Australian Government

Department of Defence
Intelligence & Security

Australian Government Information and Communications Technology Security Manual

ACSI 33

Defence Signals Directorate

Release Date: 29 September 2006

Commonwealth Copyright Administration
Copyright Law Branch
Attorney-General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600
www.ag.gov.au/cca

ISBN 0 642 29598 0

Foreword

The *Australian Government 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

Table of Contents

Part 1
ACSI 33 and ICT Security

Overview

Introduction

1.0.1. This part contains important information about this manual and how it relates to the security of Australian Government information and communications technology (ICT) systems.

Authority

1.0.2. The *Australian Government 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

1.0.3. 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

1.0.4. This part contains the following topics:

Using ACSI 33

Introduction

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

Classification of ACSI 33

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

The *ACSI 33* version marked 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.

Block classifications

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

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

Block numbering

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

- Part number
- Chapter number
- Block number

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.

Block applicability and system classifications

1.0.9. Readers will note that some block titles include a system classification or caveat reference, shown within square brackets. Block titles that do not include such a reference indicate that the block applies to all ICT systems, unless otherwise noted within the block text.

Continued on next page

Releasability of classified version

1.0.10. DSD authorises access to the SECURITY-IN-CONFIDENCE version to those with a need-to-know, in accordance with the provisions of the PSM. This may include agency security staff and commercial organisations contracted to or seeking to support Australian Government agencies.
Note: 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 **MUST NOT** be made available, directly or indirectly, to the public, or to persons not considered to have a need-to-know, unless approved by DSD.

Continued on next page

Updates

1.0.12. This manual is updated regularly. It is therefore important that agencies ensure 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:** www.dsd.gov.au/ • Defence Restricted Network
SECURITY-IN-CONFIDENCE	• OnSecure members area **URL:** www.onsecure.gov.au/ • Defence Restricted Network

Feedback

1.0.13. 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

1.0.14. 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

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

The term…	Covers information that is…
National security	classified RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET.
Non-national security	classified IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED.
Classified	security classified as either national security or non-national security. **Important:** Classified information **does not** include information deemed to be UNCLASSIFIED.
UNCLASSIFIED	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	authorised for unlimited public access or circulation, such as agency publications and websites.
Official	classified, UNCLASSIFIED, or public domain.
CABINET-IN-CONFIDENCE	prepared for consideration by Cabinet, including during preparation.

Treatment of CABINET-IN-CONFIDENCE

1.0.16. The *Cabinet Handbook* states that the **minimum** protection given to Cabinet documents is to be equivalent to information marked as PROTECTED. References in this manual to IN-CONFIDENCE **do not** include CABINET-IN-CONFIDENCE.

Treatment of AUSTEO and AGAO

1.0.17. 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

1.0.18. 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 1-9.
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. **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

1.0.19. 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 1-7.
MUST NOT	Non-use of the item is mandatory. **See:** 'Waivers against "MUSTs" and "MUST NOTs"' on page 1-7.
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 1-7.
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 1-7.
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"

1.0.20. Agencies deviating from a "**MUST**" or "**MUST NOT**" statement in this manual **MUST** provide a waiver in accordance with the requirements of Part A of the *PSM*.

In addition, agencies **MUST** advise DSD of the decision.

Deviations from "SHOULDs" and "SHOULD NOTs"

1.0.21. 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

1.0.22. 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

1.0.23. 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

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

Process

1.0.25. 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 2-17
2. Conduct risk management	• Identify the scope of the system to be protected. • Develop an initial RMP.	Chapter 4 – Risk Management on page 2-22
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 2-35
4. Implementation	• Implement the SSP(s), including the purchase of hardware and software. • Develop and document the SOPs.	Chapter 6 – Developing and Maintaining Security SOPs on page 2-38
5. Certification	• Determine what needs certifying. • Obtain certification from the relevant person or organisation.	Chapter 7 – Certifying and Accrediting ICT Systems on page 2-45
6. Accreditation	Obtain accreditation from the relevant authority.	
7. Maintenance	• Implement change control procedures. • Perform integrity checks.	Chapter 8 – Maintaining ICT Security and Managing Security on page 2-58
8. Review	Review and revisit each stage of this process annually.	Chapter 9 – Reviewing ICT Security on page 2-74

About ICT Systems

Definition: ICT system

1.0.26. For the purposes of this manual, an ICT system is considered to be 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

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

See: ‘About Certification’ on page 2-46.

Continued on next page

System modes

1.0.28. An ICT system may operate in any one of the modes described in the table below.

See: ‘System Users’ on page 2-9 for more detail about system users, and ‘Chapter 6 – Logical Access Control’ on page 3-60 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

1.0.29. 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* 2005, 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
business continuity,	HB 221:2004 *Business Continuity Management*	Standards Australia
CABINET-IN-CONFIDENCE information security	*Cabinet Handbook*, Chapter 7, Security and Handling of Cabinet Documents	PM&C
classification labelling,	*PSM* 2005, Part C, Information Security	AGD
clearances,	*PSM* 2005, Part D, Personnel Security	AGD
information handling procedures,	*PSM* 2005, Part C, Information Security	AGD
information security management,	• AS/NZS ISO/IEC 17799:2006 – *Information technology – Code of practice for information security management*, and • AS/NZS ISO/IEC 27001:2006 – *Information technology – Security techniques – Information security management systems – Requirements*	Standards Australia
information security responsibilities,	*PSM* 2005, 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

Continued on next page

Further information (continued)

For further information on...	See...	Available from…
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* 2005, Part E, Physical Security.	AGD
reporting of security incidents,	*PSM* 2005, 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

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 perform various functions including the provision of:

- 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 communication and computer 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

2.1.6. 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	www.dsd.gov.au/

Other Organisations

Other organisations

2.1.7. 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:** www.ag.gov.au/agd/www/pscctrainingcentre.nsf
T4 Protective Security Section – Australian Security Intelligence Organisation	Protective security risk reviews and advice, and equipment testing. **URL:** www.asio.gov.au/work/content/protect.html
National Archives	Advice and guidelines on archives legislation and its application to ICT systems. **URL:** www.naa.gov.au
Australian Government Information Management Office – Department of Finance	Development, coordination and oversight of Government policy on electronic commerce, online services and the Internet. **URL:** www.agimo.gov.au
The Office of the Federal Privacy Commissioner	Advice on how to comply with the Privacy Act and related legislation. **URL:** www.privacy.gov.au
Department of Foreign Affairs and Trade	Policy and advice for security overseas. **URL:** www.dfat.gov.au
Australian National Audit Office	Performance audits and "Better Practice" guides for areas including information security. **URL:** www.anao.gov.au
High Tech Crime Centre – Australian Federal Police	Law enforcement in relation to e-crime and other high tech crimes. **URL:** www.ahtcc.gov.au
Australian Computer Emergency Response Team	Computer incident prevention, response and mitigation strategies. **URL:** www.auscert.org.au

Appointing an IT Security Adviser (ITSA)

Requirement for ITSA

2.1.8. 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

2.1.9. 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

2.1.10. 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

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

Allocation of ITSA functions

2.1.12. 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

2.1.13. 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

2.1.14. 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

2.1.15. 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

2.1.16. 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

2.1.17. 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

2.1.18. 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**

2.1.19. Paragraph C4.8 of the *PSM* states that "Agency security personnel… are not, however, responsible for making the decisions about what requires protection and what type of protection is most appropriate. This remains the responsibility of the manager with functional control of the resource."

Documentation responsibilities

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

- RMP, **See:** 'Chapter 4 – Risk Management' on page 2-22.
- SSP, **See:** 'Chapter 5 – Developing an SSP' on page 2-35.
- SOP, **See:** 'Chapter 6 – Developing and Maintaining Security SOPs' on page 2-38.

Certification and accreditation responsibilities

2.1.21. 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 reaccreditation,
- 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 2-45 for more detail.

SOPs

2.1.22. 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.

