Australian Government
Department of Defence

Australian Government Information and Communications Technology Security Manual

ACSI 33

Defence Signals Directorate

Release Date: 19 September 2005

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.

All Australian Government information whether classified or not, is protected from unauthorised disclosure under the *Crimes Act 1914*. Australian Government information may only be released in accordance with the *Commonwealth Protective Security Manual*.

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 and Communications 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 ICT Security

Overview

Introduction

1.0.1. This part contains important information relating to this manual and how it relates to the security of Australian Government Information and Communications Technology (ICT) systems.

Authority

1.0.2. The *Commonwealth Protective Security Manual (PSM)* sets out the policies, practices and procedures required to achieve an appropriate security environment within the Australian Government. The *PSM* requires agencies to comply with this manual for the protection of information held on information and communications systems.

Compliance

1.0.2.1. Agencies **MUST** be compliant with the manual released no more than two years previously.

DSD **RECOMMENDS** that agencies maintain compliance with the current release of the manual.

Important: In some cases, DSD may make a determination that a newly introduced policy requirement is of particular importance, and that agencies will be required to meet the new policy within a shorter time frame.

Contents

1.0.3. This part contains the following topics:

Using ACSI 33

Introduction

1.0.4. The information in this topic will help you to use this manual more effectively.

Classification of ACSI 33

1.0.5. This manual comes in two versions as shown in the table below.

The *ACSI 33* version classified as…	Covers the following system classifications…
UNCLASSIFIED	• UNCLASSIFIED, • IN-CONFIDENCE, • RESTRICTED, and • PROTECTED.
SECURITY-IN-CONFIDENCE	As per the UNCLASSIFIED version plus: • HIGHLY PROTECTED, • CONFIDENTIAL, • SECRET, and • TOP SECRET.

Paragraph classifications

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

Text that only appears in the SECURITY-IN-CONFIDENCE version is shown in blue.

Paragraph numbering

1.0.7. Paragraph numbers consist of several fields separated by full stops. The fields are ordered as follows:

- Part number
- Chapter number
- Paragraph number

Note: A fourth field is used to indicate new paragraphs that have been inserted since the last hardcopy release.

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 being read.

Continued on next page

Paragraph applicability and system classifications

1.0.8. Readers will note that some paragraph titles include a system classification or caveat reference, shown within square brackets. Paragraph titles that do not include such a reference indicate that the paragraph applies to all ICT systems.

Updates

1.0.9. This manual is a living document. It is therefore important that agencies ensure that they are using the latest release.

The table below provides the websites from which the latest releases of this manual will be available.

***ACSI 33* version**	**Location**
UNCLASSIFIED	• DSD's Internet website **URL:** http://www.dsd.gov.au/ • OnSecure **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

1.0.10. DSD welcomes feedback about this manual. To suggest improvements, or advise of inaccuracies or ambiguities, please contact DSD.

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

Target audience

1.0.11. The target audience for this manual is:

- IT Security Advisers (ITSAs),
- Agency Security Advisers (ASAs),
- agency ICT 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 ICT security responsibilities, and
- security personnel with some understanding of and responsibility for ICT security.

Continued on next page

Terminology

1.0.12. This manual 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	Information that is security 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 or circulation, such as agency publications and websites.
CABINET-IN-CONFIDENCE	Documents prepared for consideration by Cabinet, including those in preparation.

Treatment of CABINET-IN-CONFIDENCE

1.0.13. The *Cabinet Handbook* states that the **minimum** protection given to Cabinet documents is to be equivalent to information marked as PROTECTED. Unless otherwise noted, references in this manual to IN-CONFIDENCE **do not** include CABINET-IN-CONFIDENCE.

Treatment of AUSTEO and AGAO

1.0.14. The classification marking of information defines the **minimum** protection required. Information that is also marked with the AUSTEO or AGAO caveat may require additional protection in some areas, as detailed in this manual.

Continued on next page

How to use ACSI 33

1.0.15. The table below contains suggestions for using this manual.

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

Continued on next page

Keywords for requirements

1.0.16. The table below defines the keywords used within this manual to indicate the level of requirements. All keywords are presented in bold, uppercase 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"

1.0.17. 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"

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

a. the reasons for the deviation,
b. an assessment of the residual risk resulting from the deviation,
c. a date by which to review the decision,
d. the ITSA's involvement in the decision, and
e. management's approval.

DSD **RECOMMENDS** that ITSAs retain a copy of all deviations.

Continued on next page

Legislation and other Government policy

1.0.19. Compliance with the requirements of this manual 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 manual 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.

The High-Level Process of ICT Security

About the process

1.0.20. ICT 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

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

Process

1.0.22. The table below describes the stages that DSD **RECOMMENDS** agencies follow to implement the appropriate ICT 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 an ICT Security Policy 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 ICT security plan for use across related systems. • Develop or amend an SSP, possibly based on the high-level ICT security plan, to cover each system.	Chapter 5 – Developing an SSP on page 2-36
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 2-39
5. Certification	• Determine what needs certifying. • Obtain certification from the relevant person or organisation.	Chapter 7 – Certifying and Accrediting ICT Systems on page 2-46
6. Accreditation	Obtain accreditation from the relevant authority.	
7. Maintenance	• Implement change control procedures. • Perform integrity checks.	Chapter 8 – Maintaining ICT Security and Managing Security on page 2-59
8. Review	Review and revisit each stage of this process annually.	Chapter 9 – Reviewing ICT Security on page 2-72

About ICT Systems

Definition: ICT system

1.0.23. For the purposes of this manual, an ICT 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.

Definition: ICT system classification

1.0.23.1 The classification of an ICT system is the highest classification of information for which the system is accredited.

See: 'About Certification and Accreditation' on page 2-47.

Continued on next page

System modes

1.0.24. For the purposes of this manual, an ICT 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 3-62 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 control to the compartmented information is enforced by the system.
Multilevel	Information at two or more 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

1.0.25. The table below identifies the location of further information contained in other documents. To obtain copies of these documents, please contact the indicated organisation.

For further information on...	See...	Available from…
AGAO	*PSM* 2000, Part C, Information Security	AGD
AUSTEO	Section 3 of the *Inter-Agency Security Supplement to the Commonwealth Protective Security Manual* **Note:** This document is classified CONFIDENTIAL.	AGD
CABINET-IN-CONFIDENCE information security	*Cabinet Handbook*, Chapter 7, Security and Handling of Cabinet Documents	PM&C
classification labelling,	*PSM* 2000, Part C, Information Security	AGD
clearances,	*PSM* 2000, Part D, Personnel Security	AGD
information handling procedures,	*PSM* 2000, Part C, Information Security	AGD
information security management,	• AS/NZS ISO/IEC 17799:2001 – *Information Technology - Code of Practice for Information Security Managemen*t, and • AS/NZS 7799.2:2003 – *Information Security Management*	Standards Australia
information security responsibilities,	*PSM* 2000, Part A, Protective Security Policy	AGD
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.	AGD
reporting of security incidents,	*PSM* 2000, Part G, Guidelines on Security Incidents and Investigations.	AGD
risk management,	• AS/NZS 4360:2004 *Risk Management*, and • HB 436:2004 *Risk Management Guidelines*	Standards Australia
storage and archival of Government information,	*Archives Act 1983*	National Archives of Australia

This page is intentionally blank.

Part 2
ICT Security Administration

Overview

Introduction

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

Contents

2.0.2. This part contains the following chapters:

Chapter 1 – ICT Security Roles and Responsibilities

Overview

Introduction

2.1.1. This chapter contains information relating to ICT security roles and responsibilities.

System specific responsibilities

2.1.2. 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

2.1.3. This chapter contains the following topics:

DSD

DSD's role

2.1.4. 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.

In addition, DSD plays an important role working with industry to develop new cryptographic products. It also established the Australasian Information Security Evaluation Program (AISEP) in order to deal with the increasing requirement to evaluate information security products.

Within DSD, the Information Security Group performs these roles.

Contacting DSD

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

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

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

Other Organisations

Other organisations

2.1.6. 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 protective security. The PSCC's Training Centre provides protective security 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 ICT systems. **URL:** http://www.naa.gov.au/
Department of Finance (Australian Government Information Management Office)	Development, coordination and oversight of Government policy on electronic commerce, online services and the Internet. **URL:** http://www.finance.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 (ITSA)

Requirement for ITSA

2.1.7. Agencies **MUST** 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. However, the agency ITSA retains overall responsibility.
See: 'IT Security Adviser Responsibilities' on page 2-6.

Appointing an ITSA

2.1.8. The ITSA **MUST** have:

a. ready access to and full support from line management,
b. familiarity with information and/or ICT 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:

d. operating systems,
e. access control features, and
f. auditing facilities.

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

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

Clearance and briefing status

2.1.9. The ITSA **MUST** be**:**

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

IT Security Adviser Responsibilities

Primary responsibility

2.1.10. The ITSA is responsible for overseeing ICT security within an agency.

Allocation of ITSA functions

2.1.11. 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

2.1.12. The ITSA is responsible for:

- identifying and recommending security improvements to systems,
- ensuring security aspects are considered as part of the change management process,
- coordinating the development, maintenance and implementation of all security-related system documents, in conjunction with the System Managers, and
- investigating and reporting security incidents to DSD, in conjunction with the ASA.

Technical security advice and training responsibilities

2.1.13. 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

2.1.14. 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

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

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

Certification and accreditation responsibilities

2.1.16. 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

2.1.17. 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**

2.1.18. Part C 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

2.1.19. 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 2-36.
- SOP, **See:** 'Chapter 6 – Developing and Maintaining Security SOPs' on page 2-39.

Certification and accreditation responsibilities

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

- ensuring that the system complies with the relevant ICTSP 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 ICT Systems' on page 2-46 for more detail.

SOPs

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

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

Continued on next page

Ensuring adherence to procedures	2.1.22. The System Manager is responsible for ensuring that procedures recorded in security documentation are followed.

System Users

Types of system users

2.1.23. 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

2.1.24. 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

2.1.25. 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

2.1.26. Agencies **SHOULD**:

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

Chapter 2 – Security Documentation

Overview

Introduction

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

Contents

2.2.2. This chapter contains the following topics:

Not included

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

Requirements for ICT Security Documentation

Document requirements

2.2.4. Agencies **MUST** have security risk assessments, policies and plans that cover their ICT 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 and Communications Technology Security Policy

2.2.5. Agencies **MUST** have an ICT Security Policy (ICTSP) document. The ICTSP 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 an ICT Security Policy' on page 2-19.

Risk Management Plan for ICT systems

2.2.6. 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

2.2.7. 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 2-36.

SOPs

2.2.8. 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 2-39.

Continued on next page

Using higher level documents to avoid repetition

2.2.10. 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,
- classification,
- system functionality,
- common technical platform, and
- management boundaries.

Using a documentation framework

2.2.11. 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 ICT 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

2.2.12. An ICTSP 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
ICTSP	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

2.2.13. 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 ICT Security Documentation' on page 2-12.

Develop the content

2.2.14. DSD **RECOMMENDS** that ICT 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

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

DSD **RECOMMENDS** that:

a. all high level ICT 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

2.2.16. Agencies **SHOULD** develop a schedule for reviewing all ICT 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 ICT Security Documents

Purpose

2.2.17. ICT 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 ICT security documentation in accordance with Part C of the *PSM*.

General guidance

2.2.18. 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: 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 are:

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

Document classification

2.2.19. Agencies **SHOULD** apply the following classifications, as a minimum, to ICT 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	UNCLASSIFIED
• IN-CONFIDENCE, • PROTECTED	SECURITY-IN-CONFIDENCE
RESTRICTED	• SECURITY-IN-CONFIDENCE or • RESTRICTED

Templates

References

2.2.21. 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
ICT Security Policy (ICTSP)	*AS/NZS 7799.2:2003 Information Security Management - Part 2*	Standards Australia **URL:** www.standards.com.au	Annex A contains the basis of an Information Security Policy which is slightly broader than an Information and Communications 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,* now replaced by *AS/NZS 4360:2004,* 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 quite lengthy. However, an appendix 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 an ICT Security Policy

Overview

Introduction

2.3.1. This chapter contains information about ICTSPs.

An ICTSP may also be known as an Information System Security Policy (ISSP) or Information Technology Security Policy (ITSP).

Template

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

Contents

2.3.3. This chapter contains the following topics:

About ICTSPs

Definition: ICTSP

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

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

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

ICTSP contents

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

National ICTSP documents

2.3.6. The key Australian Government ICTSP documents to be considered when developing agency policy documents are the:

- *PSM*, and
- this manual.

Inconsistencies between policies

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

Developing an ICTSP

Process

2.3.8. The table below describes the process an ITSA may follow when developing an ICTSP for an agency.

Further details are supplied in the following paragraphs.

Stage	Description
1	Gain management support for the development of an ICTSP.
2	Determine the overall scope, objectives and structure of the ICTSP.
3	Identify all existing applicable policies and standards and record them in the ICTSP.
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 ICTSP.
6	Identify general and specific responsibilities for ICT security management.
7	Gain management approval and signoff.
8	Publish and communicate the ICTSP to agency staff.

Identifying existing policies and standards

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

- *PSM*,
- this manual,
- *AS/NZS ISO/IEC 17799:2001*,
- *AS/NZS 7799.2:2003*, and
- agency-specific policies.

Other applicable policies and standards may be available from:

- ASIO T4 Protective Security Group,
- Commonwealth Law Enforcement Board,
- Information Security Group, DSD,
- National Archives of Australia,
- Department of Finance (Australian Government Information Management Office),
- The Office of the Federal Privacy Commissioner, and
- Attorney-General's Department.

Continued on next page

Policy questions

2.3.10. 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

2.3.11. Once the overall policy has been defined, it 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

2.3.12. 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

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

This chapter contains information about developing and using an RMP to manage risk affecting ICT systems in compliance with the requirements of the ICTSP.

Once an agency has a clear picture of its risk environment, it can then determine whether the minimum measures given in this manual are sufficient to address the identified risks, or whether additional measures will be required to provide an appropriate security environment.

ICT security risk management

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

Consistency with standards

2.4.3. The risk management process used in this manual 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 4360:2004 *'Risk Management*',
- HB 436:2004 *'Risk Management Guidelines'*, and
- HB 231:2004 *'Information Security Risk Management Guidelines*'.

The material in this manual does not duplicate these guidelines.

Development and maintenance

2.4.4. 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

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

Template

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

Continued on next page

Contents

2.4.7. This chapter contains the following topics.

The Process of Developing a Risk Management Plan

Important

2.4.8. 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

2.4.9. 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 an 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

2.4.10. 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

2.4.11. 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 2-34.
5	Determine appropriate controls for each risk. **See:** 'Stage 5: Developing a Risk Treatment Plan' on page 2-35.
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

The Process of Developing a Risk Management Plan, Continued

Producing an RMP

2.4.12. 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 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

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

Further detail

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

Procedure

2.4.15. 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 ICT system(s) concerned? • What are the internal drivers? • What is the key to the success of the ICT system(s)? • Are there shared risks with other agencies? • What resources are available? • How does the ICT 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

2.4.16. The next stage in the process of conducting an RMP is to perform a risk assessment, starting by identifying the risks.

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

Stage 2: Identifying the Risks

Prerequisite

2.4.17. 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

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

Procedure

2.4.19. 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

2.4.20. The next stage in the process of conducting a risk assessment is to analyse the risks.

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

Stage 3: Analysing the Risks

Prerequisite

2.4.21. 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

2.4.22. 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

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

Procedure

2.4.24. 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.

