auditing	‘Intrusion Detection Systems’ on page 3-65.
Networks	‘Chapter 9 - Network Security’ on page 3-93.

Malicious Code and Anti-Virus Software

Introduction

505. This section contains information on protection against malicious code and the use of anti-virus software.

See: 'Recovering from Malicious Code Infections' on page 3-49 for information on handling a virus outbreak.

Definition: malicious code

506. Malicious code is any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include:

- logic bombs,
- trapdoors,
- Trojan programs,
- viruses, and
- worms.

Methods of infections or delivery

507. Malicious code can spread through a system from a number of sources including:

- files containing macro viruses or worms,
- email attachments and web downloads with malicious active content,
- executable code in the form of applications,
- security weaknesses in a system or network, and
- contact with an infected system or media.

Contents

508. This section contains the following topics.

Countermeasures Against Malicious Code

Management responsibility

509. Agencies **MUST**:

e. employ countermeasures to prevent the introduction of malicious code in the organisation, and
f. ensure that all instances of detected malicious code outbreaks are handled according to the appropriate procedures.

Recommended counter-measures

510. The table below outlines the protective countermeasures that DSD **RECOMMENDS** agencies implement for all information systems.

See: 'Minimum standards for malicious code control' on page 3-48 for implementation strategies.

Primary area of focus	RECOMMENDED countermeasures
Security awareness and user education	• Accept software and data from trusted sources only. • Educate and train all users in proper security techniques. **See:** 'User Training and Awareness' on page 3-16.
Anti-virus scanners	For all workstations, servers and gateways: • install an authorised anti-virus scanner, • regularly update virus signatures, and • regularly scan all disks.
Integrity checkers	Use checksums to detect unauthorised modifications. **Note:** DSD **RECOMMENDS** that the checksum database be held offline.
System isolation	• Progressively minimise connectivity according to the classification of the system. • Use gateways within the network to isolate sensitive internal systems. **See:** 'Gateways' on page 3-99.
Firewall	Install a firewall to restrict access by remote systems. **See:** 'Firewalls' on page 3-100.
Active content blocking	• Use filters to block unwanted content. • Use settings within the applications to disable unwanted functionality. • Use digital signatures to restrict active content to trusted sources only.
Access control mechanisms	Implement adequate access control mechanisms to prevent unauthorised user access. **See:** 'Chapter 6 - Logical Access Control' on page 3-58.

Continued on next page

Minimum standards for malicious code control

511. Agencies **MUST**:

a. develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering how to:
   1) minimise the likelihood of malicious software being introduced into the system(s),
   2) detect any malicious software installed on the system(s), and
   3) respond to any incidents resulting from malicious software.
b. make their users aware of the agency's policies, plans and procedures in part (a) above, and
c. deploy an anti-virus scanner, with regularly updated signatures.

Recovering from Malicious Code Infections

Requirements for containment and recovery

512. The capacity to contain and recover from malicious code is primarily reliant on the ability to:

- isolate infected systems,
- purge malicious code from a system,
- restore the integrity of a system, and
- recover data from backup media.

Handling malicious code infection

513. The procedure for handling a malicious code infection is located in 'Managing Incidents'.

See: 'Managing Incidents' on page 2-67.

Software Applications

Introduction

514. This section explains security requirements for software applications.

Software applications include:

- database applications,
- web servers and client browsers, and
- email servers and clients.

Software security policy

515. All application server and client security mechanisms **SHOULD:**

a. comply with the general standards outlined in this section, and
b. be documented in the SSP.

Security standards

516. The table below describes the **minimum** general standards for software security mechanisms.

Security component	Minimum standards
User identification and authentication	All users **MUST** be uniquely identified and authenticated before access is given to an agency's systems and applications. **See:** • *PSM* C7.33, and • 'Chapter 6 - Logical Access Control' on page 3-58.
Resource access control	All system resources **MUST** have an associated access control list. **See:** 'Chapter 6 - Logical Access Control' on page 3-58.
Audit logs and trails	The required events, based on an RMP, **MUST** be logged. **See:** 'Managing Audit Logs' on page 3-69.

Database Security

Data labelling

517. Agencies **SHOULD** label all database records with their classification and any other markings such as codewords, caveats and releasability indicators if the records:

a. may be exported to a different system, or
b. are of differing classifications and/or have different handling requirements.

Database files

519. The database's files **SHOULD** be protected from access that bypasses the database's normal access controls. This may be achieved by appropriate permission settings on directories and files at the operating system level.

Integrity

521. The database **SHOULD** maintain internal integrity when records are inserted, deleted or amended.

Availability

522. The database **SHOULD**:

a. have transaction rollback capability to recover from errors, and
b. be covered by adequate procedures for recovery from data loss or corruption.

Accountability

523. The database **SHOULD** provide accountability of users' actions.

See: 'Chapter 6 - Logical Access Control' on page 3-58.

Search engines

524. Users that do **not** have access to a document **SHOULD NOT** see the document title in a list of results from a search engine query.

Where users can see the titles of documents that they cannot access, the titles **SHOULD** be appropriately sanitised.

Web Application Security

Why have web security controls?

525. Web security controls are established to:

- protect the integrity of information submitted to, contained in, or retrieved from a website,
- protect the confidentiality of information on a need-to-know basis,
- ensure appropriate levels of user authentication, and
- protect the availability of the system from malicious code attacks.

Applying controls

526. Web security controls apply to all web applications that access HTML documents on web servers.

Example: Client browsers.

Components of a web application

527. The web application may include:

- a web server,
- a web browser,
- HTML or XML documents,
- active content (such as scripts or code),
- Uniform Resource Locator (URL), and
- cookies.

Anonymity and privacy problems

528. A browser provides information to every site it visits. Privacy and security problems arise because the web server may keep details of the:

- IP address that requested the page,
- URL accessed on the site,
- user's name or client browser's identity,
- amount of information transmitted to and from the site,
- status of the request,
- user's email address,
- operating system of the browser's host system, and
- the URL of the referring page.

The information provided may allow the external site a point of entry into the internal network.

Cookies

529. DSD **RECOMMENDS** agencies consider blocking inbound cookies, noting that such a decision may restrict the legitimate activity of the agency's users.

Continued on next page

Applications and plug-ins

530. Web browsers can be configured to allow the automatic launching of downloaded files. This may occur with or without the user's knowledge thus making the computer vulnerable to attack.

DSD **RECOMMENDS** agencies consider blocking the automatic launching of downloaded files, noting that such a decision may restrict the legitimate activity of the agency's users.

Client-side active content

531. Client-side active content is software that enhances the user's interactive functionality with the website. The software is automatically transferred from the web server to the user's computer when the user visits the website.
Examples: Java and ActiveX.

DSD **RECOMMENDS** agencies consider blocking client-side active content, noting that such a decision may restrict the legitimate activity of the agency's users.

Users

532. Agencies **SHOULD**:

a. ensure that users are informed of the dangers associated with using the Internet, and
b. keep user accounts for the operating system on the web servers to a minimum.

Website content

533. Agencies **SHOULD**:

a. establish formal procedures to manage the publication of material on the agency's website(s) and changes to existing content, and
b. review all active content on web servers for security issues.

Servers and clients

534. Agencies **SHOULD** harden and patch web servers and clients.

Note: A number of organisations publish hardening guides.

Auditing and access control

535. Agencies **SHOULD**:

a. configure auditing to produce logs and analyse the logs for any security issues, and
b. ensure that web servers available to the public are separated from the agency's internal systems.

Electronic Mail Security

Introduction

536. Electronic mail (email) security controls are established to:

- protect the confidentiality of information on a need-to-know basis,
- ensure an appropriate level of user authentication,
- ensure an appropriate level of email integrity, and
- protect the system from malicious code attacks.

Email usage policy

537. Agencies **MUST** have a policy governing the use of email.

Components of email system

538. The table below identifies the main components of an email system.

Component	Description
Mail server	A software tool that receives, routes or stores email messages from clients and other servers.
Mail client	A software tool run by the end-user to view messages and attachments.
Message	The content of the email, either in raw text, HTML or XML, including any attachments.
Attachment	Files included with the message. **See:** 'Malicious Code and Anti-Virus Software' on page 3-46.