Ensuring adherence to procedures

2.1.23. The System Manager is responsible for ensuring that procedures recorded in security documentation are followed.

System Users

Types of system users

2.1.24. 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

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

Requirements: privileged access

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

a. 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

2.1.27. Agencies **SHOULD**:

a. restrict privileged access to a minimum, and
b. closely audit privileged access.
   See: ‘Chapter 7 – Active Security’ on page 3-67.

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:

Topic	See page
Requirements for ICT Security Documentation	2-11
The Documentation Process	2-14
Classifying ICT Security Documents	2-16
Templates	2-17

Not included

2.2.3. The following subjects are covered elsewhere:

Subject	See
Documenting ICT security policies	'Chapter 3 – Identifying and Developing an ICT Security Policy' on page 2-18
Documenting risk management	'Chapter 4 – Risk Management' on page 2-22
Documenting system security plans	'Chapter 5 – Developing an SSP' on page 2-35
Documenting standard operating procedures	'Chapter 6 – Developing and Maintaining Security SOPs' on page 2-38

Requirements for ICT Security Documentation

Document requirements

2.2.4. Agencies **MUST** have security risk assessments, policies and plans that cover 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*.

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 2-18.

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 2-22.

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 2-35.

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 2-38.

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. Agencies **SHOULD** ensure that the agency's RMPs, ICTSPs, SSPs and SOPs are logically connected and consistent for each system.

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 code 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 2-11.

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 role of the security executive is defined in paragraph A4.9 of 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 is not given, due to the diversity of SOP requirements.

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.org.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.org.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 Federal Information Systems*	National Institute of Standards and Technology (US) **URL:** csrc.nist.gov/publications/nistpubs/index.html	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 2-17.

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 2-11.

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 blocks.

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 17799:2006*,
- *AS/NZS ISO/IEC 27001:2006*, 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 2-12.

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 2-17.

Continued on next page

Overview, Continued

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 2-12.

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 2-26.
2	Identify the risks for each asset. **See:** 'Stage 2: Identifying the Risks' on page 2-28.
3	Analyse the identified risks. **See:** 'Stage 3: Analysing the Risks' on page 2-29.
4	Assess and prioritise the risks. **See:** 'Stage 4: Assessing and Prioritising Risks' on page 2-33.
5	Determine appropriate controls for each risk. **See:** 'Stage 5: Developing a Risk Treatment Plan' on page 2-34.
6	Collate the information gathered in stages 1 - 5 to produce the RMP. **See: '**Producing an RMP' on page 2-25.

Continued on next page

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 2-28.

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 2-26.

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 2-29.

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 2-28.

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 2-33.

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

Stage 3: Analysing the Risks, Continued

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	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
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 2-29.

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 2-34.

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 2-33.

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 2-29.
5	Assess the residual risk rating according to the criteria recorded on the risk register and update the risk register. **See:** 'Stage 4: Assessing and Prioritising Risks' on page 2-33.
6	Record the accepted controls in the control register. Develop the RTP by defining responsibilities, timetable and monitoring methods for the implementation of each accepted control.

Chapter 5 – Developing an SSP

Overview

Introduction

2.5.1. This chapter contains information about developing SSPs.

Template

2.5.2. **See:** ‘Templates’ on page 2-17.

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 2-19.

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 2-12.

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.

Contents

2.6.3. This chapter contains the following topics.

Developing Security SOPs

Definition: SOPs

2.6.4. 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

2.6.5. 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

2.6.6. 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 2-35.

Maintenance

2.6.7. 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 2-60.
b. part of a regular review of documentation.
See: ‘Chapter 9 – Reviewing ICT Security’ on page 2-74.

Continued on next page

Procedure

2.6.8. 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 2-12.

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

2.6.9. The information in this topic may be used 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

2.6.10. 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 off-site, 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, including involvement in physical security incident management where the incident could impact on ICT security.

Continued on next page

System Manager SOPs

2.6.11. 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. testing and applying software patches/updates, c. applying appropriate hardening techniques, and d. 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

2.6.12. 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.

Continued on next page

System Users

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

System Users SOPs

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

Topic	Information that SHOULD be included
Roles and responsibilities	Who is responsible for what aspects of security.
Warning	A warning that: a. users' actions may be audited, and b. users will be held accountable for their actions.
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

2.6.15. 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 user support section 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

2.6.16. 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.

Certification is a prerequisite for accreditation.

Clarification of policies and standards

2.7.2. From the start of the certifying and accrediting process, it is advisable to have ongoing discussions with the Certification and Accreditation Authorities for clarification of, and guidance concerning, the relevant policies and standards.

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

Contents

2.7.3. This chapter contains the following sections:

Not included

2.7.4. 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 Certifications

Definition: Certification Authority

2.7.5. A Certification Authority is an entity with the authority to assert that ICT systems comply with the required standards.

Definition: certification

2.7.6. Certification is the assertion by a Certification Authority 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.

Definition: provisional certification

2.7.7. Provisional certification may be granted by a Certification Authority when the system is lacking compliance in some non-critical aspect(s) of the design, policy or management.

It is issued to indicate that full certification can be expected, subject to successful completion of the provisions identified in the certification report.

Withdrawal of provisional certification

2.7.8. The certifier **SHOULD** include the timeframe for the completion of the provisions in the certification report. Failure to meet the provisions within the specified timeframe **SHOULD** result in the provisional certification being withdrawn.

Reviewing certification reports

2.7.9. DSD **RECOMMENDS** that agencies review certification reports, including the chosen release date, when determining the risks associated with connecting to other certified systems. Particular attention to the details of the certification report may be required if the system has only provisional certification.

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

Certification to Australian Government standards

2.7.10. For the purposes of ICT system certifications to Australian Government standards, agencies **MUST** ensure that all certifications are performed against the latest release of this manual.

If the certifier identifies aspects of a system that do not comply with the current release, but do comply with policy released within the last 24 months, certification may still be granted if the overall integrity of the system is not significantly compromised by the lack of compliance with the current release.

Certifiers **MUST** identify in the certification report all instances of non-compliance with the current release.

Continued on next page

What is certified?

2.7.11. The table below describes what may be certified and the Certification Authorities 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 2-78 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 2-50 for more detail.
products approved for Government use listed on the Evaluated Products List (EPL),	DSD. **See:** 'Evaluated Products List' on page 3-20 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

Certification process

2.7.12. The table below describes the five stages of the 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 2-22.
3	design documentation,	that the documents have been developed and meet the standards required. Design documents required for certification may include the: • Logical/Infrastructure Diagram, • Concept of Operations, • List of Mandatory Requirements, • Risk Based Requirements, and • List of Critical Configurations.
4	SSP and SOPs,	that they meet the required standards and include: • security administrative tasks, • proactive security checking tasks, • proactive security auditing tasks, and • a contingency plan. **See:** • 'Chapter 5 – Developing an SSP', on page 2-35, and • 'Chapter 6 – Developing and Maintaining Security SOPs' on page 2-38.
5	current system configuration,	• the configuration checking of critical components, and • that the tools in use meet the requirements and are functional.

Gateway Certification

Purpose of gateway certifications

2.7.13. 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 Australian Government standards, 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

2.7.14. 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 2-78 for information on the program.

Gateway Certification Guide

2.7.15. 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

Gateway Certification, Continued

Gateway certification standards

2.7.16. 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.

Independent gateway certifications

2.7.17. 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.

What is looked for in a review?

2.7.19. As part of the review, 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 gateway certification

2.7.20. 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.

Provisional gateway certification does not preclude the gateway from operating, but does mandate that the provisions identified in the certification report be corrected within a specified timeframe.

Continued on next page

Recertification

2.7.21. 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.

As part of the recertification process, the gateway certifier **SHOULD** review the effectiveness of change management procedures.

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

Comsec Certification

Definition: Comsec certification

2.7.22. Comsec certification:

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

Granting Comsec certification

2.7.23. 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

2.7.24. 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.

About Accreditations

Definition: accreditation

2.7.26. 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

2.7.27. 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.

Requirement for accreditation

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

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

Documenting accreditations

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

Accreditation for classification

2.7.31. 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 3-93.