Next stage

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

See: 'Stage 4: Assessing and Prioritising Risks' on page 2-34.

Continued on next page

Consequence determination

2.4.26. The table below describes the consequence ratings given as an example in the *PSM*. Agencies performing a risk assessment may use this table, or develop their own agency-specific table.

If the consequences include…	Then an appropriate consequence rating is…
• critical injuries or death, • critical financial loss, • key agency functions or service delivery significantly compromised for more than one day, • national or international adverse publicity causing serious embarrassment to Government or complete loss of stakeholder confidence, or • Government closes or significantly restructures the agency,	catastrophic.
• serious injuries requiring hospitalisation, • very high financial loss, • key agency functions or service delivery significantly compromised for up to one day, • wide-spread adverse publicity causing embarrassment to Government or serious loss of stakeholder confidence, or • ministerial intervention,	major.
• injuries requiring hospital treatment but not admission, • high financial loss, • key agency functions or service delivery significantly compromised for up to one hour, • substantial adverse publicity or loss of stakeholder confidence, or • top management intervention,	moderate.
• minor injuries treated at scene, • medium financial loss, • key agency functions or service delivery compromised for up to 30 minutes, • some adverse publicity or loss of stakeholder confidence, or • management review of current policies and procedures instigated,	minor.
• no injuries, • low financial loss, • key agency functions or service delivery not affected, • no adverse publicity or loss of stakeholder confidence, or • managed by existing policies and procedures,	insignificant.

Continued on next page

Document Consequence Table

2.4.27. The Consequence Table used in an RMP **SHOULD** be documented in the RMP.

Likelihood determination

2.4.28. The table below contains ratings that can be selected to show how likely it is that a risk will occur. Agencies performing a risk assessment 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

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

Risk matrix

2.4.30. 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

2.4.31. The table below identifies and explains the risk levels used in the matrix. Agencies performing a risk assessment 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.

Continued on next page

Matrix

2.4.32. The matrix below, in conjunction with the legend, may be used to determine the risk level. Agencies performing a risk assessment 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

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

Stage 4: Assessing and Prioritising Risks

Prerequisite

2.4.34. 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

2.4.35. 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

2.4.36. 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

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

Procedure

2.4.38. 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

2.4.39. 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 2-35.

Stage 5: Developing a Risk Treatment Plan

Prerequisite

2.4.40. 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 2-34.

Definition: Risk Treatment Plan

2.4.41. 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

2.4.42. 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

2.4.43. 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

2.4.44. 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 2-34.
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

2.5.1. This chapter contains information about developing SSPs.

Template

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

Contents

2.5.3. This chapter contains the following topics.

About SSPs

Definition: System Security Plan

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

- is a means for implementing the ICTSP 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

2.5.5. The purpose of an SSP is to indicate how all the relevant security requirements identified in the ICTSP 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 the system.
See: 'ICTSP contents' on page 2-20.

Development and maintenance

2.5.6. 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

2.5.7. 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

2.5.8. 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, ICTSP, 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

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

Excluded material

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

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

Deleted block

2.6.3. <deleted>

Contents

2.6.4. This chapter contains the following topics.

Developing Security SOPs

Definition: SOPs

2.6.5. 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

2.6.6. 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

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

Agencies **SHOULD** ensure that SOPs are consistent with all relevant SSPs.

See: 'Chapter 5 – Developing an SSP' on page 2-36.

Maintenance

2.6.8. 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 ICT Security' on page 2-72.

Continued on next page

Procedure

2.6.9. 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

2.6.10. 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

2.6.11. 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 ICT 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

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

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

Topic	Procedures that SHOULD be included
System maintenance	Managing the ongoing security and functionality of system software and hardware, including: a. maintaining awareness of current software vulnerabilities, b. applying appropriate hardening techniques, and c. updating anti-virus software.
Hardware destruction	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

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

The table below describes the **minimum** set of 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

2.6.14. 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

2.6.15. 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

2.6.16. 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.
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

2.6.17. Agencies **MUST** provide guidance to users on their responsibilities relating to ICT 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

2.6.18. 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 ICT Systems

Overview

Introduction

2.7.1. This chapter contains information about certifying and accrediting the security of ICT 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

2.7.2. This chapter contains the following sections:

Not included in this chapter

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

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

About Certification and Accreditation

Definition: certification

2.7.4. 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.

Certification Authority

2.7.4.1. The Certification Authority is the entity with the authority to assert that ICT systems comply with the required standards.

Certification to Australian Government standards

2.7.4.2. For the purposes of ICT system certifications to Australian Government standards, agencies may choose which of the last 24 months' releases to be certified against. Certifiers **MUST** identify the chosen release date in the certification report.

Exception: Where the system does not comply with the chosen release but does comply with policy defined in a more recent release without compromising the overall integrity, certification may still be granted. Certifiers **SHOULD** note such exceptions in the certification report.

DSD **RECOMMENDS** that certifiers identify in their certification reports any specific policy requirements defined in the current release that have not been met, in order to assist the agency to prioritise future work.

Reviewing certification reports

2.7.4.3. DSD **RECOMMENDS** that agencies review certification reports, including the chosen release date, when determining the risks associated with connecting to other certified systems.

Example: An agency choosing a service provider to supply gateway services may decide to give preference to a gateway certified against a more recent release.

Continued on next page

What is certified?

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

Note: The degree of assurance provided by a certification may vary depending on who performs the certification; self-certification of gateways and ICT 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.

See: 'Infosec-Registered Assessor Program (I-RAP)' on page 2-77 for information on the Program.

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' in Part E of the *PSM*.
Gateways,	• DSD, • an I-RAP Assessor, or • the ITSA. **See:** 'Gateway Certification' on page 2-51 for more detail.
products approved for Government use listed on the Evaluated Products List (EPL),	DSD. **See:** 'DSD Approved Products' on page 3-21 for more detail.
ICT systems,	the ITSA. **Note:** The ITSA's certification may be based on reviews performed by DSD or an I-RAP Assessor.
Comsec,	• the Comsec Custodian, or • the ITSA.

Continued on next page

Definition: accreditation

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

- processing information classified up to a particular level,
- 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

2.7.7. 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 documentation

2.7.8. DSD **RECOMMENDS** that agencies document all system accreditations.

Requirement for accreditation

2.7.9. Agencies **MUST** accredit all agency systems.

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

Continued on next page

System accreditation: classification

2.7.10.1 Agencies **MUST NOT** allow an ICT system to process, store or transmit information classified above the classification for which the system is accredited.

Exception: If the information is transmitted via intermediate systems in a suitably encrypted form then the intermediate systems do not need to be accredited for the classification.
See: 'Requirements for transit encryption' on page 3-95.

System accreditation: caveats

2.7.11. Agencies **MUST** process, store or transmit information marked with a caveat only on systems that have been accredited for the relevant caveat.

Exception: If the information is transmitted via intermediate systems in a suitably encrypted form then the intermediate systems do not need to be accredited for the caveat.

Examples:
- Suitably encrypted AUSTEO information may be transmitted between two AUSTEO systems via a public network.
- SECRET AUSTEO must not be processed on a TOP SECRET system that has not been accredited to process AUSTEO.

RESTRICTED information on non-national security systems

2.7.13. 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

2.7.14. 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

2.7.16. 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 provides Australian Government agencies with some assurance that their gateway, or their service provider's 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

2.7.17. Gateways, as with all ICT 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 from DSD or I-RAP stating that the gateway environment meets Australian Government policies, standards and guidelines. This form of certification offers a level of independent assurance.

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.

See: 'Infosec-Registered Assessor Program (I-RAP)' on page 2-77 for information on the Program.

Gateway certification standards

2.7.18. All gateways **SHOULD** undergo certification.

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

Continued on next page

Independent gateway certifications

2.7.19. DSD **RECOMMENDS** that independent DSD or I-RAP assessors perform the gateway certifications for agencies developing gateways that:

a. will connect to public networks, or
b. will not connect to public networks, but where the level of risk warrants a certified gateway.

Agencies **SHOULD** ensure that any companies contracted by them to provide gateway services have received a gateway certification from DSD or an I-RAP assessor.

Note: Commercial organisations wishing to provide gateway services should contact DSD to discuss the proposal and to confirm certification arrangements.

Gateway Certification Guide

2.7.21. DSD publishes a separate document, the "*Gateway Certification Guide*", which defines the standards required to meet Australian Government and industry best practice for gateways. All gateway certifications undertaken by DSD and I-RAP assessors are performed against the *Gateway Certification Guide*.

DSD **RECOMMENDS** that agencies certify their gateways against the standards contained in the *Gateway Certification Guide*.

URL: www.dsd.gov.au/library/infosec/gateway.html

Continued on next page

Stages of the certification process

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

Stage	Review the…	To verify…
1	ICTSP,	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 2-36, and • 'Chapter 6 – Developing and Maintaining Security SOPs' on page 2-39.
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?

2.7.23. 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

2.7.24. 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

2.7.25. 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.

Comsec Certification

Definition: Comsec certification

2.7.26. 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

2.7.27. 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

2.7.28. 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

2.7.30. Agencies **SHOULD** undertake the following activities prior to accreditation:

a. develop an RMP,
b. clearly define the controls that need to be put in place, and
c. confirm that all relevant certifications have been provided.
See: 'What is certified?' on page 2-48.

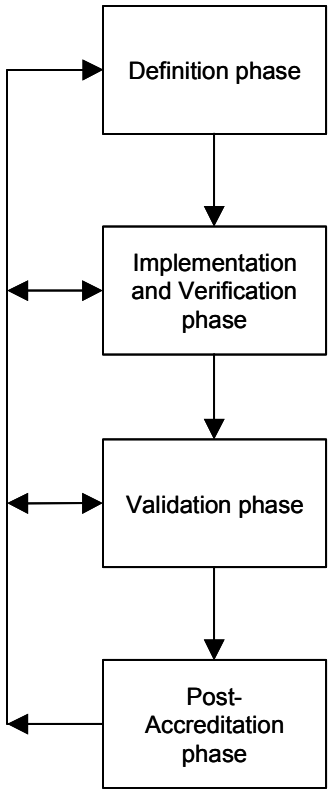
Clarification of policies and standards

2.7.31. 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

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



Continued on next page

Definition phase

2.7.33. 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 2-36.

Implementation and verification phase

2.7.34. 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

2.7.35. 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

2.7.36. 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

2.7.37. 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

2.7.38. 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 ICT Security and Managing Security ' on page 2-59.

Chapter 8 – Maintaining ICT Security and Managing Security Incidents

Overview

Introduction

2.8.1. Maintaining ICT security is an ongoing task. It involves putting into place mechanisms to protect information and system resources. The ICT 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 ICT security?

2.8.2. Information and Communications Technology is continually changing. Methods used to breach ICT security are also continually changing. Once ICT 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 ICT 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

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

Staff who maintain security

2.8.4. Agencies **SHOULD**:

a. clearly define the roles and responsibilities for maintaining ICT security, and
b. provide the resources required to successfully complete such tasks.

Continued on next page

Contents

2.8.5. This chapter contains the following sections.

Managing Change

Identifying the need for change

2.8.6. 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.

Change management standards

2.8.7. Agencies **SHOULD** ensure that:

a. the change management process as defined in the relevant ICT security documentation is followed,
b. the proposed change is approved by the relevant authority,
c. any proposed change that may impact the security of the ICT system is submitted to the Accreditation Authority for approval, and
d. all associated system documentation is updated to reflect the change.

These standards apply equally to urgent changes. The change management process **SHOULD** define appropriate actions to be followed before and after urgent changes are implemented.

Change Management Process

Types of system changes

2.8.9. 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

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

Stage	Who	Description
1	System User, System Manager or ITSA	Produce a written change request.
2		Submit the change request for approval.
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		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 ICT changes. **Example:** Regular security bulletins via electronic mail.

Detecting Security Incidents

Definition: security incident

2.8.11. A security incident, in ICT terms, is an event that impacts on the confidentiality, integrity or availability of a system through an act of unauthorised access, disclosure, modification, misuse, damage, loss or destruction.

Standards

2.8.12. Agencies **MUST** develop, implement and maintain tools and procedures, derived from a risk assessment, covering the detection of potential security incidents, incorporating:

a. countermeasures against malicious code,
   See: 'Standards for malicious code counter-measures' on page 3-49.
b. intrusion detection strategies,
   See: 'Intrusion Detection Systems' on page 3-69.
c. audit analysis,
   See: 'Event Logging' on page 3-71.
d. system integrity checking, and
   See: 'System Integrity' on page 3-76.
e. vulnerability assessments.
   See: 'Vulnerability Analysis' on page 3-77.

In general, resources spent on prevention will be more effective than those spent on detection. Agencies **SHOULD** use the results of the risk assessment to determine the appropriate balance of resources allocated to prevention versus detection.

User awareness

2.8.12.1. Many potential security incidents may be noticed by staff rather than software tools, if agency staff are well-trained and aware of security issues.

See: 'User Training and Awareness' on page 3-16.

Continued on next page

Tools used

2.8.13. The table below describes some software security tools that can be used to detect activity that may indicate a security incident.

DSD **RECOMMENDS** that agencies do not build honeypots or honeynets unless the agency is involved in the research or development of intrusion detection products.

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

2.8.14. 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.

Implementation of tools

2.8.15. It is difficult for a security administrator to keep pace with all current and potential threats to information systems. Appropriately configured and managed software security tools will present a security administrator with more options to mitigate identified risks.

Managing Security Incidents

Incident management documentation

2.8.16. Agencies **MUST** detail security incident responsibilities and procedures for each agency system in the relevant SSP and in SOPs.
See:
- 'Chapter 5 – Developing an SSP' on page 2-36.
- 'Chapter 6 – Developing and Maintaining Security SOPs' on page 2-39.

Agencies **MUST** develop an Incident Response Plan and supporting procedures, and ensure users are aware of these.
See: 'Incident Response Plan' on page 2-70.

Internal reporting

2.8.17. Agencies **MUST** direct staff to report security incidents to the ITSA as soon as possible after the incident is discovered, in accordance with agency procedures.

Standards

2.8.18. Agencies **SHOULD**:

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

Recording incidents

2.8.19. 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 ICT 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

2.8.20. 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 **SHOULD** include the requirement to notify the ITSA of:

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

Agencies **MUST** treat any such spillage as an incident, and follow the Incident Response Plan to deal with it.
See: 'Incident Response Plan' on page 2-70.

Handling malicious code infection

2.8.21. DSD **RECOMMENDS** that agencies follow the steps described in the table below when malicious code is detected.

Note: Once information on the functionality and impact of the malicious code infection is determined, these steps may be adapted to address the particular issues resulting from the incident.

Step	Action
1	Isolate the infected computer or network.
2	Scan all connected systems, and any media used within a set period leading up to the incident, for malicious code. **Note:** Consider the infected date of the machine, and the possibility that the record may be inaccurate, when determining the appropriate period.
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 and perform any other activities required by the incident response plan. **See:** • 'Reporting of incidents' on page 2-68 for information on reporting requirements and additional assistance available from DSD. • 'Incident Response Plan' on page 2-70.

Continued on next page

Allowing continued attacks

2.8.22. 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

2.8.23. 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 ICT evidence is contained in *HB 171:2003 Guidelines for the Management of IT Evidence*.

External Reporting of Security Incidents

Purpose

2.8.24. Reporting security incidents provides a means to assess the overall damage and take remedial action across the Australian Government. Incident reports are the basis for identifying trends in incident occurrences and for developing new policy, procedures, techniques and training measures to prevent the recurrence of similar incidents.