Server auditing

539. Agencies **SHOULD** perform regular email server auditing to detect threats such as denial of service attacks and use of the server as a mail relay.

See: 'Audit Trail Events' on page 3-67.

Web-based email services

540. Agencies **SHOULD NOT** allow staff to send and receive email using web-based email services.

Continued on next page

Automatic forwarding of received emails

541. Agencies **SHOULD NOT** allow staff to automatically forward emails that may contain classified information to systems with a lower classification.

Example: The automatic forwarding of email to a web-based email system.

Agencies **SHOULD** warn staff that the automatic forwarding of email to another staff member may result in the new recipient seeing material that:

a. they do not have a need-to-know, or
b. the intended recipient and/or sender considered private.

Classification labelling

542. Agencies **SHOULD**:

a. label all agency originated email with the appropriate classification level, and
b. configure email gateways to verify that all outbound email carries a legitimate classification label.

Centralised email gateway

544. DSD **RECOMMENDS** that agencies route email through a centralised email gateway.

Minimum standards

545. Agencies **MUST**:

a. develop and maintain a set of email policies, plans and procedures, derived from a risk assessment, covering topics such as:
   1) integrity of the email's content,
   2) authentication of the source,
   3) non-repudiation of the source,
   4) verification of delivery,
   5) confidentiality of the email's content, and
   6) retention of logs and/or the email's content, and
b. make their users aware of the agency's email policies, plans and procedures.

Continued on next page

Guidelines

546. Agencies **SHOULD**:

a. harden and patch email servers and clients,
   Note: A number of organisations publish hardening guides.
b. restrict access to email servers to administrative users,
c. scan inbound and outbound email, including any attachments for:
   1) malicious code, and
   2) content in conflict with the agency's email policy,
d. configure auditing to produce logs and analyse the logs for any security issues,
e. ensure that email servers available to the public are separated from the agency's internal systems, and
f. disable mail relaying.

Software Development

Introduction

547. These requirements apply to all systems that require development, upgrade or maintenance for the operating system or application software.

Software development environments

548. The following apply to software development environments.

a. IT environments **SHOULD** contain the following three environments:
   1) development,
   2) testing, and
   3) production.
b. The three environments **SHOULD** be mutually inaccessible.
c. New development and modifications **SHOULD** only take place in the development environment.
d. Write-access to vendor's distribution media or integrity copies of operational software **SHOULD** be disabled.

Software testing

550. Software **SHOULD** be reviewed and/or tested for security vulnerabilities before it is used in a production environment.

Software **SHOULD** be reviewed and/or tested by an independent party, and **not** by the developer.

Additional references

551. Additional information relating to software development is also contained in the *AS/NZS ISO/IEC 17799:2001,* 10.5 Security in Development and Support Processes.

Chapter 6 - Logical Access Control

Overview

Introduction

601. This chapter contains information on logical access control.

Documentation

602. Agencies **MUST**:

a. develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering user:
   1) identification,
   2) authentication, and
   3) authorisation, and
b. make their users aware of the agency's policies, plans and procedures in part (a) above.

Contents

603. This chapter contains the following sections:

Not included

604. This chapter does not contain information on the following topics:

Topic	See
Physical access	'Chapter 1 - Physical Security' on page 3-2.
Clearances	'Chapter 2 - Personnel' on page 3-15.
Network security	'Chapter 9 - Network Security' on page 3-93.

Additional references

605. Additional information relating to access control is also contained in the:

- *PSM*, Part C - Information Security, 7.33 IT Logical access controls, and
- *AS/NZS ISO/IEC 17799:2001,* 9 Access Control.

User Identification and Authentication

User identification and authentication

606. All users of a system **MUST** be uniquely identifiable and **MUST** be authenticated before access is given to a system.
See: *PSM* C7.33.

Exception: Systems containing only PUBLIC DOMAIN or UNCLASSIFIED information are not required to identify and authenticate users.

User authentication can be done by one or more of the following:
- passwords,
- cryptographic tokens,
- smartcards, and
- biometrics.

DSD **RECOMMENDS** that agencies combine the use of multiple methods when identifying and authenticating users.

Password selection

607. Passwords **SHOULD**:

a. be a minimum of 7 characters, and
b. consist of at least 3 of the following character sets:
   1) lowercase characters (a-z),
   2) uppercase characters (A-Z),
   3) digits (0-9), and
   4) punctuation and special characters.
      Examples: !@#$%^&*

Password management

609. Agencies **SHOULD**:

a. require passwords to be changed at least every 90 days,
b. prevent users from changing their password more than once a day,
c. check passwords for poor choices, and
d. force the user to change an expired password on initial logon or if reset.

DSD **RECOMMENDS** that agencies require users to physically present themselves to the person who is resetting their password.

Reset passwords **SHOULD NOT** be predictable.
Examples: "password" or a user's SID should not be used.

Continued on next page

Screen and session locking

611. Agencies **SHOULD** configure systems with a screen and/or session lock.

The lock **SHOULD** be configured to activate after a predetermined period of user inactivity. This period **SHOULD** be no longer than 15 minutes.

The lock **SHOULD** blank the screen however the screen **SHOULD NOT** appear to be turned off.

The lock **MUST** require the user to reauthenticate before the system is unlocked.

If the locking mechanism has been configured, users **SHOULD NOT** be able to disable it.

Displaying when a user last logged in

613. DSD **RECOMMENDS** that agencies configure systems to display the date and time of the user's previous login during the login process.

Suspension of access

614. Agencies **SHOULD**:

a. suspend access after a specific number of unsuccessful logon attempts,
   Note: DSD **RECOMMENDS** that a limit of 3 attempts be allowed.
b. remove or suspend user accounts as soon as possible after the user leaves the agency, and
   Note: This is especially important for systems which can be accessed remotely.
c. suspend inactive accounts after an agency specified number of days.

Privileged and System Accounts

Use of privileged accounts

616. Agencies **SHOULD**:

a. ensure that the use of privileged accounts is controlled and accountable, **Example:** UNIX administrators login using their own userid and then 'su' to the privileged account.
b. ensure that administrators are assigned an individual account for the performance of their administration tasks,
c. keep privileged accounts to a minimum, and
d. **NOT** allow the use of privileged accounts for non-administrative work.

Default passwords in equipment and software

619. Agencies **SHOULD** replace default passwords, and delete or rename default accounts within system equipment and software.

Group accounts

621. DSD **RECOMMENDS** that agencies avoid the use of group and other non-user specific accounts.

Authorisation

Introduction

623. This topic discusses authorisation, including ACLs.

Guidelines

624. Agencies **SHOULD**:

a. limit user access on a need-to-know basis,
b. provide users with the least amount of privileges required for them to do their job, and
c. require any requests for access to a system to be authorised by the user's supervisor or manager.

Definition: access control list

625. An access control list (ACL) is a list of entities, together with their access rights, which are authorised to have access to a resource.

A collection of access control lists is sometimes referred to as an access control matrix.

Developing an ACL

626. The table below describes a process for developing an ACL.

Stage	Description
1	Establish groups of all system resources based on similar security objectives. **Examples:** Resources include files, directories, data, applications, and services.
2	Determine the data owner for each group of resources.
3	Establish groups encompassing all system users based on similar functions or security objectives.
4	Determine the group owner or manager for each group of users.
5	Determine the degree of access to the resource for each user group. **Examples:** Possible degrees of access are read, write, delete, and execute.
6	Decide on the degree of delegation for security administration, based on the internal security policy. **Example:** • Delegate group membership to identified group managers. • Delegate resource access control to identified data owners.

Continued on next page

Example of an access control matrix

627. The table below is an example of an access control matrix.

Note: The matrix associates identified user groups with specific system resources.

Legend: R=read; W=write; X=execute; N=no access; F=full access.