Continued on next page

Accreditation for caveats

2.7.32. 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.

Continued on next page

Accreditation for national and non-national classifications

2.7.33. Agencies intending to process, store or transmit both nationally and non-nationally classified information **SHOULD** ensure that the accreditation documentation states the highest classification for which the system is accredited in each of the two streams.

Example: An agency with a system accredited for PROTECTED information may also choose to receive and store RESTRICTED information on it. In this case, the system would need to be accredited for “PROTECTED and RESTRICTED”.

The table below shows the hierarchy of classifications, based on the general standard of security controls required for each.

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.

A system built to meet the standards for…	Will also meet the standards for systems with information classified as…
TOP SECRET	All other classifications
SECRET	• CONFIDENTIAL, • HIGHLY PROTECTED, • PROTECTED, and • RESTRICTED, • IN-CONFIDENCE.
CONFIDENTIAL	• PROTECTED, • RESTRICTED, and • IN-CONFIDENCE.
HIGHLY PROTECTED	• PROTECTED, • RESTRICTED, and • IN-CONFIDENCE.
PROTECTED	• RESTRICTED, and • IN-CONFIDENCE.
RESTRICTED	IN-CONFIDENCE.
IN-CONFIDENCE	No other classifications.

Accreditation is not transferable

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

Continued on next page

Prerequisites

2.7.36. Accreditation Authorities **SHOULD** undertake the following activities prior to accreditation:

a. review the RMP,
b. review any deviations from mandatory requirements specified in this manual and the *PSM*, and
c. confirm that all relevant certifications have been provided.
   See: 'What is certified?' on page 2-48.

Provisional accreditation

2.7.37. 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.

Post-accreditation activities

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 2-58.

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 documents

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

Overview, Continued

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.

Business Continuity

Definition: business continuity

2.8.11. Business continuity ensures the ongoing availability of identified processes and resources in support of critical business objectives.

Scope

2.8.12. Business continuity covers a wide range of concepts including business resilience and long term performance, as well as the more traditional areas of risk management, contingency planning, incident and emergency response, and disaster recovery, much of which is outside the scope of pure ICT security policy.

The remainder of this section focuses on standards relating to the availability of systems; the following sections address detecting, managing and responding to security incidents.

Availability requirements

2.8.13. Part C of the *PSM* requires agencies to determine availability requirements for their systems. Once these have been determined, agencies **MUST** implement appropriate measures to support these requirements for all ICT systems.

Such measures may include:

- information backups,
- remote storage,
- remote processing,
- redundant ICT systems, and
- redundant environmental systems.
  Example: Uninterruptible Power Supply (UPS).

Backup strategy

2.8.14. Agencies **SHOULD**:

a. backup all information identified as critical to their business,
b. store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the standards for the classification of the information, and
c. test backup and restoration processes regularly to confirm their effectiveness.

Additional references

2.8.15. Additional information relating to availability and business continuity is also contained in the:

- *PSM*, Part C - Information Security,
- AS/NZS ISO/IEC 17799:2006, 14 Business Continuity Management, and
- HB 221:2004 - *Business Continuity Management*

Detecting Security Incidents

Definition: security incident

2.8.16. 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

2.8.17. 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 3-58.
b. intrusion detection strategies,
   See: ‘Intrusion Detection Systems’ on page 3-68.
c. audit analysis,
   See: ‘Event Logging’ on page 3-70.
d. system integrity checking, and
   See: ‘System integrity’ on page 3-46.
e. vulnerability assessments.
   See: ‘Vulnerability Analysis’ on page 3-75.

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

2.8.18. 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 3-15.

Continued on next page

Tools used

2.8.19. 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 and has resolved any relevant legal issues.

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. **See:** ‘Intrusion Detection Systems’ on page 3-68.
Intrusion prevention systems	Some intrusion detection systems are combined with functionality to repel detected attacks. Caution and assessment of the potential impact need to be exercised if this capability is to be used. **See:** ‘Host-based intrusion prevention systems’ on page 3-59.
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. **See:** ‘System integrity’ on page 3-46, and the subsequent blocks on ‘Characterisation’.
Log analysis	Involves collecting and analysing event logs using pattern recognition to detect anomalous activities. **See:** • ‘Event Logging’ on page 3-70, and • ‘Auditing’ on page 3-74.

Effectiveness of tools

2.8.20. 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.

Continued on next page

Implementation of tools

2.8.21. 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

2.8.22. Agencies **MUST** detail security incident, including physical security incident, responsibilities and procedures for each agency system in the relevant SSP and in SOPs.

See:

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

Agencies **MUST** develop an Incident Response Plan and supporting procedures, and ensure users are aware of these.

See: ‘Incident Response Plan’ on page 2-72.

Internal reporting

2.8.23. Agencies **MUST** direct staff to report security incidents to the ITSA (and the ASA if physical security is involved) as soon as possible after the incident is discovered, in accordance with agency procedures.

Standards

2.8.24. 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.

DSD assistance

2.8.25. Agencies may choose to request assistance from DSD for 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 **RECOMMENDS** that any requests for DSD assistance are made as soon as possible after the incident is detected, and that no actions which may affect the integrity of the evidence are carried out prior to DSD involvement.

DSD’s response will be commensurate with the urgency of the incident; a 24-hour, 7-day service is available if necessary. Contact details for reporting incidents to DSD are:

Email	incidents@dsd.gov.au
Phone	02 6266 0009 (24x7)

Continued on next page

Recording incidents

2.8.26. 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.

Handling data spillages [U, IC, R, P]

2.8.27. 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 2-72.

Continued on next page

Handling malicious code infection

2.8.29. 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	Decide whether to request assistance from DSD. If such assistance is requested and agreed to, delay any further action until advised by DSD to continue. **See:** 'DSD assistance' on page 3-66. **Note:** This is to ensure that evidence relating to the incident is not accidentally damaged or destroyed.
3	Scan all previously connected systems, and any media used within a set period leading up to the incident, for malicious code. **Notes:** • Consider the infected date of the machine, and the possibility that the record may be inaccurate, when determining the appropriate period. • Characterisation techniques may be used to assist in determining the scope of the infection. **See:** 'Definition: characterisation' on page 3-46.
4	Isolate all infected systems and/or media to prevent reinfection.
5	Change all passwords and key material stored or potentially accessed from compromised systems.
6	Advise users of any relevant aspects of the compromise, including a recommendation to update all passwords on compromised systems.
7	Use current anti-virus software to remove the infection from the systems and/or media. If this fails: • seek advice from the vendor, or • perform a complete operating system reinstallation.
7	Report the incident and perform any other activities required by the incident response plan. **See:** • 'Reporting of incidents' on page 2-70 for information on reporting requirements and additional assistance available from DSD. • 'Incident Response Plan' on page 2-72.

Continued on next page

Allowing continued attacks

2.8.30. Agencies 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

2.8.31. 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

2.8.32. 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

2.8.33. 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: www.dsd.gov.au/infosec/assistance_services/incident.html

Definition: significant

2.8.34. 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 to DSD

2.8.35. Agencies, via their ASA or ITSA, **MUST** report significant ICT security incidents to DSD without delay. Other incidents may be reported at agency discretion.

See: ‘DSD assistance’ on page 3-66 for incident contact details.

Incidents and outsourcing

2.8.36. 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.

Cryptographic keying material

2.8.37. 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.

Continued on next page

Additional references

2.8.39. Additional information relating to external reporting requirements is contained in the *PSM*, Part G - Guidelines on Security Incidents and Investigations.

Incident Response Plan

Developing the plan

2.8.40. 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 2-73.
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

2.8.41. 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 Part G of the *PSM*,
d. the criteria by which the responsible authority would initiate formal, police or ASIO investigations of an incident,
e. references to other related agency documents,
   Examples: Business Continuity Plan, 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

2.8.42. 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.

Developing the procedures

2.8.43. 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.

Continued on next page

Training

2.8.44. 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 against "MUSTs" and "MUST NOTs"' on page 2-7.

Who can perform a review?