ISIDRAS

2.8.25. 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 ICT systems.

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

Definition: significant

2.8.26. ISIDRAS defines four categories of incidents, of increasing severity. Categories 3 and 4, as defined on the ISIDRAS website, are considered to be "significant".

Reporting of incidents

2.8.27. Agencies, via their ASA or ITSA, **MUST** report significant ICT security incidents to DSD. Other incidents may be reported at agency discretion.

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.

DSD's response will be commensurate with the urgency of the incident; a 24-hour, 7-day service is available if necessary.

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

Incidents and outsourcing

2.8.28. The requirement to lodge an incident report still applies where an agency has outsourced some or all of its ICT functionality.

DSD **RECOMMENDS** that the service provider, in consultation with the agency, lodge the ISIDRAS report on behalf of the agency.

Continued on next page

Cryptographic keying material

2.8.29. Reporting any incident involving the loss or misuse of cryptographic keying material is particularly important.

Agencies **MUST** notify all system users of any suspected loss or compromise of keying material.

Incident Response Plan

Developing the plan

2.8.31. Each agency **MUST** develop an Incident Response Plan which, as a minimum, defines:

a. broad guidelines on what constitutes an incident,
b. the minimum level of training for users and system administrators,
See: 'Training' on page 2-71.
c. the authority 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.

Developing the plan – additional standards

2.8.32. The Incident Response Plan **SHOULD** contain:

a. clear definitions of the types of incidents that are likely to be encountered,
b. the expected response to each incident type,
c. the authority within the agency who is responsible for initiating:
   1) a formal (administrative) investigation,
   2) a police investigation of an incident, and
   3) an ASIO investigation of national security incidents, in accordance with the *PSM*,
d. the criteria by which the responsible authority would initiate formal or police investigations of an incident,
e. references to other related agency policies,
Example: Fraud Control Plan.
f. which other agencies or authorities should be informed in the event of an investigation being undertaken, and
g. the details of the system contingency measures, or a reference to these details if they are located in a separate document.

Definition of incidents

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

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

Continued on next page

Developing the procedures

2.8.34. Agencies **SHOULD** develop and maintain procedures supporting the plan to:

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

Training

2.8.35. 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:

c. management have authorised such changes, and
d. all events are recorded.

Chapter 9 – Reviewing ICT Security

Overview

Introduction

2.9.1. A security review:

- identifies any changes to the business requirements for the subject of the 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

2.9.2. This chapter contains the following sections:

About ICT Security Reviews

When to conduct a review

2.9.3. A review of ICT 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.

Agencies **SHOULD** undertake and document reviews of the security of their ICT systems.

How frequently to review

2.9.4. DSD **RECOMMENDS** that agencies review all aspects of ICT 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: • ICTSP, • 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?

2.9.5. ICT security reviews may be performed by internal staff, or by independent third parties such as:

- an I-RAP assessor, or
- DSD.

See: ‘Infosec-Registered Assessor Program (I-RAP)’ on page 2-77 for information on the Program.

Continued on next page

Audits after reviews

2.9.6. 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 ICT Security

Basis of a review

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

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

Elements of a review

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

Examples:
- A whole-of-agency review might best be approached by a review of each program.
- A review of one particular program could be approached at the division or branch level.
- 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

2.9.9. Depending on the scope and subject of the review, DSD **RECOMMENDS** gathering current information about areas such as:

a. agency priorities,
b. business requirements,
c. threat data,
d. likelihood and consequence estimates,
e. effectiveness of existing countermeasures,
f. other possible countermeasures, and
g. best practice.

Information may be gathered from a range of sources, including:

- the police,
- DSD,
- ITSAs of other similar or related agencies
- publicly available ICT security information sources, and
- system administrators and users.

Rigour of a review

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

Continued on next page

Process

2.9.11. DSD **RECOMMENDS** that agencies follow the core ICT security process with reference to the existing documentation when performing an ICT security review.

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

Infosec-Registered Assessor Program (I-RAP)

Introduction

2.9.12. The Infosec-Registered Assessor Program (I-RAP) is a DSD initiative designed to register suitably qualified information security assessors to carry out specific types of ICT security assessments to Australian Government standards.

The Program has been developed to the Australian Government's strict requirements and is administered by Standards Australia.

URL: http://www.dsd.gov.au/infosec/evaluation_services/irap.html
URL: http://www.irap.standards.com.au

Policy and procedures

2.9.13. The work that the I-RAP Assessors can undertake under the auspices of the program is detailed in the Scope section of the *'Policy and Procedures for the Infosec-Registered Assessor Program (I-RAP)'*.

URL: http://www.irap.standards.com.au/documents/policy.pdf

This page is intentionally blank.

Part 3
ICT Security Standards

Overview

Introduction

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

Contents

3.0.2. This part contains the following chapters:

Chapter 1 – Physical Security

Overview

Introduction

3.1.1. The purpose of this chapter is to:

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

Physical security for Australian sites overseas

3.1.2. 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

3.1.3. This chapter contains the following sections:

Continued on next page

Not included

3.1.4. 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 – Hardware Security’ on page 3-30.
Logical Access Controls	‘Chapter 6 – Logical Access Control’ on page 3-62.
Comsec Standards	‘Chapter 8 – Communications Security (Comsec)’ on page 3-78.
Cabling	‘Cabling' on page 3-80.
Telephones	‘Telephones and Pagers’ on page 3-90.
Personal Electronic Devices (PEDs)	‘Portable Computers and Personal Electronic Devices’ on page 3-45.

Additional references

3.1.5. 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

3.1.6. 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

3.1.7. T4 can be contacted via:

- Phone: (02) 6234 1217
- Fax: (02) 6234 1218
- Email: t4ps@t4.gov.au

T4 Protective Security
GPO Box 2176
Canberra ACT 2601

Contacting T4

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

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

Security Construction and Equipment Committee

3.1.9. 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

3.1.10. 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.

Risk management

3.1.11. Agencies **SHOULD** ensure that site-specific physical security threats are included in their risk management process.

The basics

3.1.12. The basics of the physical security for an ICT 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 area containing the servers and communications equipment are designed to limit access to allow only those with the authorisation and requirement to enter, and to detect those attempting to gain unauthorised access.

Protecting public domain and UN-CLASSIFIED systems

3.1.13. 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

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

Examples:
- portable hard disks,
- DVDs,
- CDs,
- floppy disks,
- tapes,
- smartcards,
- flashcards, and
- thumb drives.

Storage authority

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

The effective classification level of the media may be reduced by the use of appropriate encryption.
See: 'Requirements for storage encryption' on page 3-94.

Storage requirements

3.1.16. The table below is an extract from a table in Part E 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

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

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

Definition: server room

3.1.18. A server room (SR) is a space containing servers and any associated communications equipment.

Separating servers and communication equipment from users

3.1.19. Server rooms **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.

Equipment cabinets and racks

3.1.20. 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

3.1.21. 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.

Definition: No-Lone-Zone

3.1.21.1. A No-Lone-Zone (NLZ) area is an area in which people are not permitted to be left alone. The aim of this is to enforce "two person integrity", where all actions are witnessed by at least one other person.

No-Lone-Zone requirements

3.1.22. DSD **RECOMMENDS** that areas containing sensitive materials and/or equipment be designated and operated as an NLZ area.

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

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

Continued on next page

Compartmentalisation

3.1.23. 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

3.1.24. 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

3.1.25. 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

3.1.26. 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
• public domain • UNCLASSIFIED	**See:** 'Protecting public domain and UN-CLASSIFIED systems' on page 3-5.

SR1 and SR2 standards

3.1.27. T4 has developed guides detailing the physical security standards for server rooms. Agencies may obtain these guides from, and should direct any comments or questions on their contents to, T4.

See: 'ASIO T4 Protective Security' on page 3-4.

Administrative measures

3.1.28. 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 ICT 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 and Network Infrastructure

Area type

3.1.29. 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	Intruder Resistant

Removable hard disks

3.1.30. If removable hard disks are used they **MUST** be:

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

Laptops

3.1.31. Physical security requirements for laptops are covered in Chapter 4 – Hardware Security.

See: 'Portable Computers and Personal Electronic Devices' on page 3-45.

Protecting against theft of equipment

3.1.32. Agencies **SHOULD** implement measures to protect equipment, including internal components, against theft.

Area Security Standards

Area security requirements

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

Preventing observation by unauthorised people

3.1.34. Agencies **SHOULD** prevent unauthorised people from observing ICT 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.
   Further information is available in the 'Curtains and Overlooking' section of the *SEC*.
   See: 'Security Equipment Catalogue' on page 3-4.

Tamper Evident Seals

Approved seals

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

Recording seal usage

3.1.44. 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

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

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

Purchasing seals

3.1.48. 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

3.1.49. 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:

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

Emergency Procedures

Emergency situations

3.1.51. 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 be the first priority at all times.

Chapter 2 – Personnel

Overview

Introduction

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

Contents

3.2.2. This chapter contains the following topics:

Not included

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

Topic	See
ICT Security Roles and Responsibilities	'Chapter 1 – ICT 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 3-62.

Additional references

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

- *PSM*, Part D - Personnel Security
- *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?

3.2.5. 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 – ICT Security Roles and Responsibilities' on page 2-2.

Ensuring that users are security aware can be a relatively cheap and effective method of preventing or minimising the impact of security incidents.

Training responsibility

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

Security education

3.2.7. Agencies **MUST**:

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

Degree and content of security training

3.2.9. 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,
i. the destruction and sanitisation of media and hardcopy output, and
j. how to recognise an anomaly that may indicate a possible security incident.

Continued on next page

Promoting user awareness

3.2.10. DSD **RECOMMENDS** that agencies promote user awareness of ICT 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

3.2.11. 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, • self paced tuition manuals, and • user groups.
ICT users,	• general and specific security requirements, • potential risks and countermeasures, and • system implementation,	• formal in-house courses, • customised training programs, and • external training organisations.

Disclosure of information while on courses

3.2.12. 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

Standards

3.2.13. Agencies **MUST** specify in the SSP the level of security clearance and any briefings required for each type of user given system access/accounts.

Examples:
- privileged users,
- permanent staff,
- contractors, and
- visitors.

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

Deleted block

3.2.14. <deleted, see 3.2.13.>

Responsibilities

3.2.15. 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: Part D of the *PSM*.

Deleted block

3.2.16. <deleted, see 3.6.19.1.>

Clearances for privileged users

3.2.17. 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 – ICT Product Lifecycle

Overview

Introduction

3.3.1. This chapter contains information on selection, acquisition, installation, use and disposal of ICT products.

Contents

3.3.2. This chapter contains the following topics:

DSD Approved Products

Definition: DSD Approved Product

3.3.3. A DSD Approved Product (DAP) is a product that has completed a CC, ITSEC or some other form of DSD approved evaluation (including cryptographic evaluation where appropriate) and has been approved for use by Australian Government agencies, subject to any restrictions contained in this manual and/or the product's listing on the EPL.

Definition: AISEP

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

The AISEP performs the following functions:

- evaluation and certification of ICT 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.

URL: www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep.html

Definition: Protection Profile

3.3.5. A Protection Profile (PP) is an implementation-independent set of security requirements for a category of ICT products that meets specific consumer needs.

Its purpose is to identify the security requirements for a particular product category, without specifying how those requirements are to be implemented. A PP will usually include an Evaluation Assurance Level (EAL) in its stated requirements.

A product may be evaluated against these requirements and, if successful, will be certified as meeting the PP.

DSD-approved PPs

3.3.6. DSD-approved PPs can be used to ensure that security functionality required by Australian Government ICT security policy is included in the formal evaluation process.

Further information on PPs, and the current list of DSD-approved PPs, is available from the AISEP webpages.

Continued on next page

Evaluation level mapping

3.3.7. 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.

This manual 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

3.3.8. 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
- in accordance with Australian Government policy requirements.

Finding DAPs

3.3.9. 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

Standards

3.3.10. 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. Policy stated elsewhere in this manual may specify more rigorous requirements for particular technology types.

See: 'DSD approval of cryptography' on page 3-94 for policy specific to cryptography.

Selecting a DAP

3.3.11. Where products certified as meeting a DSD-approved PP exist, agencies **SHOULD** select these products in preference to products that do not meet an approved PP.
See: 'DSD-approved PPs' on page 3-21.

DSD **RECOMMENDS** that agencies choose DAPs from developers that have 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.

Other options

3.3.12. If agencies cannot find a DAP that meets their needs, agencies **SHOULD** select products in the following order of preference:

a. products that are listed on DSD's EPL as either a Certified Product or as a product currently in evaluation,
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.

Agencies **MUST** acknowledge and accept the risk of using products that are not, and may never be, DAPs.

Continued on next page

Options if selected product isn't listed as a DAP on DSD's EPL

3.3.13. The table below provides some options available to agencies that identify a suitable product that is not listed as a DAP 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, and/or is listed as a Certified Product on DSD's EPL,	discuss with DSD the options for sponsoring the product to become a DAP. **Note:** Before a product is listed as a DAP 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 as a DAP 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

3.3.14. 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, and any caveats contained in the product's entry on DSD's EPL, 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.

Continued on next page

High Grade Equipment	3.3.15. Agencies intending to use High Grade Equipment (HGE) **SHOULD** contact DSD.

Delivery of non-DAPs

3.3.16. 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

3.3.17. 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

3.3.18. Agencies **SHOULD** ensure that leasing agreements for ICT 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

3.3.19. This section discusses the installation, configuration, administration and use of ICT products, including DAPs.

Installing and configuring DAPs

3.3.20. 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

3.3.21. 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 vulnerabilities, and/or
- the environment does not comply with assumptions and/or Organisational Security Policies 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

3.3.22. Agencies **SHOULD** ensure that products are operated and administered in accordance with the user and administrator guidance. This guidance is generally available from the developer.

Agencies **MUST** ensure that High Grade products are configured, operated and administered in accordance with all DSD standards applicable to the product. These standards are usually contained in a separate, product-specific ACSI.

Continued on next page

Patches and hardening products

3.3.23. Agencies **SHOULD** monitor relevant sources for information about new vulnerabilities, patches and hardening methods in software and hardware used by the agency.

Agencies **SHOULD** take corrective action when vulnerabilities that could affect agency systems are discovered. DSD **RECOMMENDS** that agencies perform a risk assessment when determining what action to undertake.
See: 'Use of DAPs in unevaluated configurations' on page 3-27 for policy specific to DAPs.

Agencies **SHOULD** follow the documented change management procedures when applying patches or hardening systems.
See: 'Managing Change' on page 2-61.

Disposing of Products

Secure disposal

3.3.24. It is important to dispose of equipment and media in a manner that does not compromise Australian Government information or capabilities.

See: 'Disposing of Hardware' on page 3-35.

High Grade Equipment

3.3.25. Agencies **MUST** contact DSD for advice on the disposal of HGE.

TEMPEST rated equipment

3.3.26. Agencies **SHOULD**:

a. reuse the equipment within the agency, or
b. offer the equipment to another Australian Government agency for reuse.

Agencies **MUST** contact DSD for advice if:

c. the above are unsuccessful, or
d. the equipment is non-functional.

Deleted block

3.3.27.<deleted, see 3.4.24.>

Chapter 4 – Hardware Security

Overview

Introduction

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

Definition: hardware

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

Definition: media

3.4.3. 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

3.4.4. This chapter contains the following sections:

Not included in this chapter

3.4.5. 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 3-80.