	Resources			
User Groups	**HRMS Application** Data owner = Personnel manager	**Payroll database** Data owner = Payroll manager	**Personnel drive** Data owner = Registry manager	**Forms database** Data owner = Registry manager
Personnel group Group manager = Personnel manager	WX	R	W	R
Payroll group Group manager = Payroll manager	RX	W	W	R
Registry group Group manager = Registry manager	N	N	R	R
Archives group Group manager = Personnel manager	N	N	F	F

Chapter 7 - Intrusion Detection and Incident Response

Overview

Introduction

701. This chapter discusses intrusion detection, audit analysis, system integrity checking and vulnerability assessments.

Contents

702. This chapter contains the following topics:

Intrusion Detection Systems

Introduction

703. An effective intrusion detection strategy includes the following:

- appropriate intrusion detection mechanisms,
- the analysis of audit logs,
- user training and awareness programs, and
  See: 'User Training and Awareness' on page 3-16.
- a documented incident response procedure.
  See: 'Managing Security Incidents' on page 2-63.

Additional references

704. Additional information relating to intrusion detection and audit analysis is also contained in the:

- *PSM*, Part C - Information Security, 7.35 IT System audit trails,
- *AS/NZS ISO/IEC 17799:2001,* 12.3 System audit consideration, and
- *HB 171:2003 Guidelines for the Management of IT Evidence.*

IDSs on Internet gateways

705. Agencies **SHOULD** deploy a network intrusion detection system (IDS), with regularly updated signatures, at any gateways between the agency's networks and the Internet.

IDSs on other gateways

706. DSD **RECOMMENDS** that agencies deploy a network IDS, with regularly updated signatures, at any gateways between the agency's networks and any networks not managed by the agency.

Audit Analysis

Audit requirements

707. Based on the overall audit objectives, audit requirements **MUST** include information on the:

a. audit log facility,
b. minimum audit events associated with a system or software component,
c. audit protection and archival requirements,
d. audit schedule, and
e. audit log management.

Audit trail facility

708. For each audit event, the audit log facility **MUST**, at a **minimum**, record the following information:

a. date and time of the event,
b. relevant user(s) or process where known,
c. type of event, and
d. success or failure of the event.

See: 'Audit Trail Events' on page 3-67.

DSD **RECOMMENDS** that agencies establish an accurate time source and use it consistently throughout the agency's IT systems to assist with the correlation of audit events across multiple systems.

Audit trail protection and archival

709. Audit logs **MUST** be:

a. protected from modification and unauthorised access,
b. archived using a well-documented procedure and retained for future access, and
   Note: DSD **RECOMMENDS** archiving audit trail data onto write-once media.
c. protected from whole or partial loss within the defined retention period.

Important: The retention of audit logs may be subject to the *Archives Act 1983*.

Responsibility for determining audit requirements

710. The System Manager and/or information owner, and **not** the ITSA, are responsible for determining the audit requirements of a system, consistent with the requirements of the ITSP and RMP.

Resources

711. Agencies **SHOULD** ensure that a sufficient number of appropriately trained personnel and tools are available to analyse all audit logs for security breaches or intrusions.

Audit Trail Events

Audit trails for software components

712. The types of events and information to be recorded **SHOULD** be based on a risk assessment.

The table below provides DSD's recommendations for specific software components.

If the software component is a(n)…	Then the RECOMMENDED events to audit include…
database	• user access to the database, • attempted user access that is denied, **Example:** Access denial due to incorrect password. • changes to user roles or database rights, • modifications to the data, and • modifications to the format of the database.
email system	all email sent to an external system. **Note:** If required, the email system should allow full audit of email content for a specific user or the entire system.
Multilevel network	• downgrade of classification of data, and • any attempt to release data to a system with a lower classification.
operating system	• successful and failed attempts to logon and logoff, • changes to system administration and user accounts, • failed attempts to access data and system resources, • attempts to use special privileges, • use of special privileges, • user or group management, • changes to the security policy, • service failures and restarts, • system startup and shutdown, and • changes to system configuration data. Additional events that **could** be recorded are: • access to sensitive data and processes, and • data export operations. **Examples:** email, ftp transfer, prints and floppy disk transfers.
web application	• user access to the web application, • attempted user access that is denied, • user access to the web documents, and • search engine queries initiated by users.

Other Logs

User logs

713. Retention of past and present user account information can be of significant value during an incident investigation. Therefore, agencies **SHOULD:**

a. maintain a secure log of all authorised users, their user identification and who provided the authorisation and when, and
   Note: In many cases this could be achieved by retaining the account application form filled in by the user and/or their supervisor.
b. maintain the log for the life of the system, after which the log **SHOULD** be archived in accordance with the *Archives Act 1983*.

System management logs

714. Agencies **SHOULD** record the following information in a manually updated system management log:

a. sanitisation activities,
b. system startup and shutdown,
c. component or system failures,
d. maintenance activities,
e. housekeeping activities,
   Examples: Backup and archival runs.
f. system recovery procedures, and
g. special or out-of-hour activities.
   See: 'Chapter 2 - Personnel' on page 3-15.

Managing Audit Logs

Responsibility for managing audit logs

716. In keeping with the principle of "Separation of duties", the people administering the system **SHOULD NOT** be the people who are auditing the system. The ITSA **SHOULD** be responsible for managing the audit logs.

How to manage an audit log

717. The table below describes the steps **RECOMMENDED** by DSD for the management of an audit log.

Step	Action
1	Collect relevant audit trail information from the operating system, networks or applications.
2	Collate the information.
3	Examine the audit information for events of interest based on the type of application.
4	Examine trends from past audits for correlations or patterns.
5	Transfer files to an appropriate location for archiving.
6	Inform appropriate System Managers of relevant security issues.

System Integrity

About system integrity

718. System integrity mechanisms aim to:

- minimise the likelihood of unauthorised tampering of information, and
- detect attempts or incidents of unauthorised tampering or access.
  See: 'Intrusion Detection Systems' on page 3-65 and 'Malicious Code and Anti-Virus Software' on page 3-46.

Additional references

719. Additional information relating to system integrity is also contained in the *PSM,* Part C - Information Security, 5.1 Integrity.

System integrity checks

720. Agencies **SHOULD** ensure that regular integrity checks are conducted on the agency's systems.

Agencies **SHOULD** use cryptographic hashes to verify critical files for unauthorised changes.
Examples: Critical files include operating system programs and system configuration files.
See: 'DSD Approved Cryptographic Algorithms' on page 3-79.

System changes

721. Agencies **SHOULD** ensure that:

a. only the system administrators can change system configurations,
b. changes to system configurations are managed and audited, and
   See: 'Managing Change' on page 2-61.
c. general users **do not** have access to privileged administrative utilities.

Vulnerability Assessments

Guidelines

722. Agencies **SHOULD**:

a. keep up-to-date with new security weaknesses in operating systems and application software,
b. use automated tools to assess systems for vulnerabilities, and
c. use security checklists for operating systems and common applications.

Authorisation

723. DSD **RECOMMENDS** that agencies require the authorisation of the System Manager before a vulnerability assessment is conducted on a system.

When to perform

724. DSD **RECOMMENDS** that agencies perform security vulnerability assessments:

a. before the system is first used,
b. after every significant change to the system, and
c. as required by the ITSA and/or System Manager.

Chapter 8 - Communications Security (Comsec)

Overview

Introduction

801. This chapter contains information about communications security (Comsec) standards.

Comsec certification

802. This chapter does **not** contain information about the Comsec certification process.

See: 'Chapter 7 - Certifying and Accrediting the Security of IT Systems' on page 2-45.

DSD advice

803. Contact DSD for further information regarding all Comsec issues.

Contents

804. This chapter contains the following topics:

About Comsec

Definition: Comsec

805. Comsec is the measures and controls taken to:

- deny unauthorised persons information derived from electronic communications, and
- ensure the authenticity of such communications.

Comsec includes:

- cryptosecurity,
- transmission security,
- personnel security,
- emanation security (including TEMPEST), and
- physical security.

Cabling

Cabling standards

807. Agencies **MUST** install all cabling in accordance with the relevant Australian Standards.

References:

- *Telecommunications Act (1997)*
- *AS/ACIF S009:2001 Installation Requirements for Customer Cabling (Wiring Rules).*

Cable Distribution Systems

Introduction

812. This topic discusses cable distribution systems. It contains information on:

- important definitions,
- types of conduit,
- standards for conduit penetrating walls,
- sealing conduit,
- suspending conduit, and
- connecting conduit to equipment cabinets.