2.9.5. ICT security reviews may be performed by internal staff, or by independent third parties such as I-RAP assessors or DSD.

See: 'Infosec-Registered Assessor Program (I-RAP)' on page 2-78 for information on the program.

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 2-9.

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.

Registration process

2.9.13. To be registered under I-RAP, an individual is required to:

- demonstrate relevant experience,
- attend the I-RAP course, and
- pass the I-RAP exam.

Policy and procedures

2.9.14. The *'Policy and Procedures for the Infosec-Registered Assessor Program (I-RAP)'* document contains further information on I-RAP, including a definition of the range of activities I-RAP assessors are licensed to perform. It is available via links from DSD's website to the program's current administrator.

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

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 meets the guidelines and established minimum standards of the *PSM*.

Contents

3.1.2. This chapter contains the following sections:

Not included

3.1.3. The following subjects are covered elsewhere:

Subject	See
Clearances and briefings	'Clearances and Briefings' on page 3-18.
Media security	'Chapter 4 – Hardware Security' on page 3-26.
Logical access controls	'Chapter 6 – Logical Access Control' on page 3-60.
Comsec standards	'Chapter 8 – Communications Security (Comsec)' on page 3-76.
Cabling	'Cabling' on page 3-78.
Telephones	'Telephones and Telephone Systems' on page 3-84.
Personal electronic devices (PEDs)	'Portable Computers and Personal Electronic Devices' on page 3-39.

Additional references

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

- *PSM*, Part E - Physical Security, and
- AS/NZS ISO/IEC 17799:2006, 9 Physical and environmental security.

The basics

3.1.5. 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, allowing only those with the authorisation and requirement to enter, and detecting those attempting to gain unauthorised access.

Risk management

3.1.6. Agencies **MUST** ensure that any site-specific physical security threats are included in their risk management process.

Protecting public domain and UN-CLASSIFIED systems

3.1.7. Agencies **SHOULD** implement measures to protect public domain and UNCLASSIFIED equipment from theft, damage and unauthorised access.

Physical security for Australian sites overseas

3.1.8. These are the minimum standards for the protection of sites located within Australia. Additional requirements may exist for sites located overseas; DFAT is the authority for all such sites.

See: ‘Other organisations’ on page 2-4.

PSM storage requirements

3.1.9. Much of the policy in this chapter is derived from the table following paragraph E7.62 of the *PSM*, which sets out the minimum standard of security container or secure room required for the storage of classified information within Australia.

The table is reproduced below for convenience.

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

ASIO T4 Protective Security

Introduction

3.1.10. 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

3.1.11. 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

3.1.12. DSD **RECOMMENDS** that agencies contact T4 for advice prior to the design and construction of a secure room/facility.

Security Construction and Equipment Committee

3.1.13. 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

3.1.14. 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.

Servers and Communication Equipment

Definition: server

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

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

Definition: communication equipment

3.1.16. Communication equipment includes any device designed to facilitate the transmission of information destined for multiple users. It does **not** include the cabling itself.

Examples:
- cryptographic devices,
- firewalls,
- routers,
- switches, and
- hubs.

See: 'Workstations and Network Infrastructure' on page 3-8 for physical security requirements for cabling.

Separating servers and communication equipment from users

3.1.17. Servers and any associated communications equipment **MUST** be separated from general user areas by a clearly defined perimeter. This separation can be achieved by the use of either:
- appropriate containers, or
- a purpose-built server room.

Unescorted access to the space **MUST** be limited to authorised staff cleared to the highest classification of information stored within the container or server room.

Separation using a container

3.1.18. Where the perimeter is achieved by means of a container, the equipment **MUST** be secured in accordance with the *PSM* requirements for the storage of classified information.
See: 'PSM storage requirements' on page 3-3.

The required class of container is determined by the classification of the system and the physical security standard of the area in which the container is located.

Continued on next page

Separation using a server room

3.1.19. Where the perimeter is achieved by means of a server room, the server room **MUST** meet the minimum standard of physical security defined in the table below. These standards are available from ASIO T4.
See: ‘Contacting T4’ on page 3-4.

All servers and communications equipment within the server room **MUST** be stored in locked commercial grade or better containers.

Note: The terms “SR1” and “SR2” are no longer in use; they have been replaced in this policy with the more common terms “Secure Area” and “Intruder Resistant Area” respectively. This is a change in terminology only.

If the information is classified…	And the outer perimeter is a(n)…	Then minimum standard for the server room is…
PROTECTED	Intruder Resistant Area	Secure Area
	Secure Area	Intruder Resistant Area
• RESTRICTED • IN-CONFIDENCE	Intruder Resistant or Secure Area	Intruder Resistant Area
UNCLASSIFIED	Intruder Resistant or Secure Area	**See:** ‘Protecting public domain and UN-CLASSIFIED systems’ on page 3-3.

Definition: No-Lone-Zone

3.1.20. 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

3.1.21. DSD **RECOMMENDS** that areas containing particularly 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

Administrative measures

3.1.22. A Site Security Plan and Standard Operating Procedures (SOPs) **MUST** be developed for each server room.

Subjects to be 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

Definition: workstation

3.1.23. A stand-alone or networked single-user computer.

Workstations can be configured to avoid having official information stored on them during non-business hours. This may be achieved in various ways, including thin client or diskless architectures, or the use of removable hard disks.

Definition: network infrastructure

3.1.24. The infrastructure used to carry information between workstations and servers or other communications equipment.

Examples:

- cabling,
- junction boxes,
- patch panels,
- fibre distribution panels, and
- structured wiring enclosures.

Protecting network infrastructure

3.1.25. Agencies **SHOULD** locate all patch panels, fibre distribution panels, and all structured wiring enclosures within locked spaces that prevent casual access by general users.

The ITSA **SHOULD** control the keys or equivalent access mechanism.

Continued on next page

Area type – workstations storing information

3.1.27. Agencies **MUST** ensure that workstations storing official information during non-business hours are wholly contained within areas of the appropriate standard as shown in the table below.

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

Area type – cabling and other workstations

3.1.28. Agencies **MUST** ensure that cabling and workstations configured to avoid having official information stored on them during non-business hours are wholly contained within areas of the appropriate standard as shown in the table below.

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

Removable hard disks

3.1.32. 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.
See: ‘PSM storage requirements’ on page 3-3.

Laptops

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

See: ‘Portable Computers and Personal Electronic Devices’ on page 3-39.

Protecting against theft of equipment

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

Area Security

Area security requirements

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

Preventing observation by unauthorised people

3.1.41. 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.

Removable Media

Definition: removable media

3.1.43. 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

3.1.44. Removable media containing classified information **MUST** be stored in accordance with the *PSM* requirements for information of that classification. The required class of container is determined by the classification of the information on the media and the physical security standard of the area in which the container is located.
See: ‘PSM storage requirements’ on page 3-3.

The effective classification level of the media may be reduced by the use of appropriate encryption.
See: ‘Requirements for storage encryption’ on page 3-93.

Mass storage devices

3.1.46. Devices holding removable media, such as CD and DVD towers, backup devices and RAID arrays, **MUST** be secured in containers in accordance with the *PSM* requirements for information of that classification.
See: ‘PSM storage requirements’ on page 3-3.

The required class of container is determined by the classification of the system and the physical security standard of the area in which the container is located.

Tamper Evident Seals

When to use seals

3.1.47. The use of seals is rarely mandated; however, agencies may choose to use seals as an additional risk mitigation method, particularly if other standards defined in this manual cannot be met for a particular environment.

Examples:

- Apply a wafer seal over USB ports or to hard disk cases to provide a tamper-evident barrier to discourage unauthorised access.
- Attach network connectors to computers using a roto-seal.

Approved seals

3.1.48. The SCEC endorses seals to be used for various sealing requirements. Further information on endorsed seals is available in the *SEC.*
See: 'Security Equipment Catalogue' on page 3-4.

Recording seal usage

3.1.49. 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

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

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

Purchasing seals

3.1.53. Where the option is available, agencies **SHOULD** consult with the seal manufacturer to ensure that any purchased seals and/or sealing tools display a unique identifier or image appropriate to the agency.