Continued on next page

Additional references

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

- *PSM*, Part C - Information Security, and
- *AS/NZS ISO/IEC 17799:2001*, 8.6 Media handling and security.

Definition: media reclassification

3.4.7. 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

3.4.8. 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

3.4.9. Hardware containing media **MUST** be classified at or above the classification of the media.

Classifying non-volatile media

3.4.10. 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

3.4.12. 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

3.4.13. In general, volatile media may be treated as UNCLASSIFIED once the power is removed from the media.

Continued on next page

Labelling hardware and media

3.4.15. All classified media **MUST** be labelled with the appropriate classification in accordance with Part C of the *PSM*.
Exception: Labels are not required for internally mounted media **if** the hardware containing the media is labelled.

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.

Labelling of High Grade Equipment and High Grade Cryptographic Equipment

3.4.16. In order to maintain their tamper-evident design, HGE **MUST NOT** have any non-essential labels applied to external surfaces.

HGCE **MUST NOT** have **any** labels applied to external surfaces without DSD authorisation.
Important: This overrules any other labelling requirements stated elsewhere within this manual.

Registering media

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

Repairing and Maintaining Hardware

On-site repairs

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

On-site repairs using an uncleared technician

3.4.21. 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]

3.4.22. Agencies may have hardware from UNCLASSIFIED systems repaired off-site at the agency's discretion provided due care is taken to protect official information.

Off-site repairs [IC, R, P]

3.4.22.1. Agencies having hardware from IN-CONFIDENCE, RESTRICTED, or PROTECTED systems repaired off-site **MUST**:

a. use a repair company approved for that purpose by the agency, or
b. use any other company if:
    1) the media within the hardware is sanitised and declassified, or
    2) 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.

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

Disposing of Hardware

Standards

3.4.24. Agencies **MUST NOT** dispose of hardware containing classified information; the hardware must first be sanitised or destroyed using an approved method.

Agencies **SHOULD NOT** dispose of hardware containing information marked as UNCLASSIFIED until it has been authorised for public release.

Approved methods for sanitising and destroying media are contained in this chapter.
See:
- 'Media Sanitisation' on page 3-37.
- 'Media Destruction' on page 3-41.

Occupational Health and Safety (OH&S)

3.4.25. All sanitisation and destruction activities must be undertaken in accordance with any applicable OH&S requirements.

Faulty media and hardware

3.4.26. 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

3.4.28. 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 media? • If yes, then go to step 2. • If no, 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, caveats and owner.
8	Update any relevant documentation and registers.
9	Dispose of the hardware.

Media Sanitisation

Definition: media sanitisation

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

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

See:
- 'Definition: media reclassification' on page 3-32.
- 'Definition: media declassification' on page 3-32.
- 'Definition: media destruction' on page 3-41.

Requirements for sanitising media

3.4.30. 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 undergo 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

3.4.31. 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,
   Note: Includes those that are classed as "re-writable".
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]

3.4.32. 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. **See:** • 'Magnetic media sanitisation products' on page 3-39, • 'Procedure: overwriting magnetic media' on page 3-39, or • 'Degaussers' on page 3-40.
Erasable Programmable ROM (EPROM)	Erase as per the manufacturer's specification, increasing the specified UV erasure time by a factor of three.
Electrically Erasable Programmable ROM (EEPROM)	Erase as per the manufacturer's specification.
Flash memory **Example:** • Memory sticks • Thumb drives	Erase as per the manufacturer's specification, or using a third party tool. Agencies **SHOULD** verify the effectiveness of the erasure process before approving it for use as a sanitisation method. If no effective process is available, then the media **SHOULD** be destroyed. **Note:** Many manufacturers' "erasure" processes merely obscure the data, and tools designed to recover such data are readily available.
Electrostatic memory devices within printers and photocopiers **Examples:** • Laser printer cartridges, • Copier 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 if any classified information has been etched into the surface. If the functionality exists, alter the intensity on a colour-by-colour basis. Destroy the screen if classified information is present.

Continued on next page

Magnetic media sanitisation products

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

See: 'DSD Approved Products' on page 3-21.

Exception: This does not apply to software used to format media in cases where the formatting of media is allowed as a means of sanitisation.

Procedure: overwriting magnetic media

3.4.37. The table below describes the approved procedure for overwriting 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

Step	Action
1	Determine the appropriate value of ***X*** using the table in 'Overwriting procedure: determining *X*' on page 3-40. **If *X* is…** / **Then…** a number / go to step 2. 'F' / format the media. End of procedure. **Important:** Do **not** use a 'quick' format method.
2	• 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.
3	Do the following ***X*** times: • overwrite the entire media with ***C***, then • overwrite the entire media with ***-C***. **Example:** If ***X*** equals 0 (zero) then this step is skipped, however, if ***X*** equals 2 then the sequence would be ***C***, ***-C, C***, ***-C***.
4	Overwrite the entire media with random data.

Continued on next page

Overwriting procedure: determining *X*

3.4.38. 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.

Important: If the media is to be disposed of in an uncontrolled manner, such as at a public auction or thrown in the garbage, then the public domain (PD) column is to be used to determine the value of ***X***.

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

Degaussers

3.4.39. When sanitising with a degausser, agencies **MUST** use a degausser of sufficient field strength for the coercivity of the media being sanitised.
Important: Coercivity varies between media types, and between brands and models of the same type. Care is needed when determining the required coercivity as a degausser of insufficient strength will not be effective.

The degaussers listed on the National Security Agency's *Degausser Products List* are deemed to be DSD Approved Products for the purposes of this manual.
URL: www.nsa.gov/ia/government/mdg.cfm

Agencies using a product on NSA's list **MUST** comply with the directions provided within the list by NSA.
Note: Agencies are advised to consult DSD where these directions appear to conflict with policy within this manual.

Media Destruction

Definition: media destruction

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

To destroy media effectively, only the actual material within which the data is stored requires destruction.
Examples: The metal casing of a hard disk platter and the plastic substrate of a CD do not need to be destroyed.

Media destruction requirements

3.4.43. Agencies **MUST** destroy **unsanitised** classified media prior to disposal in accordance with the table below.

Reasons for not sanitising media include:

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

See: 'Disposal process' on page 3-36.

Media type	Destruction required? IC, R, P
Electrostatic memory devices within printers and photocopiers. **Examples:** • laser printer cartridges, • photocopier drums.	No
Magnetic and optical media. **Examples:** • floppy disks, • hard disks, • tapes, • CDs.	Yes
Non-volatile semi-conductor memory.	Yes
Volatile semi-conductor memory.	No(1)

(1) No destruction required once all power supplies, including batteries, are removed.

Continued on next page

Media destruction methods

3.4.44. To destroy media, agencies **MUST**:

a. break up the media, or
b. heat the media until it has either burnt to ash or melted.

Agencies **SHOULD** use the methods shown in the table below, and employ equipment approved by the SCEC for the purpose.
See: 'Security Equipment Catalogue' on page 3-4.

Item	Methods				
	Furnace/ incinerator	**Hammer mill**(1)	**Dis-integrator**(1)	**Grinder/ sander**(1)	**Cut**(1)
Electrostatic memory devices within printers and photocopiers	Y	Y	Y	Y	-
Floppy disk	Y	Y	Y	-	Y
Hard disk	Y	Y	Y	Y	-
Optical disk	Y	Y	Y	Y	Y
Semi-conductor memory	Y	Y	Y	-	-
Tape	Y	Y	Y	-	Y

(1) The size of the particles resulting from the application of this destruction method **MUST** be appropriate for the intended waste handling and storage procedures, with respect to the media's initial classification.
See: 'Media waste particles – storage and handling' on page 3-43.

Supervision

3.4.45. Agencies **MUST** perform the destruction of classified material under the supervision of an officer cleared to the highest level of media being destroyed.

The officer **MUST**:

a. supervise the handling of the material to the point of destruction, and
b. ensure that the destruction is complete.

Continued on next page

Supervision for accountable material

3.4.46. Agencies **MUST** perform the destruction of accountable material, as defined in Part C of the *PSM*, under the supervision of two officers cleared to the highest level of media being destroyed.

The officers **MUST**:

a. supervise the handling of the material to the point of destruction,
b. ensure that the destruction is complete, and
c. sign a destruction certificate.

Media waste particles – storage and handling [IC, R, P]

3.4.47. When the media is reduced to particles able to pass through a screen of the specified aperture, the resulting waste may be stored and handled as for the classification given in the table below.

Important: This table affects the storage and handling requirements only; it does not reduce the requirement for complete destruction prior to disposal. However, if the resulting classification is given as "U", then the requirement for complete destruction has been met, and the particles may be disposed of.
See: 'Media disposal' on page 3-43.

If the initial classification is…	**Then, with a screen of this aperture, waste can be stored and handled as for…**	
	<= 9mm	**<= 12mm**
IN-CONFIDENCE	U	U
RESTRICTED	U	U
PROTECTED	U	IC

Media disposal

3.4.49. Agencies disposing of classified media **MUST** ensure that the recording media has been:

a. burnt to ash,
b. melted, or
c. reduced to a particle size that meets the requirements for UNCLASSIFIED storage and handling based on the media's **initial** classification.

Agencies **SHOULD** dispose of UNCLASSIFIED media waste in a manner that does not attract undue attention to it.

Continued on next page

Further advice

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

See: ‘Contact details’ on page 3-4.

Portable Computers and Personal Electronic Devices

Introduction

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

Definition: PED

3.4.52. For the purposes of this manual, PEDs are defined as portable devices that can process, store 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

3.4.53. PEDs include, but are not limited to:

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

Related topics

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

Topic	See
Telephones and pagers	'Telephones and Pagers' on page 3-90.
Physical security standards	'Chapter 1 – Physical Security' on page 3-2.
Cryptography	'Chapter 9 – Cryptography' on page 3-93.
Wireless communications	'Wireless Communications' on page 3-85.

Certification and accreditation

3.4.55. For the purposes of certification and accreditation, portable computers and PEDS may be considered to form part of an ICT system either individually or grouped by functional requirements.

See: 'Chapter 7 – Certifying and Accrediting ICT Systems' on page 2-46.

Unaccredited devices

3.4.56. Agencies **SHOULD NOT** allow unaccredited portable computers and PEDs to connect to agency ICT systems or store official information.

Continued on next page

Storage and handling

3.4.57. Agencies **MUST** protect portable computers and PEDs storing classified information to at least the same level as hardcopy material of the same classification, in accordance with the *PSM* requirements for access, storage and handling.
Exception: Some storage and handling requirements may be reduced by the use of encryption products.
See: 'Requirements for storage encryption' on page 3-94.

DSD **RECOMMENDS** that agencies encrypt data on all portable computers and PEDs.

Even UNCLASSIFIED portable computers and PEDs have some intrinsic value and therefore require protection against theft.
See: 'Protecting public domain and UNCLASSIFIED systems' on page 3-5.

Operation

3.4.58. Portable computers and PEDs containing classified information **SHOULD** be:

a. operated in physically protected areas classed as intruder resistant or better,
b. kept under continual, direct supervision when in use, and
c. stored in physically protected areas appropriate for that classification when not in use.

See: 'Chapter 1 – Physical Security' on page 3-2.

Device configuration

3.4.59. If intending to use portable computers or PEDs to process classified information, agencies **SHOULD** ensure that all data collection and communications functions of the devices not identified as business requirements are removed or disabled as effectively as possible within the limitations of the particular device.
Examples: Bluetooth, infrared, cameras, microphones.

See: 'Product Selection**'** on page 3-23 for information on selecting products.

Continued on next page

Labelling portable computers and PEDs

3.4.60. Agencies **SHOULD** put a protective marking 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

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

See: 'Emergency Procedures' on page 3-14 for more information.

Chapter 5 – Software Security

Overview

Introduction

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

Types of software

3.5.2. Software includes:

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

Software security standards

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

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

Contents

3.5.4. This chapter contains the following sections:

Not included in this chapter

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

Topic	See
Security Incidents	'Chapter 8 – Maintaining ICT Security and Managing Security Incidents' on page 2-59.
Physical Security	'Chapter 1 – Physical Security' on page 3-2.
Access Control	'Chapter 6 – Logical Access Control' on page 3-62.
Auditing	'Intrusion Detection Systems' on page 3-69.
Networks	'Chapter 10 – Network Security' on page 3-110.

Malicious Code and Anti-Virus Software

Definition: malicious code

3.5.6. 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

3.5.7. 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.

Standards for malicious code counter-measures

3.5.8. 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),
b. make their users aware of the agency's policies, plans and procedures
c. <deleted, see 3.5.9.1.>
d. <deleted>, and
e. ensure that all instances of detected malicious code outbreaks are handled according to the procedures.

See: 'Chapter 8 – Maintaining ICT Security and Managing Security Incidents' on page 2-59.

Deleted block

3.5.9. <deleted, see 3.5.9.1-4.>

Continued on next page

Anti-virus scanners

3.5.9.1. DSD **RECOMMENDS** that agencies, for all servers and workstations:

a. install agency-approved anti-virus scanners,
b. ensure that users do not have the ability to disable the scanner,
c. regularly update virus signatures, and
d. regularly scan all disks.

See: 'Data import from a less classified system' on page 3-121 for mandatory malicious code countermeasures required when transferring data.

Host based intrusion prevention systems

3.5.9.2. DSD **RECOMMENDS** that agencies install host-based intrusion prevention systems (HIPS) on high risk servers.

Integrity checking

3.5.9.3. DSD **RECOMMENDS** that agencies use checksums to detect unauthorised modifications to files identified as being of particular importance, with the checksum database held offline.

Active content blocking

3.5.9.4. DSD **RECOMMENDS** that agencies use:

a. filters to block:
   1) unwanted content, and
   2) exploits against applications that cannot be patched,
b. settings within the applications to disable unwanted functionality, and
c. digital signatures to restrict active content to trusted sources only.

Containment and recovery

3.5.10. 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

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

See: 'Handling malicious code infection' on page 2-66.

Database Security

Data labelling

3.5.12. Agencies **SHOULD** label all database records with the appropriate protective marking 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

3.5.14. Agencies **SHOULD** protect database files from access that bypasses the database's normal access controls.

Deleted block

3.5.16. <deleted>

Deleted block

3.5.17. <deleted>

Accountability

3.5.18. Agencies **SHOULD** ensure that databases provide accountability of users' actions.

See: 'Chapter 6 – Logical Access Control' on page 3-62.

Search engines

3.5.19. Agencies **SHOULD** ensure that users who do not have sufficient clearance to access a file cannot see the file title in a list of results from a search engine query.

If this requirement is not met, then agencies **MUST** ensure that all file titles are appropriately sanitised to meet the minimum security clearance of system users.

Web Application Security

Why have web security controls?

3.5.20. 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.

Web usage policy

3.5.20.1. Agencies that allow staff to browse the Internet **MUST** have a policy governing web use.

Applying controls

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

Example: Client browsers.

Components of a web application

3.5.22. 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

3.5.23. 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.

Continued on next page

Cookies

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

Applications and plug-ins

3.5.25. 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.

Agencies **SHOULD** block the automatic launching of files downloaded from external websites.

Client-side active content

3.5.26. 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

3.5.27. 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

3.5.28. 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

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

Continued on next page

Auditing and access control

3.5.30. 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

Why have email security controls?

3.5.31. 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

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

Components of email system

3.5.33. 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 3-49.

Server auditing

3.5.34. 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: ‘Event logs for software components’ on page 3-73.