What are cable distribution systems?

813. Cable distribution systems are used to distribute cabling around a facility in a controlled manner. DSD **RECOMMENDS** that agencies use separate cabling distribution systems for classified cabling.

Definition: conduit

814. Conduit is a tube, duct, or pipe used to protect cables from tampering, sabotage or accidental damage.

Cables sharing a common conduit

815. The table below shows the combinations of cable classifications that are approved by DSD to share a common conduit.

Agencies **MUST NOT** deviate from these approved combinations.

Group	Approved combination
1.	any combination of: • PUBLIC DOMAIN, • UNCLASSIFIED, • IN-CONFIDENCE, • PROTECTED, • HIGHLY PROTECTED, and • RESTRICTED.

Labelling and Registration

Installing conduit labelling

824. Conduits installed in public or visitor areas **SHOULD** be labelled in a manner that does not attract undue attention by people who may not have the appropriate security clearances or a need-to-know of the existence of such cabling.

SOPs

826. Site conventions for labelling and registration **SHOULD** be recorded in the SOPs.

Cable register

828. Agencies **SHOULD** maintain a register of cables. The register **SHOULD** record at least the following:

a. cable number ID,
b. type of cable,
c. source,
d. destination,
e. remarks, and
f. floor plan diagram.

Cable inspections

830. Agencies **SHOULD** inspect cables for inconsistencies with the cable register on a regular basis.

The frequency of the inspections **SHOULD** be defined in the SSP.

Cryptography

Purpose of cryptography

837. Cryptography can be used to provide:

- confidentiality,
- integrity,
- authentication, and
- non-repudiation.

DSD approval of cryptographic products

838. Paragraph C5.15 of the *PSM* states that "all measures using cryptography to protect Commonwealth information must be approved by DSD and must be implemented in accordance with DSD guidelines."

Requirements for storage encryption

839. The table below provides the **minimum** levels of assurance that are acceptable for the encryption of classified information whilst in storage.

Example: Hard disk encryption for laptops.

Classification	Minimum assurance requirements
• IN-CONFIDENCE, • RESTRICTED, or • PROTECTED	EAL2

Continued on next page

Requirements for transit encryption [IC, R, P]

840. The table below provides the **minimum** levels of assurance that **MUST** be used for the encryption of IN-CONFIDENCE, RESTRICTED and PROTECTED information whilst in transit over a network.

If the information is classified…	And the network it will be travelling over is…	Then the minimum assurance requirement is…
IN-CONFIDENCE,	• PUBLIC DOMAIN, or • UNCLASSIFIED,	a DSD approved cryptographic protocol.
RESTRICTED,	• PUBLIC DOMAIN, or • UNCLASSIFIED,	EAL2.
	• IN-CONFIDENCE, • PROTECTED, or • HIGHLY PROTECTED,	a DSD approved cryptographic protocol.
PROTECTED,	• PUBLIC DOMAIN, or • UNCLASSIFIED,	EAL2.
	IN-CONFIDENCE,	a DSD approved cryptographic protocol.

DSD Approved Cryptographic Algorithms

Introduction

843. This section explains the cryptographic algorithms that DSD has approved for the protection of non-national security classified information and RESTRICTED information. There are three types of algorithms:

- asymmetric/public key algorithms,
- hashing algorithms, and
- symmetric encryption algorithms.

Important: The fact that a product uses one or more of these algorithms does not automatically mean that the product is "DSD approved".

Asymmetric/ public key algorithms

844. The table below identifies the approved asymmetric/public key algorithms. For each algorithm it lists their approved uses, conditions of use and one or more references.

Algorithm	Approved uses	Conditions of use	Reference(s)
Diffie-Hellman (DH)	Agreeing on encryption session keys.	The modulus **MUST** be at least 1024 bits.	W. Diffie and M. E. Hellman, *New Directions in Cryptography,* IEEE Transactions on Information Theory, vIT-22, n.6, Nov 1976, 644-654.
Digital Signature Algorithm (DSA)	Digital signatures. **Note:** This is DSD's **RECOMMENDED** algorithm for this purpose.	The modulus **MUST** be at least 1024 bits.	FIPS 186.
Rivest-Shamir-Adleman (RSA)	• Digital signatures. • Passing encryption session keys or similar keys.	The modulus **MUST** be at least 1024 bits. **Note:** The public keys used for passing encryption session keys **MUST** be different to the keys used for digital signatures.	Public Key Cryptography Standards PKCS#1, RSA Laboratories.

Continued on next page

Hashing algorithms

845. The table below identifies the approved hashing algorithms, and one or more references for each of the algorithms.
Note: SHA-1 is the **RECOMMENDED** hashing algorithm.

Algorithm	Reference(s)
Message Digest v5 (MD5)	• AS 2805.13.3 • RFC 1321
Secure Hashing Algorithm (SHA-1)	• AS 2805.13.3 • FIPS 180

Symmetric encryption algorithms

846. The table below identifies the approved symmetric encryption algorithms, their conditions of use and one or more references.

These algorithms are approved for the encryption of information classified:

- IN-CONFIDENCE,
- PROTECTED,
- HIGHLY PROTECTED,
- CABINET-IN-CONFIDENCE with **no** national security information above RESTRICTED, and
- RESTRICTED.

Note: Symmetric encryption using AES or 3DES **SHOULD NOT** use Electronic Codebook (ECB) Mode.

Algorithm	Conditions of use	Reference(s)
Advanced Encryption Standard (AES)	AES supports key lengths of 128, 196 and 256 bits, all of which are suitable.	FIPS 197
Triple DES (3DES)	Triple DES **MUST** use either: • 2 distinct keys in the order key1, key2, key1, or • 3 distinct keys.	• AS 2805.5.4 • ANSI X9.52

DSD Approved Cryptographic Protocols

Approved protocols

847. DSD, in general, only approves the use of cryptographic products that have been formally evaluated. However, DSD approves of the use of some commonly available cryptographic protocols even though their implementations within specific products have **not** been formally evaluated by DSD. This approval is limited to cases where the system is used in accordance with DSD's published guidelines.

Using evaluated products

848. Before using unevaluated products that implement these protocols, agencies **MUST**:

a. consider the risks, and
b. investigate evaluated products, and systems such as Fedlink, that provide greater security assurance.

Agencies **MUST NOT** use these protocols to transmit or store on a network of a lower classification:

a. national security classified information classified CONFIDENTIAL, and above, or
b. CABINET-IN-CONFIDENCE information.

Links

849. The table below lists the approved protocols and provides links to the relevant guidelines.

Protocol	See page
Secure Sockets Layer and Transport Layer Security (SSL/TLS)	3-82
Secure Shell (SSH)	3-83

Secure Sockets Layer and Transport Layer Security (SSL/TLS)

Policy

850. DSD approves the use of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for encryption and authentication only when configured and implemented in accordance with the guidance provided in this topic.

Risk considerations

851. DSD has not formally evaluated the implementation of each cryptographic algorithm in any of the common web browsers and servers that implement SSL and/or TLS. There is a small possibility that one or more of these software products contain software bugs. This possibility should be taken into account when considering using SSL and/or TLS.

Important: These protocols do **not** protect data during storage. There is usually a greater risk that data will be accessed while stored at either end of the transaction link where SSL/TLS will not protect it.

Configuration guidelines

852. Agencies **SHOULD** configure SSL and TLS as follows:

a. only allow TLS and/or SSL version 3.0 sessions,
b. ensure the key exchange algorithm is RSA with a key length of at least 1024 bits, and
c. ensure that only DSD approved cryptographic algorithms are able to be used. **See:** DSD Approved Cryptographic Algorithms on page 3-79.

Secure Shell (SSH)

What is Secure Shell?

853. Secure Shell (SSH) can be used for:

- logging into a remote machine,
- executing commands on a remote machine, and
- transferring files.

Both commercial and open-source implementations of the SSH protocol are available.