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

Emergency Procedures

Emergency situations [U, IC, R, P]

3.1.54. 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, including destruction as necessary, of classified material and equipment.

Important: Health and safety is 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:

Topic	See page
User Training and Awareness	3-15
Training Resources	3-17
Clearances and Briefings	3-18

Not included

3.2.3. The following subjects are covered elsewhere:

Subject	See
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 3-60.

Additional references

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

- *PSM*, Part D - Personnel Security, and
- AS/NZS ISO/IEC 17799:2006, 8 Human resources security.

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. how to recognise an anomaly that may indicate a possible security incident,
d. contacts in the event of a real or suspected security incident,
e. the legitimate use of system accounts,
f. configuration control,
g. access and control of system media,
h. the security of accounts, including sharing passwords,
i. authorisation requirements for applications, databases and data,
j. the destruction and sanitisation of media and hardcopy output, and
k. the risks associated with accessing information from non-agency systems, particularly the Internet.

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*.

Responsibilities

3.2.14. Agencies **MUST** ensure users have the appropriate clearance and need-to-know as in Part D of the *PSM* before they are permitted to access a system.

Clearances for privileged users

3.2.15. 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:

Evaluated Products List

Definition: Evaluated Products List

3.3.3. The Evaluated Products List (EPL) consists of products that have completed Common Criteria (CC), Information Technology Security Evaluation Criteria (ITSEC) or some other form of DSD approved evaluation, as well as products in evaluation in the AISEP.

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

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

Evaluation level mapping

3.3.5. 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	N/A	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	E0	N/A	E1	E2	E3	E4	E5	E6

Benefits of selecting an EPL product

3.3.6. Choosing products listed on the EPL provides 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 similar document.

Product Selection

Product selection standard

3.3.7. Agencies **SHOULD** select products from the EPL whenever the product is required to enforce a security function related to the protection of official information and systems.

Important: Policy stated elsewhere in this manual may override this product selection standard by specifying more rigorous requirements for particular functions.

Selection preference order

3.3.8. The following order of preference applies to the selection of products:

a. products from the EPL listed as having completed CC, ITSEC or other DSD approved evaluation, with a DSD cryptographic evaluation either completed or identified as not required,

b. products from the EPL listed as having completed CC, ITSEC or other DSD approved evaluation, with a DSD cryptographic evaluation shown as "underway",
Note: Where an evaluation assurance level (EAL) is mandated for an encryption product, products that have not completed a DSD cryptographic evaluation do not satisfy this requirement.

c. products from the EPL listed as being either in evaluation in the AISEP, or as a certified product on the Common Criteria Portal website,

d. products that are in evaluation by a foreign scheme with which the AISEP has a recognition agreement, and

e. products that have had no formally recognised evaluation.

Documenting product choice

3.3.9. When choosing a product, agencies **MUST** document:

a. the desired degree of assurance in the product's key functions,

b. the actual degree of assurance provided by the chosen product, based on the level of evaluation it has received for its key functions,

c. justification for any decisions to drop to the next level in the defined selection order of preference, and

d. acknowledgement and acceptance of any risk introduced by the use of a product of lower assurance than desired, particularly if using a product that has not, and may never, complete all relevant evaluation processes.

Continued on next page

Additional guidance

3.3.10. DSD **RECOMMENDS** that, prior to purchase:

a. agencies intending to use products that are listed only on the Common Criteria Portal website discuss with DSD the option of sponsoring the product through the DSD compliance process,

b. agencies intending to use unevaluated products contact the product vendor to discuss having the product formally evaluated, and incorporate the requirement for successful evaluation into any contracts made with the vendor,

c. agencies intending to use a product that the vendor claims is in evaluation in a DSD-recognised foreign scheme contact DSD to confirm this claim, if such evidence is not readily available from the foreign scheme's website.

Ongoing maintenance

3.3.11. DSD **RECOMMENDS** that agencies choose EPL products 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.

Assessing the suitability of EPL products

3.3.12. In assessing an EPL product 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 the 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.

High Grade Equipment

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

Acquiring Products

Purchasing and delivery

3.3.14. When acquiring products for use in a sensitive environment, it may be important to limit opportunities for the products to be accidentally or maliciously replaced or altered during the purchase and delivery process.

Delivery of EPL products

3.3.15. Agencies **SHOULD** ensure that EPL products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

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

Delivery of non-EPL products

3.3.16. DSD **RECOMMENDS** that agencies ensure that products purchased without the delivery assurances provided through the use of formally evaluated procedures are delivered in a manner that provides confidence that they receive the product they expect to receive.

Leasing arrangements

3.3.17. 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

3.3.18. This section discusses the installation, configuration, administration and use of ICT products.

Installing and configuring EPL products

3.3.19. Agencies **SHOULD** ensure that products are installed and configured in a manner consistent with the evaluated 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 EPL products in unevaluated configurations

3.3.20. An EPL product 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 not covered by a formal assurance continuity process 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 an EPL product 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 EPL products

3.3.21. 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.

Disposing of Products

Secure disposal

3.3.22. 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 3-30.

High Grade Equipment

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

TEMPEST rated equipment

3.3.24. 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:

a. the above are unsuccessful, or
b. the equipment is non-functional.

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:

Section	See page
Classifying, Labelling and Registering	3-27
Repairing and Maintaining Hardware	3-29
Disposing of Hardware	3-30
Media Sanitisation	3-32
Media Destruction	3-36
Portable Computers and Personal Electronic Devices	3-39

Not included

3.4.5. The following subjects are covered elsewhere:

Subject	See
Physical security	'Chapter 1 – Physical Security' on page 3-2.
Cabling	'Cabling' on page 3-78.

Additional references

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

- *PSM*, Part C - Information Security, and
- AS/NZS ISO/IEC 17799:2001, 10.7 Media handling.

Classifying, Labelling and Registering Hardware

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

Classifying, Labelling and Registering Hardware, Continued

Labelling hardware and media

3.4.15. Agencies **MUST** ensure that the classification of all media is readily visually identifiable. Agencies **SHOULD** achieve this by labelling media with a protective marking that states the maximum classification and set of caveats applicable to the information stored on the media.

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.

Exception: Labels are not required for internally mounted media if the hardware containing the media is labelled.

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

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

Repairing and Maintaining Hardware

On-site repairs

3.4.21. 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

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

a. appropriately cleared and briefed, and
b. sufficiently familiar with the hardware to understand the repair work being performed.

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

Off-site repairs [U]

3.4.23. 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]

3.4.24. 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 who is sufficiently familiar with the hardware to understand the repair work being performed, 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

3.4.26. 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 3-32.
- ‘Media Destruction’ on page 3-36.

Occupational Health and Safety (OH&S)

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

Faulty media and hardware

3.4.28. 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 3-36.

Continued on next page

Disposal process

3.4.30. 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

3.4.31. 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 3-27.
- ‘Definition: media declassification’ on page 3-27.
- ‘Definition: media destruction’ on page 3-36.

Requirements for sanitising media

3.4.32. 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
   Note: This includes moving from UNCLASSIFIED to public domain.
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

3.4.33. 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 “rewritable”.
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]

3.4.34. 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 3-34, • 'Procedure: overwriting magnetic media' on page 3-34, or • 'Degaussers' on page 3-35.
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) and flash memory **Examples:** • 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 3 pages of UNCLASSIFIED text with no blank areas on each colour cartridge within the device. If the print cycle cannot be completed due to a malfunction, an appropriately trained person **SHOULD** take out the device and wipe the total drum surface with a lint-free non-abrasive cloth. Manually turn drums within their cartridges to achieve this.
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

3.4.37. Agencies **SHOULD** use an EPL product for the sanitisation of magnetic media.

See: ‘Evaluated Products List’ on page 3-20.