Web-based email services

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

Continued on next page

Automatic forwarding of received emails

3.5.36. Agencies **MUST** ensure that the standards for blocking unmarked and outbound emails are also applied to automatically forwarded emails.
See:
- 'Blocking of unmarked emails' on page 3-60.
- 'Blocking of outbound emails' on page 3-60.

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.

Centralised email gateway

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

Email security documentation standards

3.5.39. 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 message,
   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.

See: 'Electronic Mail – Protective Marking Policy' on page 3-58 for standards relating to the protective marking policy for email.

Continued on next page

Email technical standards

3.5.40. Agencies **SHOULD:**

a. harden and patch email servers and clients,
b. restrict access to email servers to administrative users,
c. <deleted, see 3.5.40.1.>
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,
f. disable open mail relaying so that mail servers will only relay messages destined for the agency's domain(s) and those originating from within the domain, and
g. ensure that account names cannot be determined from external mail servers.

Technical standards for blocking emails

3.5.40.1. Agencies **SHOULD** block:

a. inbound and outbound email, including any attachments, that contain:
   1) malicious code,
   2) content in conflict with the agency's email policy, and
   3) content that cannot be identified by the system,
b. emails addressed to internal email aliases with source addresses located from outside the domain, and
c. all emails arriving via an external connection where the source address uses an internal agency domain name.

See: 'Blocking of unmarked emails', 'Blocking of outbound emails', and 'Blocking of inbound emails' on page 3-60 for further standards on blocking emails based on their protective markings.

Electronic Mail – Protective Marking Policy

Marking classified emails

3.5.41. Agencies **MUST** ensure that all agency-originated emails that contain security classified information are marked with a protective marking that identifies the maximum classification and set of caveats for the information in the body of the email and any attachments.

Exception: Emails generated automatically by ICT systems **SHOULD** be marked with an appropriate protective marking.

Marking unclassified emails [U, IC, R]

3.5.42. Agencies **SHOULD** ensure that all agency-originated emails that do not contain any classified information are marked with an appropriate protective marking such as UNCLASSIFIED or PERSONAL.

Marking unclassified emails [P]

3.5.43. Agencies **MUST** ensure that all agency-originated emails that do not contain any classified information are marked with an appropriate protective marking such as UNCLASSIFIED or PERSONAL.

Marking tools

3.5.44.1 Agencies **SHOULD NOT** allow a protective marking to be inserted into user-generated emails without user intervention.

If an agency provides a tool that allows users to select from a list of protective markings, then the list **SHOULD NOT** include protective markings for which the system is not accredited.

Personal emails

3.5.45. DSD **RECOMMENDS** that agencies advise staff to mark emails that do not contain any official information with a label such as PERSONAL rather than UNCLASSIFIED.

Note: For the purpose of this policy, such markings are considered to be a form of protective marking.

Protective marking standard

3.5.46. The standard for the application of protective markings to emails will be promulgated separately once it has been finalised.

Continued on next page

Dealing with emails from outside of the Australian Government

3.5.47. DSD **RECOMMENDS** that agencies:

a. encourage external organisations that send email to the agency to adopt the protective marking system described in this policy, and/or
b. mark emails that originated from outside of the Australian Government as UNCLASSIFIED, unless the email is already marked.
   Important: The automatic marking of emails as UNCLASSIFIED, even if from a source outside of the Australian Government, creates the risk that an email will be marked as UNCLASSIFIED yet contain sensitive, and possibly classified, information.

Note: This allows agency systems to handle the email in accordance with the protective marking.

Marking emails from outside of the Australian Government

3.5.48. The following only applies if an agency decides to mark emails that originated from sources outside of the Australian Government as UNCLASSIFIED.

Agencies **SHOULD** perform the marking on:

a. a per-sender basis, or
   Example: mark as UNCLASSIFIED all emails from person@company.com
b. a per-domain/organisation basis.
   Example: mark as UNCLASSIFIED all emails from organisation.org

Note: DSD **RECOMMENDS** the former.

Agencies **SHOULD** perform the marking at the point at which the email enters the agency's system.
Note: This ensures that all copies of the email within the agency will be marked the same.

DSD **RECOMMENDS** that emails that have been marked automatically be identifiable to the reader.
Example: A message could be added to the start of the email such as "Note: This email was not from an Australian Government source and has been automatically marked as UNCLASSIFIED."

Checking emails for a protective marking

3.5.49. Agencies **SHOULD** ensure that the protective marking is used as the basis for any decisions to permit or block the email.

Continued on next page

Blocking of unmarked emails

3.5.50. Agencies **SHOULD** prevent staff from sending unmarked emails by blocking the email at:

a. the user's computer, and/or
b. the email server.

Blocking of outbound emails

3.5.51. Agencies **MUST** configure systems to block any outbound emails with a valid protective marking indicating that the content of the email exceeds the classification of the:

a. receiving system, and/or
b. the path over which the email would be transferred.
   Note: This may need to take into consideration any encryption applied to the email.

Agencies **SHOULD** log the fact the emails were blocked.

DSD **RECOMMENDS** that the sender be notified of the blocked email.

Blocking of inbound emails

3.5.52. Agencies **SHOULD** configure email systems to reject and log inbound emails with protective markings indicating that the content of the email exceeds the accreditation of the receiving system.

DSD **RECOMMENDS** that the intended recipient be notified of the blocked email.

Printing

3.5.53. DSD **RECOMMENDS** that agencies configure systems so that the protective marking appears at the top and bottom of every page when the email is printed.

Software Development

Introduction

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

Software development environments

3.5.55. Agencies **SHOULD** ensure that software development environments are configured such that:

a. there are 3 ICT environments:
   1) development,
   2) testing, and
   3) production,
b. information flow between the environments is strictly limited according to a defined and documented policy, with access granted only to users with a clear business requirement,
c. new development and modifications only take place in the development environment, and
d. write-access to vendor's distribution media or integrity copies of operational software is disabled.

Software testing

3.5.57. 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

3.5.58. 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

3.6.1. This chapter contains information on logical access control.

Documentation

3.6.2. 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

3.6.3. This chapter contains the following sections:

Not included

3.6.4. 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 10 – Network Security' on page 3-110.

Additional references

3.6.5. Additional information relating to access control is also contained in the AS/NZS ISO/IEC 17799:2001, 9 Access Control.

User Identification and Authentication

Standards

3.6.6. Agencies **MUST** ensure that all users of classified systems are:

a. uniquely identifiable, and
b. authenticated on each occasion that access is granted to the system.

DSD **RECOMMENDS** that all users of UNCLASSIFIED systems be:

c. uniquely identifiable, and
d. authenticated on each occasion that access is granted to the system.

Methods for user identification and authentication

3.6.9. User authentication can be achieved by various means, including:

- passwords,
- passphrases,
- cryptographic tokens,
- smartcards, and
- biometrics.

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

Agencies **MUST NOT** use a numerical password (often defined as a Personal Identification Number (PIN)) as the sole method of authorising a user to access a classified system.

Protecting authentication information

3.6.9.1. Agencies **MUST NOT** allow staff to store unprotected authentication information that grants access to a system, or decrypts an encrypted data storage device, on or with the system or device to which the authentication information grants access.

Password selection

3.6.11. 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: !@#$%^&*

Continued on next page

Password management

3.6.13. 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,
d. force the user to change an expired password on initial logon or if reset, and
e. **NOT** allow passwords to be reused within 8 password changes.

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.

Screen and session locking

3.6.15. Agencies **SHOULD:**

a. configure systems with a screen and/or session lock,
b. configure the lock to activate after no more than 15 minutes of user inactivity,
c. configure the lock to completely conceal all information on the screen,
d. **NOT** permit the screen to appear to be turned off while the session is still active,
e. require the user to reauthenticate before the system is unlocked, and
f. **NOT** permit users to disable the locking mechanism.

Displaying when a user last logged in

3.6.17. 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 [U, IC, R, P]

3.6.18. Agencies **SHOULD**:

a. lock user accounts after a specified number of failed logon attempts,
b. remove or suspend user accounts as soon as possible after the user no longer requires access due to changing roles or leaving the agency, and
c. suspend inactive accounts after a specified number of days.

DSD **RECOMMENDS** that:

d. a limit of 3 failed logon attempts be permitted, and
e. account resets can only be performed by an administrator.

Privileged and System Accounts

Definition: privileged access

3.6.19.1. 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.

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

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

Use of privileged accounts

3.6.20. Agencies **SHOULD**:

a. ensure that the use of privileged accounts is controlled and accountable,
   Example: UNIX administrators login using their own userid and then 'sudo' to perform privileged actions.
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

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

Group accounts

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

If agencies choose to allow non-user-specific accounts, agencies **MUST** ensure that some other method of determining the identification of the user is implemented.

Access and Authorisation

Standards

3.6.30. 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.

Logon banner

3.6.30.1. Agencies **SHOULD** have a logon banner that requires a user response before access to a system is granted. DSD **RECOMMENDS** seeking legal advice on the exact wording of the banner.

The banner may cover issues such as:

- access being permitted to authorised users only,
- the user's agreement to abide by relevant security policies,
- the user's awareness of the possibility that system usage is being monitored,
- the definition of acceptable use for the system, and
- legal ramifications of violating the relevant policies.

Definition: access control list

3.6.34. 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.

Continued on next page

Developing an ACL

3.6.35. 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.

Example of an access control matrix

3.6.36. 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 mgr	**Payroll database** Data owner = Payroll mgr	**Personnel drive** Data owner = Registry mgr	**Forms database** Data owner = Registry mgr
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 – Active Security

Overview

Introduction

3.7.1. Active security is the capability to predict, detect, and respond to anomalous ICT activity. These capabilities include processes and tools such as Intrusion Detection Systems (IDSs), event logging, audit analysis, system integrity checking and vulnerability analysis.

Contents

3.7.2. This chapter contains the following topics:

Intrusion Detection Systems

Definition: intrusion detection system

3.7.2.1. An intrusion detection system (IDS) is a system designed to detect inappropriate or malicious activity occurring on a network or host by analysing the activity for suspicious patterns and anomalies.

Intrusion detection strategy

3.7.3. Agencies **SHOULD** define and implement an intrusion detection strategy, based on the results of a risk assessment, that includes:

a. appropriate intrusion detection mechanisms, including network-based IDS (NIDS) and host-based IDS (HIDS) as required,
b. the audit analysis of event logs, including IDS logs,
c. a periodic audit of IDS procedures,
d. user training and awareness programs, and
See: 'User Training and Awareness' on page 3-16.
e. a documented incident response procedure.
See: 'Incident Response Plan' on page 2-70.

Event management and correlation

3.7.3.1. DSD **RECOMMENDS** that agencies deploy tools for:

a. the management and archival of security event information, and
b. the correlation of events of interest across all agency networks.

Additional references

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

- 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

3.7.5. Agencies **SHOULD** deploy IDSs in all gateways between the agency's networks and the Internet. DSD **RECOMMENDS** that an IDS be located within the gateway environment, immediately inside the outermost firewall.

When signature-based intrusion detection is used, agencies **SHOULD** keep the signatures up to date.

Continued on next page

IDSs on other gateways

3.7.6. DSD **RECOMMENDS** that agencies deploy intrusion detection systems at all gateways between the agency's networks and any network not managed by the agency.

When signature-based intrusion detection is used, agencies **SHOULD** keep the signatures up to date.

Configuring the IDS

3.7.6.1. In addition to agency-defined configuration requirements, DSD **RECOMMENDS** that an IDS located inside a firewall be configured to generate a log entry, and an alert if desired, for any information flows that contravene any rule within the firewall ruleset.

Example: If the firewall is configured to block all traffic on a particular range of port numbers, then the IDS should inspect traffic for these port numbers and alert if they are detected.

Event Logging

Logging requirements

3.7.7. Agencies **MUST** develop and document logging requirements reflecting the overall audit objectives derived from the ICTSP and RMP, covering:

a. the logging facility, including:
   1) log server availability requirements, and
   2) the reliable delivery of log information to the log server,
b. the minimum list of events associated with a system or software component to be logged, and
c. event log protection and archival requirements.
d. <deleted, see 3.7.16.1.>
e. <deleted, see 3.7.16.1.>

Event log facility

3.7.8. For each logged event, the log facility **MUST**, at a **minimum**, record the following information, where applicable:

a. date and time of the event,
b. relevant user(s) or process,
c. event description,
d. success or failure of the event,
e. event source (e.g. application name), and
f. terminal location/identification.

See: 'Event logs for software components' on page 3-73.

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

Continued on next page

Event log protection and archival

3.7.9. Event logs **MUST** be:

a. protected from modification and unauthorised access,
   Note: DSD **RECOMMENDS** that systems be configured to save event logs to a separate, secure log server.
b. archived using a well-documented procedure and retained for future access, and
   Note: DSD **RECOMMENDS** archiving event log data onto write-once media.
c. protected from whole or partial loss within the defined retention period.

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

Deleted block

3.7.10 <deleted, see 3.7.16>

Deleted block

3.7.11. <deleted, see 3.7.17.1.>

Continued on next page

Event logs for software components

3.7.12. 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 log 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, • addition of new users, especially privileged users, • 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

3.7.13. 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.
   Important: The retention of user logs may be subject to the *Archives Act 1983*.

System management log information

3.7.14. A system management log **SHOULD** be manually updated to record the following information:

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.

System management logs [U, IC, R, P]

3.7.14.1. DSD **RECOMMENDS** that agencies maintain system management logs for the life of the system.

Auditing

Purpose

3.7.15.1. The purpose of auditing is to assist in the detection and attribution of any violations of agency security policy, including security breaches and intrusions. The frequency, depth and specific objectives of audit analyses, derived from the ICTSP and the RMP, may be unique to each system.

Responsibilities

3.7.16. Agencies **SHOULD NOT** assign system audit responsibilities to system administrators.

The ITSA **SHOULD** be responsible for managing and auditing the event logs.

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 ICTSP and RMP.

Audit requirements

3.7.16.1. Agencies **MUST** develop and document audit requirements reflecting the overall audit objectives derived from the ICTSP and RMP, covering:

a. the scope of audits,
b. the audit schedule,
c. action to be taken when violations are detected,
d. reporting requirements, and
e. specific responsibilities.

How to audit an event log

3.7.17. The table below describes the steps **RECOMMENDED** by DSD for the audit analysis of an event log.

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

Resources

3.7.17.1. Agencies **SHOULD** ensure that a sufficient number of appropriately trained personnel and tools are available to analyse all logs for potential violations of agency security policy.

System Integrity

About system integrity

3.7.18. System integrity mechanisms are designed 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 3-69 and 'Malicious Code and Anti-Virus Software' on page 3-49.

System integrity checks

3.7.19. 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 (DACAs)' on page 3-96.

System changes

3.7.20. 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 Analysis

Vulnerability analysis strategy

3.7.21. Agencies **SHOULD** implement a vulnerability analysis strategy by:

a. monitoring public domain information about new vulnerabilities in operating systems and application software,
b. considering the use of automated tools to perform vulnerability assessments on agency systems in a controlled manner,
c. running manual checks against system configurations to ensure only allowed services are active and that disallowed services are prevented, and
   Example: "Netstat" commands to check the status of open sessions against the configuration parameters.
d. using security checklists for operating systems and common applications.

Authorisation

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

When to perform

3.7.23. 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.

DSD **RECOMMENDS** that agencies perform the analysis at a time that minimises possible disruptions to agency systems.

Resolving vulnerabilities

3.7.24. Agencies **SHOULD** analyse and treat any risks to its systems identified during a vulnerability analysis.
See: 'Chapter 4 – Risk Management' on page 2-23.