SCP and SFTP

854. Secure Copy (SCP) and Secure FTP (SFTP) use SSH and are therefore also covered by these guidelines.

Configuration guidelines

855. The table below outlines the settings that **SHOULD** be implemented.

Note: The configuration directives are based on the OpenSSH implementation of SSH. Agencies implementing SSH may need to adapt these settings to suit other SSH implementations.

Configuration description	Configuration directive
Disallow the use of SSH version 1	Protocol 2
On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces	ListenAddress xxx.xxx.xxx.xxx
Disable connection forwarding	AllowTCPForwarding no
Disable gateway ports	Gatewayports no
Disable the ability to login directly as root	PermitRootLogin no
Disable host-based authentication	HostbasedAuthentication no
Disable rhosts-based authentication	RhostsAuthentication no IgnoreRhosts yes
Don't allow empty passwords	PermitEmptyPasswords no
Allow either password-based or public key-based authentication or both	PasswordAuthentication yes PubkeyAuthentication yes
Allow only the use of DSD approved cryptographic algorithms	**See:** DSD Approved Cryptographic Algorithms on page 3-79
Configure a suitable login banner	Banner /directory/filename
Configure a login authentication timeout of no more than 60 seconds	LoginGraceTime xx
Disable X forwarding	X11Forwarding no

Continued on next page

Passwordless logins

856. Some implementations of SSH allow logins without the use of a password. This capability can be used for automated processes such as backups.

Agencies that use passwordless logins **SHOULD** use the "forced command" option within the authorised_keys file to specify what command is executed upon logging in.

Ssh-agent

857. Agencies **SHOULD NOT** use "ssh-agent" or other similar key caching programs.

FIPS 140

What is FIPS 140?

858. The Federal Information Processing Standard (FIPS) 140 is a United States standard for the validation of cryptographic modules, both hardware and software.

FIPS 140, formally referred to as FIPS 140-2, is in its second iteration. For the purpose of this document, the standard is referred to as FIPS 140.

What FIPS 140 is not

859. FIPS 140 is **not** a substitute for the evaluation of IT security products under the Common Criteria. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other information security functionality.

For more information on FIPS 140

860. **See:** http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Policy for cryptographic evaluations at the EAL2 level

861. Vendors entering products into the Australasian Information Security Evaluation Program (AISEP) for evaluation at EAL2 may, at their discretion, choose to have the product's cryptographic functionality evaluated by DSD, or validated under FIPS 140.

If the cryptographic functionality is validated under FIPS 140 then DSD will review the validation report to confirm compliance with Australia's national cryptographic policy.

Note: This policy also applies to products evaluated to EAL2 overseas and submitted to the AISEP for Mutual Recognition.

Policy for cryptographic evaluations at all other levels

862. Cryptographic evaluations of products at higher evaluation assurance levels will normally be conducted by DSD. DSD may, at its discretion and in consultation with the vendor, reduce the scope of a DSD cryptographic evaluation of a product validated under FIPS 140.

If the cryptographic functionality is validated under FIPS 140 then DSD will review the validation report to confirm compliance with Australia's national cryptographic policy.

Note: This policy also applies to products evaluated overseas and submitted to the AISEP for Mutual Recognition.

Continued on next page

Approved algorithms

863. Some algorithms approved for use under FIPS 140 have not been evaluated and are not currently approved by DSD for the protection of classified information.

Modules that have been FIPS 140 validated, but do not include any DSD approved algorithms in the validation, will **not** be approved by DSD for the protection of classified information.

Key Management

Introduction

864. Key management covers the use and management of cryptographic keys and associated hardware and software in accordance with policy. It includes their:

- generation,
- registration,
- distribution,
- installation,
- usage,
- protection,
- storage,
- archival,
- recovery,
- deregistration,
- revocation, and
- destruction.

References

865. The table below provides additional references.

Grade of cryptography	Reference
commercial grade	*AS 11770.1-2003 Information technology – Security techniques – Key management.*

High Grade Cryptographic Equipment standards

866. Agencies **MUST** comply with *ACSI 53* and *ACSI 105(B)* when using High Grade Cryptographic Equipment (HGCE).

Agencies operating both HGCE and commercial grade cryptographic products may wish to use ACSI 53 for their commercial grade products also.

Definition: cryptographic system

867. A cryptographic system is a related set of hardware and/or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.

Definition: cryptographic system material

868. Cryptographic system material includes, but is not limited to, key, equipment, devices, documents, and firmware or software that embodies or describes cryptographic logic.

Continued on next page

Cryptographic system requirements

869. In general, the requirements specified for IT systems apply equally to cryptographic systems. Where the requirements for cryptographic systems are different, the variations are contained within this chapter, and overrule all requirements specified elsewhere within this document.

Cryptographic system administrator access

870. Cryptographic system administrator access is privileged access. Before an individual is granted cryptographic system administrator access, individuals at a minimum **SHOULD**:

a. have a demonstrated need for access,
b. read and agree to comply with the relevant KMP for the cryptographic system they are using,
c. possess a security clearance at least equal to the highest classification of information processed by the system,
d. agree to protect the authenticators for the system at the highest level of information it secures,
   Example: Passwords for a cryptographic system administrator account securing HIGHLY PROTECTED data.
e. agree not to share authenticators for the system without approval,
f. agree to be responsible for all actions under their accounts, and
g. agreed to report all potentially security-related problems to the ITSA.

Access register

871. DSD **RECOMMENDS** that agencies hold and maintain an access register that records cryptographic system information such as:

a. details of those with administrator access,
b. details of those whose administrator access was withdrawn,
c. details of system documents,
d. accounting procedures, and
e. audit procedures.

Accounting

872. Agencies **SHOULD** be able to readily account for all transactions relating to cryptographic system material including identifying hardware and software, and who has been issued with the equipment.

Continued on next page

Audits

873. Agencies **SHOULD** conduct audits of cryptographic system material:

a. on handover/takeover of administrative responsibility for the system,
b. on change of individuals with access to the cryptographic system, and
c. at least annually.

DSD **RECOMMENDS** that agencies perform audits:

a. to check all cryptographic system material as per the accounting documentation, and
b. to confirm that agreed security measures documented in the KMP are being followed.

DSD **RECOMMENDS** that these audits be conducted by two individuals with cryptographic system administrator access.

Area security and access control

874. Cryptographic system equipment **SHOULD** be stored in a room that meets the server room security level appropriate for the classification of data the system processes.
See: 'Chapter 1 - Physical Security**'** on page 3-2.

Areas in which cryptographic system material is in use **SHOULD** be separated from other classified and unclassified areas and designated as controlled areas.
Example: A locked cabinet containing the cryptographic system is within the server room, with the key held by a cryptographic system administrator.

Cryptographic system material remains in the custody of an individual who has been granted cryptographic system administrator access.

Key recovery

875. In July 1998, Cabinet directed that, where practical, encryption products must provide a means of key or data recovery to allow recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

Definition: Key Management Plan

876. A Key Management Plan (KMP) describes how cryptographic services are securely deployed within an agency. It documents critical key management controls to protect keys and associated material during their life cycle, along with other controls to provide confidentiality, integrity and availability of keys.

Requirement for KMP

877. Agencies **SHOULD** develop a KMP where they have implemented a cryptographic system in hardware or software.

Continued on next page

KMP contents

879. The table below describes the minimum contents which **SHOULD** be documented in the KMP.

Note: The level of detail included with the KMP must be consistent with the criticality and classification of the information to be protected.

Topic	Content
Objectives	Objectives of the cryptographic system and KMP, including organisational aims.
References	• Relevant ACSIs. • Vendor documentation. • Related policies.
Classification	Classification of the cryptographic system: • hardware, • software, and • documentation.
System Description	• Maximum classification of information protected. • The use of keys. • The environment. • Administrative responsibilities. • Key algorithm. • Key length. • Key lifetime.
Topology	Diagram(s) and description of the cryptographic system topology including data flows.
Key Management	• Who generates keys. • How keys are delivered. • How keys are received. • Key distribution, including local, remote, central. • How keys are installed. • How keys are transferred. • How keys are stored. • How keys are recovered. • How keys are revoked. • How keys are destroyed.