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

3.4.39. 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 3-35
- ***C*** = a character/bit pattern
- ***-C*** = the bit-wise complement/inverse of ***C***

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

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Determine the appropriate value of <b><i>X</i></b> using the table in ‘Overwriting procedure: determining <i>X</i>’ on page 3-35.
<table>
<tr><th>If <i>X</i> is…</th><th>Then…</th></tr>
<tr><td>a number</td><td>go to step 2.</td></tr>
<tr><td>‘F’</td><td>format the media. End of procedure.
<b>Important:</b> Do <b>not</b> use a ‘quick’ format method.</td></tr>
</table></td></tr>
<tr><td>2</td><td>• Overwrite the entire media with <b><i>C</i></b>.
• Verify that all areas of the media have been overwritten with <b><i>C</i></b>.
• Overwrite the entire media with <b><i>-C</i></b>.
• Verify that all areas of the media have been overwritten with <b><i>-C</i></b>.

<b>Important:</b> If there are any errors, such as defective sectors, do not proceed with overwriting as it will be ineffective. In these cases the media <b>SHOULD</b> be destroyed.</td></tr>
<tr><td>3</td><td>Do the following <b><i>X</i></b> times:
• overwrite the entire media with <b><i>C</i></b>, then
• overwrite the entire media with <b><i>-C</i></b>.

<b>Example:</b> If <b><i>X</i></b> equals 0 (zero) then this step is skipped, however, if <b><i>X</i></b> equals 2 then the sequence would be <b><i>C</i></b>, <b><i>-C,</i></b> <b><i>C</i></b>, <b><i>-C</i></b>.</td></tr>
<tr><td>4</td><td>Overwrite the entire media with random data.</td></tr>
</table>

Continued on next page

Overwriting procedure: determining *X*

3.4.40. 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 3-34.

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

3.4.41. 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

3.4.44. 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

3.4.45. 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 3-31.

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(2)

(1) No destruction required if the toner has been removed from the surface of the device.

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

Continued on next page

Media destruction methods

3.4.46. 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 approved methods as 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	Yes	Yes	Yes	Yes	No
Floppy disk	Yes	Yes	Yes	No	Yes
Hard disk	Yes	Yes	Yes	Yes	No
Optical disk	Yes	Yes	Yes	Yes	Yes
Semi-conductor memory	Yes	Yes	Yes	No	No
Tape	Yes	Yes	Yes	No	Yes

(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 3-38.

Supervision

3.4.47. 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.

Supervision for accountable material

3.4.48. 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.

Continued on next page

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

3.4.49. 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 3-38.

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

3.4.51. 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.

Further advice

3.4.52. 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

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

Definition: PED

3.4.54. 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

3.4.55. PEDs include, but are not limited to:

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

Related topics

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

Topic	See
Physical security standards	‘Chapter 1 – Physical Security’ on page 3-2.
Wireless communications	‘Wireless Communications’ on page 3-83.
Telephones and pagers	‘Telephones and Telephone Systems’ on page 3-84.
Cryptography	‘Chapter 9 – Cryptography’ on page 3-91.
Data transfers	‘Chapter 11 – Data Transfer’ on page 3-126.

Certification and accreditation

3.4.57. 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 2-45.

Continued on next page

Storage and handling

3.4.59. 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 3-93.

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 3-3.

Operation

3.4.61. 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

3.4.63. 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 3-21 for information on selecting products.

Continued on next page

Labelling portable computers and PEDs

3.4.64. 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

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

See: 'Emergency Procedures' on page 3-13 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 systems, and
- web applications.

Why have software security controls?

3.5.3. Software security controls are established to:

- 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.

Software security standards

3.5.4. 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

3.5.5. This chapter contains the following sections:

Continued on next page

Not included

3.5.6. The following subjects are covered elsewhere:

Topic	See
Security incidents	'Chapter 8 – Maintaining ICT Security and Managing Security Incidents' on page 2-58.
Physical security	'Chapter 1 – Physical Security' on page 3-2.
Access control	'Chapter 6 – Logical Access Control' on page 3-60.
Logging and auditing	'Chapter 7 – Active Security' on page 3-67.
Networks, including data transfer	'Chapter 10 – Network Security' on page 3-109.

Software Fundamentals

Documentation

3.5.7. All server and workstation security objectives and mechanisms **SHOULD** be documented in the relevant SSP or similar document.

Hardening during installation

3.5.8. Agencies **SHOULD** reduce potential vulnerabilities on their systems by:

a. removing unneeded software,
b. removing unused accounts,
c. removing unnecessary file shares,
d. renaming required default accounts,
e. replacing default passwords,
f. ensuring patching is up-to-date,
g. disabling unused features on installed software and operating systems, and
h. disabling access to all unnecessary input/output devices at the BIOS level.
Examples: CD-ROMS, floppy disks, USB drives, wireless network interfaces.

Many more techniques for hardening systems exist. DSD **RECOMMENDS** that agencies consider seeking and applying additional information on hardening techniques relevant to their specific system software.

Server environments [U, IC, R, P]

3.5.10. In addition to the requirements for hardening during installation defined above, DSD **RECOMMENDS** that agencies:

a. limit information that could be disclosed outside the agency about what software is installed, and
Examples:

- User Agent on web requests disclosing the web browser type,
- network and mail client information in mail headers, and
- mail server software headers.

b. implement access controls on relevant objects to limit users and programs to the minimum access required to perform their duties.
Examples: Objects may include directories, files, programs, databases, and communications ports.

Workstation environments [U, IC, R, P]

3.5.12. DSD **RECOMMENDS** that agencies develop a hardened Standard Operating Environment (SOE) for workstations, covering the:

a. requirements for hardening during installation,
See: ‘Hardening during installation’ on page 3-44.
b. implementation of access controls on relevant objects to limit users and programs to the minimum access required to perform their duties,
c. installation of workstation firewalls, and
d. configuration of either remote logging or the transfer of local event logs to a central server.

Continued on next page

Ongoing patching and hardening

3.5.14. Agencies **SHOULD:**

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

b. take corrective action, including a risk assessment as necessary, when vulnerabilities that could affect agency systems are discovered,
See: ‘Use of EPL products in unevaluated configurations’ on page 3-24 for policy specific to evaluated products.

c. follow their documented change management procedures when applying patches or hardening systems, including the testing of patches and updates prior to their application to live systems, and
See: ‘Managing Change’ on page 2-60.

d. replace obsolete software and hardware with products for which ongoing support is available.

As part of the requirement for corrective action defined above, DSD **RECOMMENDS** that all relevant security-related patches are tested and applied as soon as possible.

Other mitigations

3.5.15. Where known vulnerabilities cannot be patched, agencies **SHOULD** use other protective measures as determined from a risk assessment.

Appropriate protective measures may include:

a. controls to resolve the vulnerability:
   1) engaging a software developer to correct the software (if the source code is available),
   2) consider moving to a different product with a more responsive vendor,
   3) asking the vendor for an alternate method of managing the vulnerability,

b. controls to prevent attacks from succeeding:
   1) mail filters that strip potentially harmful content to mail clients,
   2) web proxy filters that strip harmful content to web browsers,
   3) additional access controls on file and configuration settings,
   4) firewalls configured to block high risk traffic,

c. controls to detect attacks:
   1) virus, spyware and malware scanners, and
   2) other mechanisms as appropriate for the detection of exploits using the known vulnerability.

Continued on next page

Server separation

3.5.16. Where high risk servers, such as web, email, file and IP telephony servers, have connectivity to public domain networks, agencies **SHOULD**:

a. maintain effective functional separation between servers allowing them to operate independently,
b. minimise communications between servers at both the network and filesystem level, as appropriate, and
c. limit users and programs to the minimum access required to perform their duties.

DSD **RECOMMENDS** that this separation be achieved either:

d. physically, using single dedicated machines for each function, or
e. using virtualisation technology to create separate virtual machines for each function.

Separation may also be achieved through the use of techniques to restrict a process to a limited portion of the file system, but this is less effective.

System integrity

3.5.17. System integrity mechanisms are designed to:

- minimise the likelihood of unauthorised tampering of information, and
- detect attempts or incidents of unauthorised tampering or access.