Agencies **SHOULD** follow the change process when implementing changes to mitigate the risks.
See: 'Change Management Process' on page 2-62.

In some cases, a vulnerability may have been introduced as a result of poor security practices, or accidental or malicious activities. DSD **RECOMMENDS** that agencies consider this when investigating and resolving vulnerabilities.
See: 'Managing Security Incidents' on page 2-65.

Chapter 8 – Communications Security (Comsec)

Overview

Introduction

3.8.1. This chapter contains information about communications security (Comsec) standards.

DSD advice

3.8.2. Contact DSD for further information regarding all Comsec issues.

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

Contents

3.8.3. This chapter contains the following topics:

Not included

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

Topic	See page
Comsec Certification	2-55
Chapter 9 – Cryptography	3-93

About Comsec

Definition: Comsec

3.8.5. Comsec is the measures and controls taken to:

- deny unauthorised persons access to 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

3.8.7. 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)*
- AS/NZS 3080:2000 *Telecommunications installations - Generic cabling for commercial premises*

Cable Distribution Systems

Introduction

3.8.13. This topic discusses cable distribution systems. It contains information on:

- important definitions,
- types of conduit,
- standards for conduit that penetrates walls,
- sealing conduit,
- suspending conduit, and
- connecting conduit to equipment cabinets.

What are cable distribution systems?

3.8.14. 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

3.8.15. Conduit is a tube, duct, or pipe used to protect cables from tampering, sabotage or accidental damage.

Cables sharing a common conduit

3.8.16. The table below shows the combinations of cable classifications that are approved by DSD to share a common conduit.

Agencies **MUST NOT** deviate from the approved combination(s).

Group	Approved combination
1.	any combination of: • public domain, • UNCLASSIFIED, • IN-CONFIDENCE, • PROTECTED, • HIGHLY PROTECTED, and • RESTRICTED.

Continued on next page

Fibre optic cables sharing a common conduit

3.8.18. With optical fibre cables, the cable's protective sheath can be considered to be a conduit and therefore the fibres within the sheath **MUST** only carry a single Group.
See: 'Cables sharing a common conduit' on page 3-81.

If a cable contains subunits, as shown in Figure 4, then each subunit **MUST** only carry a single Group, however each subunit within the cable may carry a different Group.

Example: The cable shown in Figure 4 could carry UNCLASSIFIED and HIGHLY PROTECTED in one subunit and CONFIDENTIAL and SECRET in another subunit.

The diagrams below represent a sample of fibre cross-sections.

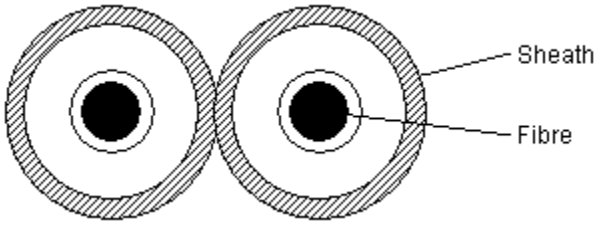


Figure 1

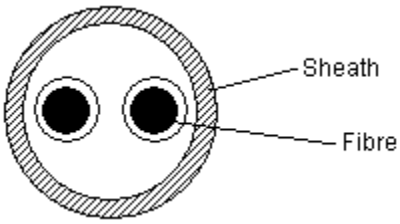


Figure 2

Continued on next page

Fibre optic cables sharing a common conduit (continued)

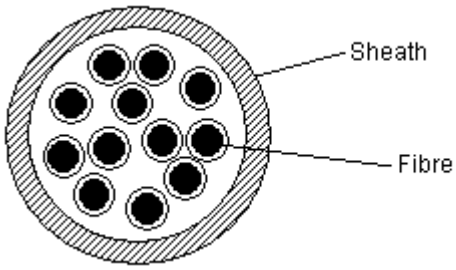


Figure 3

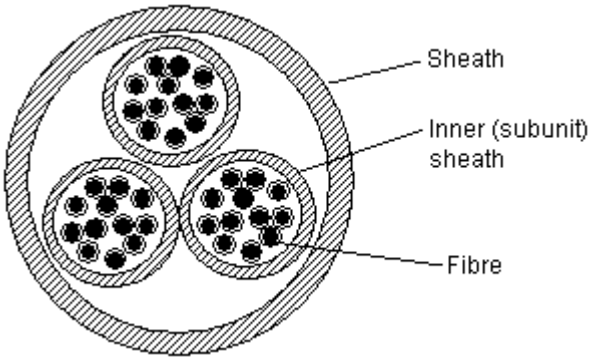


Figure 4

Labelling and Registration

Installing conduit labelling

3.8.27. 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

3.8.29. Site conventions for labelling and registration **SHOULD** be recorded in the SOPs.

Cable register

3.8.31. 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

3.8.33. 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.

Wireless Communications

Introduction

3.8.41. Some examples of wireless communications technologies and protocols include:

- IEEE 802.11,
- Bluetooth,
- Infrared,
- General Packet Radio Service (GPRS),
- Global System for Mobile communications (GSM),
- Code Division Multiple Access (CDMA),
- Multimedia Messaging Service (MMS), and
- Short Message Service (SMS).

Not included

3.8.42. This section does not contain information on the following topics:

Topic	See page
Policy and standards specific to mobile and cordless telephones	3-90

Standards

3.8.43. Agencies **SHOULD NOT** use wireless communications for the transmission of classified information.

Agencies **MUST**, where they have a requirement to use wireless communications for the transmission of classified information, ensure that the information is protected by DSD Approved Cryptography that meets the assurance level required for the transmission of the information over public domain networks.
See: 'DSD approval of cryptography' on page 3-94.

Pointing devices

3.8.45. Agencies may use wireless pointing devices.

Examples: Mice and track balls.

Telephone Systems

Use of telephone systems for the transmission of classified information [IC, R]

3.8.48. Agencies intending to use their telephone systems for the transmission of IN-CONFIDENCE or RESTRICTED information **MUST** ensure that:

a. the system has been accredited for the purpose, including the completion of a risk assessment and formal acceptance of the residual risks, **and either**
b. the sender and receiver are both located within Australia, **or**
c. all traffic that passes over external systems such as the PSTN or the Internet is encrypted in accordance with the level of encryption required for the classification of the information being transmitted.
See: 'Requirements for transit encryption' on page 3-95.

Use of telephone systems for the transmission of classified information [P]

3.8.49. Agencies intending to use their telephone systems for the transmission of PROTECTED information **MUST** ensure that:

a. the system has been accredited for the purpose, including the completion of a risk assessment and formal acceptance of the residual risks, and
b. all traffic that passes over external systems such as the PSTN or the Internet is encrypted in accordance with the level of encryption required for PROTECTED information.
See: 'Requirements for transit encryption' on page 3-95.

Emergency services

3.8.51. DSD **RECOMMENDS** that agencies route calls to emergency services (e.g. 000) through the local Private Branch Exchange (PBX).

IP Telephony

Definition: IP Telephony

3.8.52. IP Telephony (IPT) is the transport of telephone calls over Internet Protocol (IP) networks. It may also be referred to as Voice Over IP (VOIP) or Internet Telephony.

Standards

3.8.53. Agencies **MUST** ensure that IPT networks meet:

a. all the standards defined in this manual for a generic system of equal classification, as well as any relevant caveats,
b. the standards for generic telephone systems, and
   See: 'Telephone Systems' on page 3-86.
c. the standards for telephones.
   See: 'Telephones and Pagers' on page 3-90.

Gateways [U, IC, R, P]

3.8.54.1. Where the gateway requires a firewall, agencies **SHOULD** use a firewall capable of understanding the telephony protocols in use within the agency.

See: 'Gateways' on page 3-114.

Connection to the PSTN

3.8.55. Agencies **MUST** install a firewall of sufficient assurance between the agency's IP network and the voice gateway that converts the IPT traffic into a form suitable for connection to the PSTN.
See: 'Firewalls' on page 3-116.
Note: The PSTN is to be regarded as a public network for the purposes of determining the required level of assurance.

This firewall **MUST** be configured to permit only the IPT traffic through the interface that connects to the PSTN.

Network separation

3.8.55.1. Agencies **MUST NOT** run an IPT network over the same physical medium as a data network of a different classification.

Traffic separation [U, IC, R, P]

3.8.56. DSD **RECOMMENDS** that agencies separate the IPT traffic from other data traffic, either physically or logically.

Continued on next page

Infrastructure hardening [U, IC, R, P]

3.8.57. DSD **RECOMMENDS** that agencies harden all IPT components and networking devices.
Examples: IP PBX, databases, web servers, and phones.

Agencies **SHOULD NOT** run non-IPT applications on servers used for IPT services.

Call authentication and authorisation

3.8.58. Agencies **SHOULD** route calls via a call controller for authentication and authorisation before calls can be established.

Vendor recommendations

3.8.59. Agencies **SHOULD** implement all relevant security measures recommended by the vendor of the IPT products.

Note: In the event of conflict, statements within this manual have precedence over vendor recommendations.

IP phones

3.8.59.1. DSD **RECOMMENDS** that agencies use IP phones implementing signalling and media encryption.

IP phone set up [U, IC, R, P]

3.8.59.2. Agencies **SHOULD:**

a. configure IP phones to authenticate themselves to the call controller upon registration, and
b. disable auto-registration of IP phones after initial rollout.

DSD **RECOMMENDS** that agencies:

c. activate only the handset port and the phone port, and
d. do not connect workstations to IP phones.
   Note: If an agency does choose to connect workstations to IP phones, then DSD **RECOMMENDS** that agencies configure the IP phones to use VLANs to separate the IPT traffic from other data.

Securing IP phone firmware upgrades

3.8.59.4. Agencies **MUST** ensure that firmware updates are performed in a manner that verifies the integrity and authenticity of the process.

Continued on next page

Definition: softphone	3.8.59.5. A softphone is a software application that allows a computing device, such as a desktop computer, to act as an IP phone, using either a built-in or an externally connected microphone and speaker. It may also be known as a software IP phone.
Softphone standards [U, IC, R, P]	3.8.59.6. Agencies **SHOULD NOT** use software phones. If an agency deviates from this standard, then DSD **RECOMMENDS** that the agency have a separate, dedicated Network Interface Card (NIC) on the host for voice network access.

Telephones and Pagers

Definition: telephone

3.8.60. Within this section, "telephone" is used to describe a device that allows voice communications to be sent electronically over a distance.

Examples:
- standard, wired handsets,
- cordless phones,
- mobile phones,
- stand-alone VOIP handsets, and
- computer-based VOIP "softphones".

Use of telephones near classified conversations

3.8.61. Agencies **SHOULD** ensure that staff are aware of the audio risk posed by using telephones in areas where classified conversations may occur.

Definition: Off-hook audio protection

3.8.61.1. Off-hook audio protection mitigates the possibility of an active, but temporarily unattended handset inadvertently allowing discussions being undertaken in the vicinity of the handset to be heard by the remote party.

This may be achieved through the use of a hold feature, mute feature, push-to-talk handset, or equivalent.

Definition: Push-to-Talk

3.8.62. Push-To-Talk (PTT) handsets have a button which must be pressed by the user before audio can be transmitted, thus providing fail-safe off-hook audio protection.

Requirement for off-hook audio protection [P]

3.8.63. DSD **RECOMMENDS** that off-hook audio protection feature(s) are used on all telephones that are not accredited for the transmission of PROTECTED data in areas where PROTECTED information may be discussed.

Continued on next page

Cordless and mobile telephones [IC]

3.8.68. Agencies **SHOULD NOT** use cordless or mobile telephones for the transmission of IN-CONFIDENCE information **unless**:

a. the security they use has been approved by DSD, or
   See: 'Chapter 9 – Cryptography' on page 3-93 and 'DSD Approved Products' on page 3-21.
b. they can ensure that:
   1) the cordless or mobile phone user is located within Australia, and
   2) only voice traffic is passed.

Cordless and mobile telephones [R, P]

3.8.69. Agencies **MUST NOT** use cordless or mobile telephones for the transmission of RESTRICTED or PROTECTED information unless the security they use has been approved by DSD.

See: 'Chapter 9 – Cryptography' on page 3-93 and 'DSD Approved Products' on page 3-21.

Cordless telephones with Secure Telephony Devices

3.8.71. Agencies **MUST NOT** use cordless telephones in conjunction with Secure Telephony Devices such as Speakeasy.

Paging services

3.8.72. Agencies **MUST NOT** use paging services to transmit classified information.

Note: This includes Multimedia Messaging Service (MMS) and Short Message Service (SMS).

Facsimile Machines

Definition: facsimile machine

3.8.73. Within this topic, the term "facsimile machine" is used to describe a device that allows copies of documents to be sent over a telephone system.

Examples:

- Stand-alone fax machines.
- "Multifunction devices" capable of, among other things, the sending and receiving of faxes.
  See: 'Multifunction Devices' on page 3-128 for additional policies and standards.
- Computers equipped with fax processing cards.

Use for the transmission of classified information

3.8.74. Agencies intending to use facsimile machines for the transmission of classified information **MUST** ensure that:

a. all of the standards for the use of telephone systems are met at both ends for the level of classification to be sent, and
   See: 'Telephone Systems' on page 3-86.
b. the sender makes arrangements for the receiver to:
   1) collect the information from the facsimile machine as soon as possible after it is received, and
   2) notify the sender if the facsimile does not arrive within an agreed amount of time.
      Note: DSD **RECOMMENDS** that this be no longer than 10 minutes.

Chapter 9 – Cryptography

Overview

Introduction

3.9.1. This chapter contains information on cryptography.

Purpose of cryptography

3.9.2. Cryptography can be used to provide:

- confidentiality,
- integrity,
- authentication, and
- non-repudiation.

Contents

3.9.3. This chapter contains the following topics:

Cryptographic Requirements

DSD approval of cryptography

3.9.4. Agencies using cryptography to protect classified information and systems **MUST** use cryptography:

a. approved by DSD for the purpose, and
b. in accordance with the standards in this section.

Note: DSD will not, with the exception of DACPs, generally approve cryptographic functionality within products that have not been through the AISEP or a CCRA scheme.

Requirements for storage encryption

3.9.5. Agencies **MUST** use encryption products or protocols that meet the minimum level of assurance as shown in the following table if they wish to use encryption to reduce the physical handling requirements for media that contains classified information.

Note: The use of approved encryption will generally reduce the likelihood of an unauthorised party gaining access to the encrypted information. However, it does not reduce the consequences of a successful attack.

Important: Care must be taken with encryption systems that do not encrypt the entire media content to ensure that either all of the classified data is encrypted or that the media is handled in accordance with the highest classification of the unencrypted data.

If the classification of the unencrypted information is…	**Then media holding information encrypted by a product or protocol with the given assurance level may be stored and handled as for…**						
	Unapproved/ no encryption	**DACP**	**EAL1**	**EAL2**	**EAL3**	**EAL4**	**HG**
IC	IC	U	U	U	U	U	U
R	R	R	R	U	U	U	U
P	P	IC	IC	U	U	U	U

Continued on next page

Requirements for transit encryption [IC, R, P]

3.9.6. 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 DACP.
RESTRICTED,	• public domain, or • UNCLASSIFIED,	EAL2.
	• IN-CONFIDENCE, • PROTECTED, or • HIGHLY PROTECTED,	a DACP.
PROTECTED,	• public domain, or • UNCLASSIFIED,	EAL2.
	IN-CONFIDENCE,	a DACP.