Continued on next page

KMP contents (continued)

Topic	Content
Accounting	• How accounting will be undertaken for the cryptographic system. • What records will be maintained. • How records will be audited.
Maintenance	• Maintaining the cryptographic system software and/or hardware. • Destroying equipment and media.
Security incidents	• A description of the conditions under which compromise of key material should be declared. • References to procedures to be followed when reporting and dealing with security incidents.

Telephones and Pagers

Use of telephones during classified conversations

880. Agencies **SHOULD NOT** allow telephones to be used in areas while classified conversations are being held.

Definition: Push-to-Talk telephone

881. Push-To-Talk (PTT) telephone handsets prevent the possibility of an idle handset inadvertently allowing classified discussions being undertaken in the vicinity of the handset to be passed over the telephone system.

Guideline for PTT

882. Agencies **SHOULD** install PTT telephone handsets on UNCLASSIFIED telephones that are within areas where classified conversations are held.

Cordless and mobile phones

885. Cordless and mobile phones **MUST NOT** be:

a. used for classified conversations unless the security they use has been approved by DSD,
b. connected to a classified telephone system, or
c. used in conjunction with a Speakeasy.

Chapter 9 - Network Security

Overview

Introduction

901. This chapter contains information on network security.

Contents

902. This chapter contains the following topics:

Additional references

903. Additional information relating to network security is also contained in the:

- *PSM*, Part C - Information Security:
  - 7.127 Local area networks,
  - 7.128 Wireless LANs,
  - 7.137 Minimum standards for the connection of agency networks to other networks,
  - 7.140 External data transmissions including email,
  - 7.142 Internal document exchange including email,
- *AS/NZS ISO/IEC 17799:2001*:
  - 8.5 Network Management, and
  - 9.4 Network access control.

Network Management

Network management

904. Agencies **SHOULD**:

a. apply logical access controls to the network,
b. use gateways to defend the 'perimeter' and sensitive parts of their networks, and
c. be aware of the high-risk points of connectivity in the network.
   Example: Dial-in connections and Internet gateways are high-risk points.

Configuration management

905. Agencies **SHOULD** keep the network configuration under the control of a central network management group.

All changes to the configuration **SHOULD** be:

a. approved through a formal change control process,
b. documented, and
c. comply with the network security policy and security plan.

Agencies **SHOULD** regularly review the configuration to ensure it conforms with the documented configuration.

Multilevel Networks

Multilevel networks

907. The table below describes security recommendations for the two modes of Multilevel networks.

See: 'About IT Systems' on page 1-9 for a definition of modes of operation.

Mode	RECOMMENDED security mechanisms
Compartmented	• Use access control and audit strategies. **See:** 'Chapter 6 - Logical Access Control' on page 3-58. • Use a Public Key Infrastructure (PKI) to reinforce the privacy of information in a compartmented system.
Multilevel	• Use DAPs to minimise the risk of inadequately cleared staff accessing classified information. • Encourage user discipline to manage the ongoing security configuration.

Wireless Networks

Introduction

908. Wireless networks use radio frequencies to transmit information across the network, and access the wired portion of a network through an Access Point (AP).

Currently the main types of wireless networks are:

- IEEE 802.11,
- Bluetooth, and
- General Packet Radio Service (GPRS).

Policy [IC, P]

909. Agencies **SHOULD NOT** use wireless networks for the transmission of IN-CONFIDENCE or PROTECTED information unless the security they incorporate has been approved by DSD.

See: *PSM* C7.129.

Policy [R]

910. Agencies **MUST NOT** use wireless networks for the transmission of RESTRICTED information unless the security they incorporate has been approved by DSD.

See: *PSM* C7.129.

Infrared Transmissions

Policy

913. Agencies **SHOULD** disable all infrared (IR) ports on security classified system hardware.

Where agencies have a valid, documented requirement for using IR, agencies **SHOULD** ensure that:

a. the information being transmitted is **not** CABINET-IN-CONFIDENCE information nor national security information classified above RESTRICTED,
b. the systems and/or devices involved do **not** handle CABINET-IN-CONFIDENCE information nor national security information classified above RESTRICTED,
c. all transmissions occur within a controlled space,
   Note: A controlled space, as defined in *ACSI 61*, is the three dimensional space surrounding equipment or facilities that process classified information within which:
   1) unauthorised personnel are denied unrestricted access, and
   2) positive measures are taken to control the movement of personnel and materials including vehicles.
d. a risk assessment is conducted for each individual controlled space,
e. measures are taken to minimise the likelihood of direct visual access to the IR signal from uncontrolled spaces,
f. the line-of-sight distance between the IR device(s) and any uncontrolled space(s) is at least 20 metres, and
g. devices such as "infra-red boosters" are not used to amplify the strength of the transmitted signal.

Exception: Whilst DSD **RECOMMENDS** against it, agencies may use IR mice even if the conditions listed above are **not** met. However, the mouse **SHOULD** communicate with the system via a dedicated, receive-only IR port.

Internetwork Connections

Internetwork connections

915. Internetwork policies and standards act to prevent and monitor unintended information flow, and/or access.

Internetwork security policy

916. Agencies **SHOULD** ensure that:

a. the information flow over the connection is consistent with the ITSP,
b. the use of the connection is limited to those users who are authorised to use it,
c. all users are held accountable for their actions in relation to the connection,
d. all users operate over the connection within the limits of their required rights and privilege,
e. the confidentiality of information is assured,
f. any additional security required to protect caveats, codewords, special handling and/or releasability indicators are implemented, and
g. the integrity of the information flowing over the connection is preserved.

Policy for connection to public networks such as the Internet [PD, U, R, IC, P]

917. Paragraph C7.137 of the *PSM* states that networks classified PUBLIC DOMAIN, UNCLASSIFIED, RESTRICTED, IN-CONFIDENCE or PROTECTED may be connected to public networks or other non-Australian Government networks provided:

a. the whole network is behind a firewall approved by DSD for that purpose,
b. the network is certified, and
c. all security classified information is retained within the network.

For these classifications, agencies **SHOULD** use a gateway certified against the standards and guidelines contained in *ACSI 33*.

Risk of undesirable cascaded connections

920. Before connecting an agency system to another system, agencies **SHOULD** obtain a list of systems to which the other system is connected. This information **SHOULD** be requested from the other system's:

- Accreditation Authority, and
- System Manager.

Information from both sources **SHOULD** be examined to determine the existence of possible undesirable cascaded connections.

Gateways

Definition: gateway

921. A gateway is a secured connection between an internal network and an external network.

Gateways usually consist of a number of items of computer equipment including:

- firewalls,
- proxy servers,
- routers, and
- email servers.

Requirements of a gateway

922. A gateway **SHOULD**:

a. be the only communications route into and out of the internal network,
b. by default, deny all connections to the internal network from outside sources,
c. allow only explicitly authorised connections,
d. be managed via a secure path,
e. provide sufficient audit capability to detect breaches of the gateway's security and attempted network intrusions, and
f. provide real-time alarms.

Demilitarised Zones

924. A Demilitarised Zone (DMZ) may be achieved by placing the external network, public information servers, and internal network on three different physical ports of a single firewall or by the use of multiple firewalls.

Agencies **SHOULD** use DMZs to separate externally accessible systems, such as web servers, from both the public and from the agency's internal networks.

Firewall assurance levels [U, IC, R, P]

925. The following table provides the minimum levels of assurance for firewalls within gateways.

In the table below, a "traffic flow filter" refers to a device configured to filter and control the flow of data. Agencies **SHOULD** use one or more of the following, with the order of preference as shown.

1. A firewall listed on DSD's EPL.
2. A firewall or proxy not listed on DSD's EPL.
3. A router with appropriate access control lists configured.