Definition: characterisation

3.5.18. Characterisation is a technique used to analyse a system’s characteristics. It is important to security as it can be used to verify the system’s integrity at a later date.

Unfortunately, there are known techniques for defeating basic characterisations, therefore other methods of intrusion detection are also needed, particularly in situations where it is impractical to use a trusted environment for the generation of the characterisation data. However, it is very useful in post-intrusion forensics investigations where an infected disk can be compared to stored characterisation data in order to determine what files have been changed or introduced.

Files and directories may be characterised by:

- performing a cryptographic checksum on the files/directories when they are known to be virus/contaminant free, either manually or using a commercial product,
- documenting the name, type, size and attributes of legitimate files and directories, along with any changes to this information expected under normal system operation, or
- for a Windows system, taking a SYSDIFF snapshot.

Continued on next page

Requirement for characterisation

3.5.19. Agencies **SHOULD**:

a. characterise all servers whose functions are critical to the agency, and those identified as being at high risk of compromise,
b. store the characterisation information securely on read-only media,
c. update the characterisation information after every legitimate change to the system,
d. as part of the agency's ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred,
e. perform the characterisation from a trusted environment rather than the standard operating system wherever possible, and
   Example: Restart the system from a boot disk.
f. resolve any detected changes in accordance with the agency's incident management procedures.
   See: 'Managing Security Incidents" on page 2-66.

DSD **RECOMMENDS** agencies meet the requirement for characterisation using a DACA to perform cryptographic checksums.
See: 'DSD Approved Cryptographic Algorithms (DACAs)' on page 3-95.

Firmware updates

3.5.20. Agencies **MUST** ensure that any firmware updates are performed in accordance with their change management procedures, and in a manner that verifies the integrity and authenticity of the updating process.

Sourcing software [U, IC, R, P]

3.5.21. DSD **RECOMMENDS** that agencies:

a. obtain software from verifiable sources and verify its integrity using vendor supplied checksums, and
b. scan the software for malicious code.

"Phone home" functionality

3.5.23. Agencies **SHOULD** review all commercial software applications to determine whether they are configured to connect back to the vendor.

If such functionality is included, then agencies **SHOULD** make a business decision to determine whether to permit or deny these connections, including an assessment of the risks involved in doing so.

Example: Some applications include:

- "phone home" functionality, initiating a connection to the vendor site over the Internet, and
- inbound remote management.

Software Development

Introduction

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

Software development environments

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

a. there are at least 3 ICT environments covering:
   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.

Secure programming

3.5.27. Agencies **SHOULD** ensure that software developers use secure programming practices when writing code, including:

a. designing software to use the lowest privilege level required to achieve its task,

b. deny access by default,

c. check return values of all system calls, and

d. validate all user input.

Software testing

3.5.28. 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

3.5.29. Additional information relating to software development is contained in the AS/NZS ISO/IEC 17799:2006, 12.5 Security in development and support processes.

Database Security

Data labelling

3.5.30. Agencies **SHOULD** ensure that all information stored within a database is associated with an appropriate protective marking if the information:

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

Agencies **SHOULD** ensure that these protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any information retrieved or exported from the database.

Examples: Protective markings may be applied to records, tables, or to the database as a whole, depending on structure and use. Query results will often require a protective marking to reflect the aggregate of the information retrieved.

Database files

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

Accountability

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

See: 'Chapter 6 – Logical Access Control' on page 3-60.

Search engines

3.5.35. 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

Web usage

3.5.36. Agencies that allow staff to browse the Internet:

a. **MUST** have a policy governing web use, and
b. **SHOULD** ensure that users are informed of the associated dangers.

See: ‘Secure Sockets Layer and Transport Layer Security (SSL/TLS)’ on page 3-99 for policy relating to SSL connections, including the use of SSL whitelists.

Whitelisting HTTP sites

3.5.37. DSD **RECOMMENDS** that agencies consider the option of implementing whitelists for all HTTP traffic transiting their gateway.

Defining a whitelist of permitted HTTP sites, and blocking all unlisted sites, effectively removes one of the most common data delivery and exfiltration techniques used by malware. However, if agency staff have a legitimate requirement to access a numerous and rapidly changing list of websites, agencies will need to consider the costs of such an implementation.

Applying controls

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

Example: Client browsers.

Components of a web application

3.5.39. 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.

Continued on next page

Anonymity and privacy problems

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

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

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

Cookies

3.5.41. DSD **RECOMMENDS** agencies consider blocking inbound cookies, noting that such a decision may restrict legitimate agency staff activity.

Where cookies are allowed, DSD **RECOMMENDS** that agencies limit the lifetime of cookies to the current session.

Applications and plug-ins

3.5.42. 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

3.5.43. 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.

Website content

3.5.44. 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.

Electronic Mail Security

Email usage

3.5.45. Agencies that allow staff to email externally:
a. **MUST** have a policy governing the use of email, and
b. **SHOULD** ensure that users are informed of the associated dangers.

See: 'Chapter 11 – Data Transfer' on page 3-126 for additional policy on the transfer of data between networks.

Components of email system

3.5.46. 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 3-58.

Server auditing

3.5.47. 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 3-71.

Web-based email services

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

Automatic forwarding of received emails

3.5.49. 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 3-56.
- 'Blocking of outbound emails' on page 3-57.

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.

Continued on next page

Centralised email gateway

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

Email security documentation standards

3.5.52. 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 3-55 for standards relating to the protective marking policy for email.

Email technical standards

3.5.53. Agencies **SHOULD:**

a. restrict access to email servers to administrative users,

b. ensure that email servers available to the public are separated from the agency’s internal systems,

c. 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

d. ensure that account names cannot be determined from external mail servers.

Email server transport encryption [U]

3.5.54. DSD **RECOMMENDS** that agencies:

a. enable Transport Layer Security (TLS) encryption on incoming and outgoing email connections on email servers. TLS encryption between email servers is defined in RFC 3207 (and its obsolete predecessor RFC 2487) and has been implemented by most email server products,
   See: ‘Secure Sockets Layer and Transport Layer Security (SSL/TLS)’ on page 3-99.

b. configure TLS to negotiate a DACA in preference to an unapproved algorithm, finally reverting to unencrypted email transmission if no algorithm can be negotiated, and
   See: ‘DSD Approved Cryptographic Algorithms (DACAs)’ on page 3-95.

c. implement TLS authentication between email servers where significant volumes of official information is passed via email to other agencies.

Continued on next page

Technical standards for blocking emails

3.5.55. 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 3-57 for further standards on blocking emails based on their protective markings.

Electronic Mail – Protective Marking Policy

Marking classified emails

3.5.56. Agencies **MUST** ensure that protective markings are applied to all emails containing classified information that have been:

a. written or forwarded by agency staff, or
b. automatically generated by an agency system and are leaving the agency.

Agencies **SHOULD** ensure that all automatically generated emails remaining within the agency are marked with a protective marking.

Agencies **MUST** ensure that the protective marking identifies the maximum classification and set of caveats for all information in the email, including any attachments.

Marking unclassified emails [U, IC, R]

3.5.57. Agencies **SHOULD** ensure that all agency-originated emails that do not contain any classified information are given a protective marking to indicate this.

Examples:

- UNCLASSIFIED may be used for official information that is not classified, but has **not** been endorsed for public release.
- UNCLASSIFIED PUBLIC may be used for official information that is not classified, and **has** been endorsed for public release.
- PERSONAL or UNOFFICIAL may be used when the email contains no official information is present.

Marking unclassified emails [P]

3.5.58. Agencies **MUST** ensure that all agency-originated emails that do not contain any classified information are given a protective marking to indicate this.

Protective marking standard

3.5.60. The standard for the application of protective markings to emails is promulgated by the Australian Government Information Office (AGIMO), and is available from their website. Compliance with this standard will facilitate email interoperability between agencies.

URL: www.agimo.gov.au/publications/2005/october/protective_markings

Continued on next page

Marking tools

3.5.61. 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.

Emails from outside the Australian Government

3.5.62. DSD **RECOMMENDS** that agencies encourage external organisations that send email to the agency to adopt the protective marking system described in this manual.