DSD Approved Cryptographic Algorithms (DACAs)

Introduction

3.9.10. This section explains the cryptographic algorithms that DSD has approved for the protection of classified information. There are three types of algorithms:

- asymmetric/public key algorithms,
- hashing algorithms, and
- symmetric encryption algorithms.

Important: The fact that a product or protocol uses one or more DSD Approved Cryptographic Algorithms (DACAs) does not automatically mean that it is "DSD Approved."

Asymmetric/ public key algorithms

3.9.11. 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.	The modulus **MUST** be at least 1024 bits.	FIPS 186.
Elliptic Curve Diffie-Hellman (ECDH)	Agreeing on encryption session keys.	The field/key size **MUST** be at least 160 bits.	• ANSI X9.63 • ANSI X9.42
Elliptic Curve Digital Signature Algorithm (ECDSA)	Digital signatures.	The field/key size **MUST** be at least 160 bits.	• FIPS PUB 186-2 + Change Notice • ANSI X9.63 • ANSI X9.62
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

3.9.12. The table below identifies the approved hashing algorithms, and one or more references for each of the algorithms.

Note: DSD **RECOMMENDS** the SHA family of hashing algorithms.

Algorithm	Reference(s)
Message Digest v5 (MD5)	• AS 2805.13.3 • RFC 1321
Secure Hashing Algorithms (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	• AS 2805.13.3 • FIPS 180-2

Symmetric encryption algorithms

3.9.13. The table below identifies the approved symmetric encryption algorithms, their conditions of use and one or more references.

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, 192 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 (DACPs)

Approved protocols

3.9.14. In general, DSD only approves the use of cryptographic products that have passed a formal evaluation. However, DSD approves 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 the guidelines in this manual.

Before using DACPs

3.9.15. Before using an unevaluated product that implements a DSD Approved Cryptographic Protocol (DACP), agencies **MUST**:

a. investigate DAPs, and systems such as Fedlink, that provide greater security assurance,
b. ensure that the minimum requirements as stated in the 'Cryptographic Requirements' section on page 3-94 will be met, and
c. consider the risks.

Some risk considerations

3.9.16. It is possible that there are security flaws in the DACPs or in the products that implement them. This possibility should be taken into account when deciding whether to use a DACP.

If a product implementing a DACP has been inappropriately configured, it is possible that relatively weak cryptographic algorithms may be selected without the user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of risk.

While many DACPs support authentication, agencies should be aware that these authentication mechanisms are not foolproof. To be effective, these mechanisms must also be securely implemented and protected.

This can be achieved:

- by providing an assurance of private key protection,
- by ensuring the correct management of certificate authentication processes including certificate revocation checking, and
- through the use of a legitimate identity registration scheme.

Continued on next page

Implementing DACPs

3.9.17. When using an unevaluated product that implements a DACP, agencies **MUST** ensure that only DACAs can be used.

Agencies could achieve this by:

- disabling the unapproved algorithms within the products (preferred), or
- advising users not to use them via a policy.

See: 'DSD Approved Cryptographic Algorithms (DACAs)' on page 3-96.

Links

3.9.18. The table below lists the DACPs and provides links to the relevant standards.

Protocol	See page
Secure Sockets Layer and Transport Layer Security (SSL/TLS)	3-100
Secure Shell (SSH)	3-101
Secure Multipurpose Internet Mail Extension (S/MIME)	3-103

Secure Sockets Layer and Transport Layer Security (SSL/TLS)

Introduction

3.9.19. DSD approves the use of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for encryption only when configured and implemented in accordance with the standards provided below.

Risk considerations

3.9.20. SSL and TLS do **not** protect data during storage. As a result, there is usually a greater risk that data will be accessed while stored at either end of the communication path, where SSL/TLS does not protect it.

Standards

3.9.21. Agencies **SHOULD NOT** use versions of SSL prior to version 3.0.
Note: TLS is newer than SSL version 3.0.

Agencies **MUST** ensure that the standards for the use of DACPs are met.
See: 'DSD Approved Cryptographic Protocols (DACPs)' on page 3-98.

Secure Shell (SSH)

What is Secure Shell?

3.9.22. 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

3.9.23. Secure Copy (SCP) and Secure FTP (SFTP) use SSH and are therefore also covered by this section.

Standards

3.9.24. Agencies **MUST** ensure that the standards for the use of DACPs are met.
See: 'DSD Approved Cryptographic Protocols (DACPs)' on page 3-98.

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
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

3.9.25. 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

3.9.26. Agencies **SHOULD NOT** use "ssh-agent" or other similar key caching programs.

Secure Multipurpose Internet Mail Extension (S/MIME)

Introduction

3.9.27. DSD has approved the use of Secure Multipurpose Internet Mail Extension (S/MIME) for the confidentiality and integrity of message content only when implemented in accordance with the standards provided below.

Risk considerations

3.9.28. Agencies choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and any attachments for inappropriate content, and for server-based anti-virus software to scan for viruses and other malicious code.

Standards

3.9.29. Agencies **SHOULD NOT** allow versions of S/MIME earlier than 3.0 to be used.

Agencies **MUST** ensure that the standards for the use of DACPs are met.
See: 'DSD Approved Cryptographic Protocols (DACPs)' on page 3-98.

Agencies **SHOULD:**

a. install anti-virus scanners on user workstations, and
b. ensure that the signatures are regularly updated.

See: 'Malicious Code and Anti-Virus Software' on page 3-49.

FIPS 140

What is FIPS 140?

3.9.30. The Federal Information Processing Standard (FIPS) 140 is a United States standard for the validation of cryptographic modules, both hardware and software.

URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

What FIPS 140 is not

3.9.31. FIPS 140 is **not** a substitute for the evaluation of ICT 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.

Versions of FIPS 140

3.9.32. FIPS 140 is in its second iteration and is formally referred to as FIPS 140-2. This policy refers to the standard as FIPS 140 but applies to both FIPS 140-1 and FIPS 140-2.

Cryptographic evaluations

3.9.33. Cryptographic evaluations of products will normally be conducted by DSD. Where a product's cryptographic functionality has been validated under FIPS 140, DSD may, at its discretion and in consultation with the vendor, reduce the scope of a DSD cryptographic evaluation.

DSD will review the FIPS 140 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.

Approved algorithms

3.9.34. 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

3.9.35. 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

3.9.36. The table below provides additional references.

Grade of cryptography	Reference
commercial grade	AS 11770.1-2003 *Information technology – Security techniques – Key management.*

Definition: cryptographic system

3.9.38. 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

3.9.39. Cryptographic system material includes, but is not limited to, key, equipment, devices, documents, and firmware or software that embodies or describes cryptographic logic.

Cryptographic system requirements

3.9.40. In general, the requirements specified for ICT 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 manual.

Continued on next page

Cryptographic system administrator access

3.9.41. 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,
See: 'Definition: Key Management Plan' on page 3-107.
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

3.9.42. 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

3.9.43. 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

3.9.44. 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:

d. to check all cryptographic system material as per the accounting documentation, and
e. 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

3.9.45. 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 used **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

3.9.46. 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

3.9.47. 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

3.9.48. Agencies **SHOULD** develop a KMP where they have implemented a cryptographic system in hardware or software.

Continued on next page

KMP contents

3.9.50. 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.

Continued on next page

KMP contents (continued)

Topic	Content
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.
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.

Chapter 10 – Network Security

Overview

Introduction

3.10.1. This chapter contains information on network security.

Contents

3.10.2. This chapter contains the following topics:

Not included

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

Additional references

3.10.4. Additional information relating to network security is also contained in the AS/NZS ISO/IEC 17799:2001:

- 8.5 Network Management, and
- 9.4 Network access control.

Deleted block 3.10.5. <deleted, see 3.6.6, 3.10.15.>

Configuration management

3.10.6. 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 to the documented configuration.

Deleted block 3.10.8. <deleted>

Internetwork Connections

Internetwork connections

3.10.9. Internetwork policies and standards act to prevent and monitor unintended information flow, and/or access.

Internetwork security standards

3.10.10. Agencies **SHOULD** ensure that:

a. the information flow over the connection is consistent with the ICTSPs for all relevant networks,
b. the use of the connection is limited to authorised users,
c. all users are advised of their responsibilities and held accountable for their actions in relation to the connection and the connected networks,
d. all users operate over the connection within the limits of their required rights and privileges,
e. <deleted>,
f. <deleted>, and
g. <deleted>.

Determining the classification of other networks

3.10.10.1. Agencies **MUST** determine the effective classification of other networks before implementing an internetwork connection.

If the other network is not under the agency's control, then agencies **SHOULD:**

a. obtain certification and accreditation details from the network owner, and
b. review the details to determine the appropriate classification of the network, and any additional security controls required to effectively manage the connection.

If no details are available, or the details cannot be effectively mapped to the standards of this manual, then agencies **SHOULD** treat the other network as if it were public domain.

Definition: cascaded connections

3.10.11. Cascaded connections occur when one network is connected to another, which has a connection to a third network, and so on.

Continued on next page

Risk of undesirable cascaded connections

3.10.12. When intending to connect an agency network to another network, agencies **SHOULD:**

a. request a list of networks to which the other network is connected from the other network's:
   1) Accreditation Authority, and
   2) System Manager,
b. examine the information from both sources to determine if any unintended cascaded connections exist, and
c. consider the risks associated with any identified cascaded connections prior to connecting the agency network to the other network.

Gateways

Definition: gateway

3.10.13. A gateway is a secured connection between two networks.

Gateways usually consist of a number of items of computer equipment including:

- firewalls,
- proxy servers,
- routers, and
- email servers.

Definition: one-way gateway

3.10.14. One-way gateways 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.

Gateway standards

3.10.15. Agencies **MUST** ensure that:

a. all agency networks are protected from other networks by gateways, and
b. the device used to control the data flow meets the relevant standards.
   See: 'Firewalls' on page 3-116 for bi-directional gateways, and 'Diodes' on page 3-119 if the data flow is only in one direction.
c. the data flow is controlled in accordance with the relevant standards
   See: 'Data Transfer' on page 3-120.

Agencies **SHOULD** ensure that gateways:

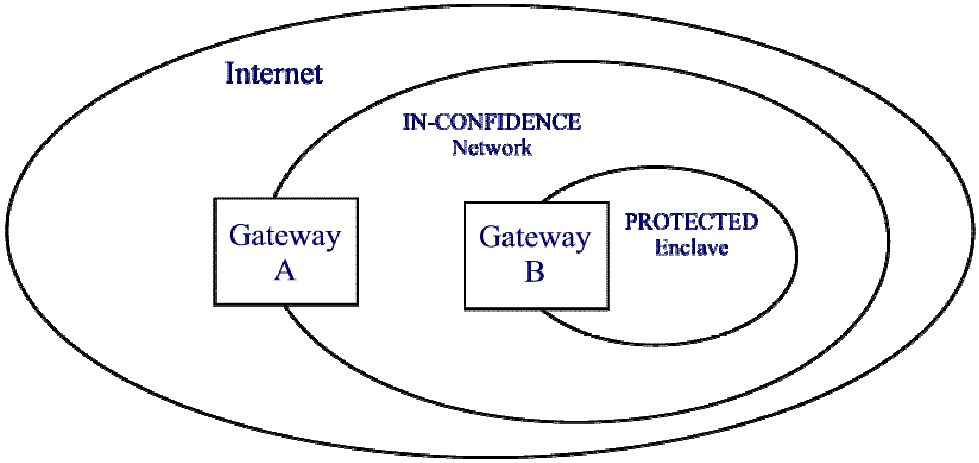
d. are the only communications routes into and out of internal networks,
e. by default, deny all connections into and out of the network,
f. allow only explicitly authorised connections,
g. are managed via a secure path,
h. provide sufficient audit capability to detect gateway security breaches and attempted network intrusions, and
i. provide real-time alarms.

Continued on next page

Cascaded connections

3.10.19. Agencies **MUST** ensure that the combination of the devices protecting the path linking the most highly classified network to the least classified network meets the minimum assurance requirement of a direct connection between the two.

Example: An agency has an IN-CONFIDENCE internal network with a gateway to the Internet, labelled as Gateway A in the diagram below. Within the internal network is a PROTECTED enclave, protected by Gateway B. Gateway A requires an EAL2 firewall as a minimum. Gateway B requires an EAL3 firewall as a minimum. However, a direct connection between the enclave and the Internet would require an EAL4 firewall, therefore a firewall of this assurance level must be located at either Gateway A or Gateway B.



See:

- 'Definition: cascaded connections' on page 3-112.
- 'Firewalls' on page 3-116.
- 'Diodes' on page 3-119.

Demilitarised Zones

3.10.20. 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.

Firewalls

Definition: firewall

3.10.21. A firewall is a network device that filters incoming and outgoing network data, based on a series of rules.

Definition: traffic flow filter

3.10.22. A traffic flow filter is a device configured to filter and control the flow of data.

Selecting a traffic flow filter

3.10.23. When selecting a traffic flow filter, agencies **SHOULD** use one or more of the following, with the order of preference as shown:

1. A firewall listed as a DAP.
   See: 'Selecting a DAP' on page 3-23.
2. A firewall or proxy that is not a DAP.
   See: 'Other options' on page 3-23.
3. A router with appropriate access control lists configured.

Continued on next page

Firewall assurance levels [U, IC, R, P]

3.10.24. Agencies **MUST** use devices that meet the minimum level of assurance as shown in the following table.

See:

- 'Selecting a traffic flow filter' on page 3-116 if, according to the table, your gateway requires a traffic flow filter.
- 'Interconnecting networks within an agency' on page 3-118 for exceptions relating to networks managed by the same agency.

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, • UNCLASSIFIED,	an EAL2 firewall.
	• 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.

Continued on next page

Interconnecting networks within an agency

3.10.28. If the networks connected by the gateway are managed by the same agency then a firewall is not mandatory for the protection of:

- the less classified of the networks, or,
  Note: the requirements for the protection of the more highly classified network from the less classified networks must still be met.
- either network if the networks are of the same classification.

In these situations, DSD **RECOMMENDS** that agencies use at least a traffic flow filter.

Diodes

Definition: diode	3.10.29. A device that allows data to flow in only one direction.
Content and volume checks	3.10.30. Agencies deploying a diode to control data flow within a one-way gateway **SHOULD** monitor the content and volume of the data being transferred to ensure that it conforms to expectations.
Assurance requirements [PD, U, IC, R, P]	3.10.31. For controlling the data flow of one-way gateways where the classifications of the interconnected networks are no higher than PROTECTED or RESTRICTED, agencies **SHOULD** use a diode with some level of formal assurance.

Data Transfer

Introduction

3.10.34. This topic contains information about securing the transfer of data between systems. Unless stated otherwise, these requirements apply to all methods of transferring data, including:

- bi-directional gateways using a firewall,
- one-way gateways using a diode,
- manual procedures that use software applications to check the data on a media item during transfer, and
- manual procedures that rely on a human to review the data.

Transfer authorisation [U, IC, R, P, HP]

3.10.34.1. Agencies **SHOULD** ensure that data transfers are either:

a. individually approved by the ITSA, or
b. performed in accordance with processes and/or procedures approved by the Accreditation Authority.

Media

3.10.34.3. Agencies transferring data manually **SHOULD** use a:

a. previously unused piece of media, or
b. 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.

Deleted block

3.10.35. <deleted>

Definition: filter

3.10.36. A filter controls the flow of data in accordance with a security policy.

Examples: Email content scanners and "dirty word" checkers.