If your network is…	And the other network is…	Then your gateway requires…
UNCLASSIFIED,	• PUBLIC DOMAIN, • UNCLASSIFIED, • IN-CONFIDENCE, • PROTECTED, • HIGHLY PROTECTED, or • National Security,	a traffic flow filter.
IN-CONFIDENCE,	PUBLIC DOMAIN,	an EAL2 firewall.
	• UNCLASSIFIED, • IN-CONFIDENCE, • PROTECTED, • HIGHLY PROTECTED, or • National Security,	a traffic flow filter.
RESTRICTED,	• PUBLIC DOMAIN, • UNCLASSIFIED, or • IN-CONFIDENCE,	an EAL2 firewall.
	• PROTECTED, • HIGHLY PROTECTED, or • National Security,	a traffic flow filter.
PROTECTED,	• PUBLIC DOMAIN, or • UNCLASSIFIED,	an EAL4 firewall.
	• IN-CONFIDENCE, or • RESTRICTED,	an EAL3 firewall.
	PROTECTED,	an EAL2 firewall.
	• HIGHLY PROTECTED, or • National Security above RESTRICTED,	an EAL1 firewall.

One-way Gateways

Definition: one-way gateway

928. One-way gateways, also known as diodes, are gateways through which data can only flow in one direction. This is generally achieved by breaking the electrical or optical connection on the return path.

Depending on the requirements a one-way gateway can be deployed two different ways. They can be configured to allow either:

- data from a less trusted system to be pushed up into a more trusted system whilst preventing data in the more trusted system from entering the less trusted system, or
- data from a more trusted system to be pushed down into a less trusted system whilst preventing data, or users, in the less trusted system from entering the more trusted system.

Content and volume checks

929. Agencies deploying a one-way gateway **SHOULD** check the content of the data being transferred and the volume of data to ensure that it conforms to expectations.

See: 'Filters' on page 3-102.

Assurance requirements [PD, U, IC, R, P]

930. If a one-way gateway is used then agencies **SHOULD** use a device with some level of formal assurance.

Filters

Definition: filter

932. A filter controls the flow of data in accordance with a security policy.

Examples: Email content scanners and "dirty word" checkers.

Guidelines

933. Agencies **SHOULD** deploy filters on gateways between its classified systems and other systems.

Data Transfer

Introduction

934. This topic contains information about data transfer requirements.

Risks associated with data transfer

935. The table below identifies some common risks and countermeasures associated with data transfer across systems.

If the data is...	Then the threat is to the…	And countermeasure is to…
exported to a less trusted system,	confidentiality of the data from the more trusted system,	check for and filter sensitive content.
imported from a less trusted system,	integrity and availability of the more trusted system,	perform integrity checks on the data.

Continued on next page

Data export guidelines

936. The table below describes guidelines for data export.

Security issue	Guidelines
Transfer authorisation	The ITSA **SHOULD** approve all transfers to less trusted systems.
Data controls	• The security mechanisms used to prevent inadvertent transfer of data from the more trusted system **SHOULD** have adequate assurance. • If the volume of data is low, then manually review the export. • If the data is closely formatted, then automatically filter exports by a software filter.
Software filters	Agencies **SHOULD** filter the data using one or more of the following techniques: • format checks, • range checks on data within fields, • data type, and • keyword search. **Example:** A search for "dirty words" may indicate the presence of classified or inappropriate material.
Media	Agencies **SHOULD** transfer the data using a: • previously unused piece of media, or • pool of media items created **only** for transfer. Agencies **SHOULD NOT** transfer data using media that has previously contained data of a higher classification than the systems between which the data is being transferred.

Data export to a lower classified system by a gateway

937. A gateway **SHOULD** restrict the export of data from a higher classified to a lower classified system by:

a. validating the classification label attached to outgoing data against the permitted classifications, and
b. filtering data using data format checks, dirty word searches and data range checks.

Remote Access

Definition: remote access

939. Remote access is any access to an agency's system from a location not within the physical control of that agency.

Standards

940. Agencies that allow users remote access to systems containing classified information **MUST** ensure that:

a. the users are authenticated at the start of each session,
   Note: DSD **RECOMMENDS** that agencies use more stringent measures to authenticate remote users than it would for users accessing the systems from sites under the physical control of the agency.
b. the users are given the minimum system access necessary to perform their duties,
   Note: DSD **RECOMMENDS** that agencies do not allow the use of privileged access remotely.
c. the users can only access the agency's system from systems accredited to at least the classification of the agency's system, and
d. any data transferred is appropriately protected during transmission and at the remote user's end.

Virtual Private Networks

Definition: Virtual Private Network

941. A Virtual Private Network (VPN) encrypts information between two or more parties. It can be used to set up a private channel using existing communications network such as the Internet.

Why use a VPN?

942. The use of a VPN:

- ensures confidentiality and integrity of data in transit by encrypting the data,
- provides some assurance that the connection originates from a trusted source, and
- eliminates the cost of using a dedicated encryption link between different sites.

Additional controls for a VPN

943. The use of VPNs does not obviate the need for traditional security measures. Agencies **SHOULD** ensure that measures are in place to:

a. authenticate the originator of the connection,
b. provide access control within the agency network,
c. audit the actions of the party obtaining access,
   See: 'Chapter 6 - Logical Access Control' on page 3-58.
d. maintain the integrity and availability of agency systems, and
   Example: Against malicious content.
e. prevent leakage of data of a higher classification to a lower classified network or system.

Selecting a VPN product

944. Agencies **MUST** use DAPs when implementing a VPN.

See: 'Cryptography' on page 3-77.

Peripheral Switches

Definition: peripheral switch

945. Peripheral switches are used to share a set of peripherals between a number of computers. The most common type of peripheral switch is the Keyboard/Video/Mouse (KVM) Switch.

KVM assurance requirements

946. The table below provides the minimum level of assurance that agencies **SHOULD** have when using a KVM switch.

If the KVM is for more than two systems then the level is determined by the highest and lowest of the system classifications involved.

Key:

Grade	Assurance Level
D	EAL2
E	None

	PD	U	IC	R	P
PD	E				
U	E	E			
IC	E	E	E		
R	D	D	E	E	
P	D	D	E	E	E

Multifunction Devices

Definition: multifunction devices

948. Within this document, the term "multifunction devices" (MFDs) refers to the class of devices that combine printing, scanning, copying, faxing and/or voice messaging functionality within the one device. These devices are designed to connect to a computer and telephone network simultaneously.

Risks with MFDs

949. The three main risks associated with MFDs are:

- a user faxing a classified document when their intention was to either print, copy or scan the document,
- a user assuming that because the capability exists, it is acceptable to fax a classified document from their PC, and
- an attacker entering the system via the telephone network connection.

Usage policy [IC, R]

950. MFDs **SHOULD NOT** have their telephone or facsimile functionality enabled unless the telephone network is accredited to at least the same security classification as the computer network.

Usage policy [P]

951. MFDs **MUST NOT** have their telephone or facsimile functionality enabled unless the telephone network is accredited to at least the same security classification as the computer network.

Policies, plans and procedures

953. Agencies deploying MFDs **MUST** develop a set of policies, plans and procedures governing the use of the equipment.

Abbreviations, Glossary and Index

Abbreviations

ACL	Access Control List
ACSI	Australian Communications - Electronic Security Instruction
AISEP	Australasian Information Security Evaluation Program
AS/NZS	Australian Standard/New Zealand Standard
ASA	Agency Security Adviser
CC	Common Criteria
CR	Certification Report
CCRA	Common Criteria Recognition Arrangement
DAP	DSD Approved Product
DMZ	Demilitarised Zone
DSD	Defence Signals Directorate
EACS	Electronic Access Control System
EAL	Evaluation Assurance Level
EPL	Evaluated Products List
HGCE	High Grade Cryptographic Equipment
I-RAP	Infosec-Registered Assessor Program
IDS	Intrusion Detection System
ISIDRAS	Information Security Incident Detection, Reporting and Analysis Scheme
IT	Information Technology
ITSA	Information Technology Security Adviser
ITSEC	Information Technology Security Evaluation Criteria
ITSP	Information Technology Security Policy
KVM	Keyboard/Video/Mouse
MFD	Multifunction Device
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PSM	*Protective Security Manual*
PTT	Push-To-Talk
RF	Radio Frequency
RMP	Risk Management Plan
ROM	Read-Only Memory
SAS	Security Alarm System
SCEC	Security Construction and Equipment Committee
SIC	SECURITY-IN-CONFIDENCE
SOP	Standard Operating Procedure
SR	Server Room
SSP	System Security Plan
ST	Security Target
TOE	Target of Evaluation
TSCM	Technical Surveillance Counter Measures
VPN	Virtual Private Network

This page is intentionally blank.

Glossary

IMPORTANT	This glossary is included for quick reference and does **not** replace *ACSI 1(B) - Information Systems Security Glossary*.
Accreditation authority	The Accreditation Authority is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.
Australasian Information Security Evaluation Program (AISEP)	The AISEP is a program under which evaluations are performed by impartial companies against the Common Criteria and ITSEC. The results of these evaluations are then certified by DSD, which is responsible for the overall operation of the program.
Certification	The assertion by an approved entity that compliance with a standard has been achieved, based on a comprehensive evaluation. Certification is generally a prerequisite for accreditation.
Certification Report (CR)	The CR contains the findings of the certification for a system, site or product. For products evaluated under the Common Criteria or ITSEC, the CR is the definitive document for product specific guidance and provides detailed security information such as a clarification of the scope of the evaluation and recommendations on use of the product.
Common Criteria (CC)	The CC is an ISO standard (ISO 15408) for IT security evaluations. The purpose of CC is to ensure that IT security evaluations world-wide are: • performed against a common set of requirements, and • that the security claims are expressed unambiguously. **See:** http://www.commoncriteriaportal.org/
Common Criteria Recognition Arrangement (CCRA)	The CCRA is a mutual recognition arrangement for Common Criteria evaluations among a group of participating countries, including Australia and New Zealand.

Continued on next page

Comsec	**See:** Communications Security
Communications security	Communications Security (Comsec) is the measure and controls taken to deny unauthorised persons information derived from telecommunications and to ensure the authenticity of such telecommunications.
Control	A control is a measure that is taken to mitigate risks.
Control register	A control register is a document used in the RMP to record the controls required for a site.
Countermeasure	**See:** Control
Cryptographic system	A cryptographic system is a related set of hardware and/or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.
Cryptography	Cryptography is the art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.
Cryptoperiod	A cryptoperiod is the time span during which each key setting remains in effect.
Declassification, media	The administrative decision to remove all classifications from the media, based on an assessment of relevant issues including the consequences of damage from disclosure or misuse, the effectiveness of any sanitisation procedure used, and the intended destination of the media.
Degaussing	Degaussing is the process of applying a magnetic force to remove information from media.

Continued on next page

Demilitarised zone (DMZ)	A DMZ is a small network with one or more servers that is kept separate from an organisation's core network, either on the outside of the organisation's firewall, or as a separate network protected by the organisation's firewall. DMZs usually provide public information to less trusted networks, such as the Internet.
Emanation security	Emanation security includes, but is not limited to, consideration of: a. audio, b. visual, c. infra-red, and d. electromagnetic emissions. TEMPEST security is a subset of emanation security.
Encryption	Encryption is the art or science concerning the principles, means, and methods for rendering plain information unintelligible.
Evaluated Products List (EPL)	The Evaluated Products List (EPL) is a list of DAPs. It is available on the DSD website. **URL:** http://www.dsd.gov.au/infosec/aisep/EPL.html
Evaluation Assurance Level (EAL)	The EAL is a standard assurance level, ranging from EAL1 to EAL7, under the Common Criteria. EAL1 offers the least assurance, while EAL7 offers the highest assurance. Each assurance level comprises a number of assurance components, covering aspects of the product's design, development and operation.
Firewall	A firewall is a network device that filters incoming and outgoing network data, based on a series of rules set by the firewall administrator.
Gateway	A gateway is a secured connection between an internal network and an external network. A gateway will usually comprise a number of items of computer equipment including: a. a firewall host, b. proxy servers, c. routers, and d. email hosts.

Continued on next page

Gateway certification	A certification that a gateway environment meets the relevant standards. Gateway certification may be performed by the agency's ITSA, or by an independent third-party such as DSD or an I-RAP assessor.
General User	A General User is a User who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security. **Note:** General Users are normally those Users who are not Privileged Users.
Hardware	The physical components of computer equipment including peripheral equipment. Examples of hardware include: a. personal computers, b. mainframe computers, c. laptops, d. printers, e. routers, f. hubs, g. personal digital assistants (PDAs), and h. mobile phones.
High Grade	An evaluation level in excess of the defined Common Criteria evaluation levels.
IT system	For the purposes of this document, an IT system is: a. a related set of hardware and software used for the communication, processing and storage of information, and b. the electronic form (not content) of the information that they hold or process.
Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS)	A scheme established by DSD to collect information on security incidents that affect the security or functionality of Australian Government computer and communication systems.

Continued on next page

Information Technology Security Adviser (ITSA)	The Information Technology Security Adviser (ITSA) is the person appointed by an agency to manage the security of the agency's information and IT systems.
Information Technology Security Evaluation Criteria (ITSEC)	The ITSEC is an older national security evaluation criteria developed by European countries in the early 1990's. The ITSEC specifies seven levels of assurance, known as E0 (Inadequate assurance) to E6 (highest assurance).
Information Technology Security Policy (ITSP)	An Information Technology Security Policy (ITSP) is a document that describes the information security policies, standards and responsibilities for an agency.
Infosec-Registered Assessor Program (I-RAP)	The Infosec-Registered Assessor Program is a DSD initiative designed to register suitably qualified information security assessors to conduct work to Commonwealth best practice standards. **URL:** http://www.dsd.gov.au/infosec/evaluation_services/irap.html
Key	A key is a sequence of random or pseudo random bits used: a. initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, b. for determining electronic counter-countermeasure patterns, or **Example:** frequency hopping or spread spectrum c. for producing other keys.
Malicious code	Malicious code is any software that attempts to subvert the confidentiality, integrity or availability of a system. Malicious code includes: a. logic bombs, b. trapdoors, c. Trojan programs, d. viruses, and e. worms.

Continued on next page

Media	Media is the component of hardware that is used to store information.
Need-to-know	The principle of telling a person only the information that they require to fulfil their role.
Non-volatile media	Non-volatile media is media which retains its information when power is removed.
Privileged User	A Privileged User is a User who can alter or circumvent system security protections. This may also apply to Users who may have only limited privileges, such as software developers, who can still bypass security precautions. A Privileged User may have the capability to modify system configurations, account privileges, audit logs, data files or applications. **Examples:** System administrators, IT security staff, Helpdesk staff.
Reclassification, media	The administrative decision to change the classification of the media, based on an assessment of relevant issues including the consequences of damage from unauthorised disclosure of misuse, the effectiveness of any sanitisation procedure used, and the intended destination of the media.
Risk	The *Australia/New Zealand Risk Management Standard (AS/NZS 4360:1999)* defines risk as 'the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.'
Risk Register	A list, or database, of the risks faced by an agency.
Risk Management Plan (RMP)	The complete documentation package generated by following the risk management process.
Sanitisation, media	The process of erasing or overwriting information stored on media. **Note:** The process of sanitisation **does not** automatically change the classification of the media, nor does sanitisation involve the destruction of the media. **See:** Glossary entries for 'Declassification', 'Reclassification'.

Continued on next page

Security Construction and Equipment Committee (SCEC)	The SCEC approves security equipment for Australian Government use.
Security Target (ST)	The security target for a product is a document defining the: a. security claims of the TOE, b. scope of the evaluation, and c. the intended operational environment of the TOE. The security claims are divided into: a. a set of security requirements, and b. details of the security functions which meet those requirements.
Session key	A key used only for the duration of a particular communications session.
System Administrator	The person responsible for the day-to-day operation of the system.
System Manager	The manager responsible for maintaining the technical and operational effectiveness of a system on behalf of the system owner.
System Owner	The senior agency manager with formal responsibility for the information resource. Usually has accreditation authority for the system.
Target of Evaluation (TOE)	The part of the product or system that is subject to an evaluation.
Technical Surveillance Counter Measures (TSCM)	Technical surveillance counter measures (TSCM) are searches for covert electronic surveillance devices. TSCM are also known as ‘sweeps’.

Continued on next page

User	A User is anyone with access to a system. **Note:** A User is not necessarily an employee of the organisation that owns the system.
Virus	**See:** Malicious Code
Volatile media	Volatile media is media which loses its information when power is removed.

Index

A

C

N

O

P

R

S