Filtering standards [U, IC, R, P]

3.10.37. Agencies **SHOULD** deploy filters on all data transfer points between systems of different classifications and/or caveats.

Deleted block

3.10.38. <deleted, see 3.10.38.1 to 3.10.41.1.>

Continued on next page

Filtering techniques

3.10.38.1. The table below identifies some common filtering techniques used to control data transfer.

Technique	Purpose
Anti-virus scan	Scans the data for viruses and other malicious code.
Data format check	Inspects the format of the data to ensure that it conforms with expected/permitted format(s).
Data range check	Checks the data within each field to ensure that it falls within the expected/permitted range.
Data type check	Inspects each file to determine its file type.
File extension check	Checks file extensions to ensure that they are permitted. **Examples:** .txt, .doc, .jpg, .pdf.
Keyword search	Searches the data for keywords or "dirty words" that may indicate the presence of classified or inappropriate material.
Metadata check	Inspects files for metadata that should be removed prior to release. **Examples:** revision history, userids and directory paths.
Protective marking check	Validates the protective marking of the data to ensure that it complies with the permitted classifications and caveats.
Visual inspection	Manually inspects the data for issues that an automated system may miss; particularly important for the transfer of image files.

Data export to a less classified system [IC, R, P]

3.10.39. Agencies **SHOULD** restrict the transfer of data to a less classified system by filtering data using at least:

a. protective marking checks.

Data import from a less classified system

3.10.40.2. Agencies **SHOULD** scan for malicious and active content.

Continued on next page

User responsibilities

3.10.41.1. Agencies **SHOULD** ensure that users:

a. are held accountable for the data they transfer, and
b. prior to initiating the data transfer, perform a:
   1) protective marking check,
   2) visual inspection, and
   3) metadata check, if relevant.

Remote Access

Definition: remote access

3.10.42. Remote access is any access to an agency system from a location not within the physical control of that agency. This includes access to devices such as routers, firewalls and IPT components.

Standards [U]

3.10.42.1. Agencies allowing users remote access to UNCLASSIFIED systems **SHOULD** ensure that:

a. users are authenticated on each occasion that access is granted to the system,
b. users are given the minimum system access necessary to perform their duties, and
c. data relating to any actions requiring the use of privileged access is protected during transmission as for IN-CONFIDENCE.
See: 'Requirements for transit encryption [IC, R, P]' on page 3-95.

Standards for classified systems

3.10.43. 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 remote users cannot view or download information that exceeds the classification of the remote user's system, and
d. any data transferred is appropriately protected during transmission and at the remote user's end.
See:
- 'Chapter 1 – Physical Security' on page 3-2.
- 'Cryptographic Requirements' on page 3-94.

Virtual Private Networks

Virtual Private Networks	3.10.44-47. <deleted>

Peripheral Switches

Definition: peripheral switch

3.10.48. 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

3.10.49. 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

Virtual LANs

Introduction

3.10.51. Many Layer 2 switches can provide a Virtual LAN (VLAN) capability that allows:

- multiple Layer 3 networks to exist separately on a switch, and
- a network of computers to behave as if they are connected to the same wire even though they may actually be physically located on different segments of the LAN.

Important: The VLAN capability within switches is not designed to enforce security and a number of vulnerabilities have been documented that may allow traffic to pass between the VLANs.

Connectivity standards

3.10.52. The table below represents the connectivity standards for VLANs sharing a common switch.

Exception: VLANs may be used to separate IP telephony traffic.
See: 'IP Telephony' on page 3-87.

Key:

Where the entry in the following table is a(n)…	The standard is…
A	DSD does **NOT RECOMMEND**
B	Agencies **SHOULD NOT**
C	Agencies **MUST NOT**

	PD	**U**	**IC**	**R**	**P**
PD	A	B	C	C	C
U	B	A	B	C	C
IC	C	B	A	B	B
R	C	C	B	A	C
P	C	C	B	C	A

Continued on next page

Configuration and administration standards

3.10.53. Administrative access **MUST** only be permitted from the most highly classified network or, for networks of the same classification, the most trusted network as determined by the Accreditation Authority.

Staff with administrative access or unsupervised physical access to the switch **MUST** have a security clearance of at least the classification of the highest classified network carried on the switch.

The physical security of the switch **MUST** meet the requirements for the highest classified network carried on the switch.

Agencies **SHOULD** implement all security measures recommended by the vendor of the switch.
Note: If any of the recommendations conflict with this manual then this manual has precedence.

Unused ports on the switches **SHOULD** be disabled.

Trunking

3.10.55. Using a technique known as trunking, a VLAN may exist across two or more connected switches.

This capability **MUST NOT** be used on switches managing VLANs of differing classifications.

Multifunction Devices

Definition: multifunction devices

3.10.56. Within this manual, 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.

See:
- 'Telephone Systems' on page 3-86, and
- 'Facsimile Machines' on page 3-92.

Risks with MFDs

3.10.57. 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 [IC, R, P]

3.10.58. MFDs **SHOULD NOT** have their facsimile functionality enabled unless the telephone network is accredited to at least the same classification as the computer network.

Policies, plans and procedures

3.10.60. 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
AGAO	Australian Government Access Only
AGD	Attorney-General's Department
AISEP	Australasian Information Security Evaluation Program
AS/NZS	Australian Standard/New Zealand Standard
ASA	Agency Security Adviser
AUSTEO	Australian Eyes Only
CC	Common Criteria
CDMA	Code Division Multiple Access
CR	Certification Report
CCRA	Common Criteria Recognition Arrangement
DACA	DSD Approved Cryptographic Algorithm
DACP	DSD Approved Cryptographic Protocol
DAP	DSD Approved Product
DMZ	Demilitarised Zone
DSD	Defence Signals Directorate
EACS	Electronic Access Control System
EAL	Evaluation Assurance Level
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
EPL	Evaluated Products List
FIPS	Federal Information Processing Standard
GPRS	Global Packet Radio Service
GSM	Global System for Mobile communications
HGCE	High Grade Cryptographic Equipment
HGE	High Grade Equipment
I-RAP	Infosec-Registered Assessor Program
ICT	Information and Communications Technology
IDS	Intrusion Detection System
ICTSP	Information and Communications Technology Security Policy
IP	Internet Protocol
IPT	Internet Protocol Telephony
IR	Infrared
ISIDRAS	Information Security Incident Detection, Reporting and Analysis Scheme
IT	Information Technology
ITSA	Information Technology Security Adviser
ITSEC	Information Technology Security Evaluation Criteria
KMP	Key Management Plan
KVM	Keyboard/Video/Mouse
MFD	Multifunction Device
MMS	Multimedia Messaging Service

Continued on next page

NLZ	No-Lone-Zone
PBX	Private Branch Exchange
PD	Public Domain
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PM&C	Department of Prime Minister and Cabinet
PP	Protection Profile
PROM	Programmable Read-Only Memory
PSM	*Protective Security Manual*
PSPC	Protective Security Policy Committee
PSTN	Public Switched Telephone Network
PTT	Push-To-Talk
RF	Radio Frequency
RMP	Risk Management Plan
ROM	Read-Only Memory
S/MIME	Secure Multipurpose Internet Mail Extension
SAS	Security Alarm System
SCEC	Security Construction and Equipment Committee
SEC	Security Equipment Catalogue
SIC	SECURITY-IN-CONFIDENCE
SMS	Short Messaging Service
SOP	Standard Operating Procedure
SR	Server Room
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Plan
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSCM	Technical Surveillance Counter Measures
VOIP	Voice Over Internet Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Glossary

IMPORTANT	This glossary is included for quick reference and does **not** replace *ACSI 1(B) - Information Systems Security Glossary*.
Accreditation	The formal acknowledgement of the Accreditation Authority's decision to approve the operation of a particular ICT system.
Accreditation Authority	The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.
AGAO	Australian Government Access Only (AGAO) is a caveat used by the Department of Defence and ASIO. The *Inter-Agency Security Supplement to the Commonwealth Protective Security Manual* states that AGAO material received in other agencies must be handled as if it were marked AUSTEO.
AISEP	The Australasian Information Security Evaluation Program (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.
Audit	An independent review of ICT event logs and related activities performed to determine the adequacy of current system measures, to identify the degree of conformance with established policy, and/or to develop recommendations for improvements to the measures currently applied.
AUSTEO	Australian Eyes Only (AUSTEO) is a caveat indicating that the information is not to be passed to or accessed by foreign nationals.
Caveat	A marking that indicates that the information has special requirements in addition to those indicated by the classification. The term covers codewords, source codewords, releasability indicators and special-handling caveats.
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.

Continued on next page

Certification Report	The Certification Report contains the findings of the certification for a system, site or product. For products evaluated under the Common Criteria or ITSEC, the Certification Report 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	An ISO standard (ISO 15408) for ICT security evaluations. The purpose of the Common Criteria is to ensure that ICT security evaluations world-wide are: • performed against a common set of requirements, and • that the security claims are expressed unambiguously. **URL:** http://www.commoncriteriaportal.org/
Common Criteria Recognition Arrangement	A mutual recognition arrangement for Common Criteria evaluations among a group of participating countries, including Australia and New Zealand.
Comsec	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.
Communica-tions security	**See:** Comsec.
Control	A measure that is taken to mitigate risks.
Control register	A document used in the RMP to record the controls required for a site.

Continued on next page

Controlled space	A controlled space, as defined in *ACSI 61*, is the three dimensional space surrounding equipment or facilities that process classified information within which: • unauthorised personnel are denied unrestricted access, and • positive measures are taken to control the movement of personnel and materials including vehicles.
Counter-measure	**See:** Control.
Cryptographic hash	An algorithm (the hash function) which takes as input a string of any length (the message), and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest.
Cryptographic system	A related set of hardware and/or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.
Cryptography	The art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.
Cryptoperiod	The time span during which each key setting remains in effect.
DAP	A DSD Approved Product (DAP) is a product that has completed a Common Criteria, ITSEC or some other form of DSD approved evaluation (including cryptographic evaluation where appropriate) and has been approved for use by Australian Government agencies, subject to any restrictions contained in this manual and/or the product's listing on the EPL.
Declassifi-cation, 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.

Continued on next page

Degaussing	The process of applying a magnetic force to remove information from media.
Destruction, media	The process of physically damaging the media with the objective of making the data stored on it inaccessible.
Diode	A device that allows data to flow in only one direction.
DMZ	A Demilitarised zone (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.
DSD Approved Product	**See:** DAP.
EAL	The Evaluation Assurance Level (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.
Emanation security	Emanation security includes, but is not limited to, consideration of: • audio, • visual, • infrared, and • electromagnetic emissions. TEMPEST security is a subset of emanation security.
Encryption	The art or science concerning the principles, means, and methods for rendering plain information unintelligible.

Continued on next page

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	**See:** EAL.
Firewall	A network device that filters incoming and outgoing network data, based on a series of rules.
Foreign national	A person who is not an Australian citizen.
Foreign system	An ICT system that is not solely owned and managed by the Australian Government. **Note:** A foreign system could be located within Australia.
Gateway	A secured connection between two networks. A gateway will usually consist a number of items of computer equipment including: • a firewall host, • proxy servers, • routers, and • email hosts.
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 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.

Continued on next page

Hardware	The physical components of computer equipment including peripheral equipment. **Examples:** • personal computers, • mainframe computers, • laptops, • printers, • routers, • personal digital assistants (PDAs), and • mobile phones.
High Grade	An evaluation level in excess of the defined Common Criteria evaluation levels.
High Grade Cryptographic Equipment	Cryptographic equipment that adheres to high grade cryptographic standards.
Host-based Intrusion Prevention System	An intrusion prevention system that is installed on individual servers or workstations to protect systems from intrusions and malicious code.
I-RAP	The Infosec-Registered Assessor Program (I-RAP) is a DSD initiative designed to register suitably qualified information security assessors to carry out specific types of ICT security assessments to Australian Government standards. **URL:** http://www.dsd.gov.au/infosec/evaluation_services/irap.html
ICT system	For the purposes of this manual, an ICT system is: • a related set of hardware and software used for the communication, processing and storage of information, and • the electronic form (not content) of the information that they hold or process.
ICTSP	An Information and Communications Technology Security Policy (ICTSP) is a document that describes the information security policies, standards and responsibilities for an agency.

Continued on next page

IP telephony	The transport of telephone calls over Internet Protocol (IP) networks. It may also be referred to as Voice-Over-IP (VOIP) and Internet Telephony.
ISIDRAS	The Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) is a scheme established by DSD to collect information on security incidents that affect the security or functionality of Australian Government computer and communication systems.
ITSA	The Information Technology Security Adviser (ITSA) is the person appointed by an agency to manage the security of the agency's information and ICT systems.
ITSEC	The Information Technology Security Evaluation Criteria (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).
Key	A sequence of random or pseudo random bits used: • initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, • for determining electronic counter-countermeasure patterns, or **Example:** frequency hopping or spread spectrum • for producing other keys.
Malicious code	Any software that attempts to subvert the confidentiality, integrity or availability of a system. Malicious code includes: • logic bombs, • trapdoors, • Trojan programs, • viruses, and • worms.
Media	The component of hardware that is used to store information.

Continued on next page

Multifunction devices	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.
Need-to-know	The principle of telling a person only the information that they require to fulfil their role.
Non-volatile media	A type of media which retains its information when power is removed.
Peripheral switches	Devices 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.
Privileged user	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, ICT security staff, Helpdesk staff.
Protection Profile	An implementation-independent set of security requirements for a category of ICT products that meets specific consumer needs.
Push-To-Talk	Push-To-Talk handsets prevent the possibility of an idle handset inadvertently allowing discussions being undertaken in the vicinity of the handset to be heard by the remote party.
Reclassifi-cation, 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.
Remote access	Any access to an agency's system from a location not within the physical control of that agency.

Continued on next page

Removable media	Storage media that can be easily removed from an ICT system and is designed for removal. **Examples:** Hard disks, CDs, floppy disks, tapes, smartcards, and flashcards.
Risk	The *Australia/New Zealand Risk Management Standard (AS/NZS 4360:2004)* 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 Management Plan	The complete documentation package generated by following the risk management process.
Risk Register	A list, or database, of the risks faced by an agency.
Risk Treatment Plan	Documents how risk treatment controls should be implemented.
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'.
SCEC	The Security Construction and Equipment Committee (SCEC) approves security equipment for Australian Government use.
SEC	The *Security Equipment Catalogue (SEC)* lists equipment that has been tested and endorsed as meeting relevant SCEC standards.
Seconded foreigner	A representative of a foreign government on exchange or long-term posting to an Australian Government agency. **Note:** These people are often referred to as "Integrees" within Defence.

Continued on next page

Security incident	An event that impacts on the confidentiality, integrity or availability of a system through an act of unauthorised access, disclosure, modification, misuse, damage, loss or destruction.
Security Target	The security target for a product is a document defining the: • security claims of the TOE, • scope of the evaluation, and • the intended operational environment of the TOE. The security claims are divided into: • a set of security requirements, and • details of the security functions which meet those requirements.
Server	A computer used to run programs that provide services to multiple users. **Examples:** File servers, mail servers, and database servers.
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	The part of the product or system that is subject to an evaluation.

Continued on next page

Traffic flow filter	A traffic flow filter is any device that has been configured to filter and control the flow of data.
TSCM	Technical surveillance counter measures (TSCM) are searches for covert electronic surveillance devices. TSCM are also known as ‘sweeps’.
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.

This page is intentionally blank.

Index

A

B

C

D

H

I

N

O

P

R

S

T

U

V

W