Receiving unmarked emails

3.5.63. DSD **RECOMMENDS** that the receiving gateway label all unmarked emails to inform the intended recipient that no protective marking was present.

The recipient will have to apply a protective marking to the email before it can be forwarded elsewhere. Agencies **SHOULD** provide guidance to staff on how to determine an appropriate protective marking in consultation with the originator of the email.

Checking emails for a protective marking

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

Blocking of unmarked emails

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

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

Continued on next page

Blocking of outbound emails

3.5.66. 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** configure systems to:

c. block any emails with missing or invalid markings, and
d. log every occurrence of a blocked email.

DSD **RECOMMENDS** that the sender be notified of any blocked emails.

Blocking of inbound emails

3.5.67. 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

3.5.68. 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.

Malicious Code and Anti-Virus Software

Definition: malicious code

3.5.69. 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

3.5.70. 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

3.5.71. 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 code being introduced into the system(s),
   2) detect any malicious code installed on the system(s),

b. make their users aware of the agency's policies, plans and procedures, and

c. 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 2-58.

Anti-virus scanners

3.5.72. 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. check vendor virus pattern signatures for updates daily,

d. apply virus pattern signature updates as soon as possible after vendors make them available, and

e. regularly scan all disks.

See: 'Data import' on page 3-131 for mandatory malicious code countermeasures required when transferring data between systems.

Continued on next page

Host-based intrusion prevention systems

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

Active content blocking

3.5.74. 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

3.5.75. 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

3.5.76. The procedure for handling a malicious code infection is located in ‘Managing Incidents’.

See: ‘Handling malicious code infection’ on page 2-68.

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:

Section	See page
User Identification and Authentication	3-61
Privileged and System Accounts	3-64
Access and Authorisation	3-65

Not included

3.6.4. The following subjects are covered elsewhere:

Subject	See
Physical access	'Chapter 1 – Physical Security' on page 3-2.
Clearances	'Chapter 2 – Personnel' on page 3-14.
Network security	'Chapter 10 – Network Security' on page 3-109.

Additional references

3.6.5. Additional information relating to access control is contained in the AS/NZS ISO/IEC 17799:2006, 11 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

3.6.7. 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 stored authentication information

3.6.8. 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.

Protecting authentication information in transit

3.6.9. Agencies **MUST** ensure that authentication information is transmitted securely, protected from all other users.

See: ‘Cryptographic Requirements’ on page 3-92 for minimum encryption assurance levels for authentication information that grants access to a classified system passing over a network of lower classification.

Continued on next page

Password selection

3.6.11. Agencies **SHOULD** implement a password policy enforcing either:

a. a minimum password length of 12 characters with no complexity requirement, or

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

Password management

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 compliance with the password selection policy, where the operating system cannot be configured to enforce complexity requirements,
d. force the user to change an expired password on initial logon or if reset,
e. **NOT** allow predictable reset passwords,
   Example: "Password1" or a user's SID.
f. **NOT** reuse passwords when resetting multiple accounts,
g. **NOT** allow passwords to be reused within 8 password changes, and
h. **NOT** allow users to use sequential passwords**.**

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

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 a maximum of 15 minutes of user inactivity,
c. configure the lock to completely conceal all information on the screen,
d. ensure the screen does not appear to be turned off while in the locked state,
e. require the user to reauthenticate to unlock the system, and
f. deny users the ability to disable the locking mechanism.

Continued on next page

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

3.6.20. 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

3.6.21. 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. allow the use of privileged accounts for administrative work only.

Shared accounts

3.6.27. DSD **RECOMMENDS** that agencies avoid the use of shared, 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

Access and authorisation standards

3.6.29. 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

3.6.31. 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

3.6.35. 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

3.6.36. 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

3.6.37. 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:

Not included

3.7.3. The following subject is covered elsewhere:

Subject	See
System integrity	‘Software Fundamentals’ on page 3-44.

Intrusion Detection Systems

Definition: intrusion detection system

3.7.4. An intrusion detection system (IDS) is a product 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

3.7.5. Agencies **SHOULD** develop, implement and maintain 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 intrusion detection procedures,
d. user training and awareness programs, and
   See: ‘User Training and Awareness’ on page 3-15.
e. a documented incident response procedure.
   See: ‘Incident Response Plan’ on page 2-72.

IDSs on Internet gateways

3.7.7. 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.

IDSs on other gateways

3.7.8. 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

3.7.9. 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.

Continued on next page

Event management and correlation

3.7.10. 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

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

- AS/NZS ISO/IEC 17799:2006, 15.3 Information systems audit considerations, and
- HB 171:2003 *Guidelines for the Management of IT Evidence.*

Event Logging

Logging requirements

3.7.12. 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 list of events associated with a system or software component to be logged, and

c. event log protection and archival requirements.

Continued on next page

Event logs for software components

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

DSD **RECOMMENDS** that agencies log the events listed in the table below 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.
network/ 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.

Continued on next page

Event Logging, Continued

Event log facility

3.7.16. For each event identified as needing to be logged, agencies **MUST** ensure that the log facility records at least the following details, 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.

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.

Event log protection and archival

3.7.17. Event logs **MUST** be:

a. protected from modification and unauthorised access,
b. archived and retained for future access, and
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*.

DSD **RECOMMENDS** that:

d. systems be configured to save event logs to a separate, secure log server, and
e. event log data be archived onto write-once media.

Other Logs

User logs

3.7.19. 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

3.7.20. 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 activities, and
g. special or out-of-hour activities.

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

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

Auditing

Purpose

3.7.24. 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

3.7.25. Agencies **SHOULD NOT** assign system audit responsibilities to staff with system administrator privileges.

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

3.7.26. 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

3.7.27. 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

3.7.28. 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.

Vulnerability Analysis

Vulnerability analysis strategy

3.7.29. 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

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

When to perform

3.7.31. 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

3.7.32. Agencies **SHOULD** analyse and treat any risks to its systems identified during a vulnerability analysis.
See: ‘Chapter 4 – Risk Management’ on page 2-22.

Agencies **SHOULD** follow the change process when implementing changes to mitigate the risks.
See: ‘Change Management Process’ on page 2-61.

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 2-66.

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 subjects are covered elsewhere:

Subject	See
Certification of communications security	'Comsec Certification' on page 2-53
Physical security of cabling	'Workstations and Network Infrastructure' on page 3-8
Cryptography	'Chapter 9 – Cryptography' on page 3-91

About Comsec

Definition: Comsec

3.8.5. Comsec is an abbreviation of “communications security”, which covers 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,
- emanations security (including TEMPEST), and
- physical security.

Comsec Handbook

3.8.6. Agencies concerned with the control, handling and/or maintenance of accountable cryptographic communications security material are referred to *ACSI 53 – Communications Security Handbook (Rules and Procedures for the Agency Comsec Officer and Custodian)*, available from DSD.

Accountable Comsec material is defined as classified material bearing the CRYPTO caveat. It applies primarily to cryptographic keying material used in securing HGCE systems.

Agencies operating HGCE should note that information contained in *ACSI 53* supersedes that in this manual.

See: ‘Contacting DSD’ on page 2-3.

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.

Using 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 3-79.

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.

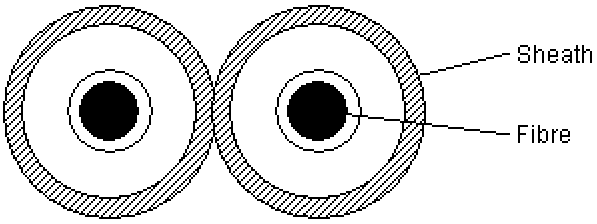


Figure 1

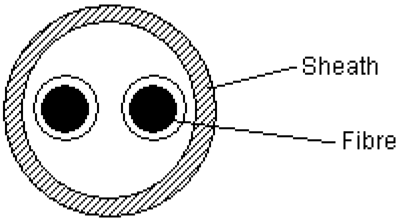


Figure 2

Continued on next page

Fibre optic cables sharing a common conduit (continued)

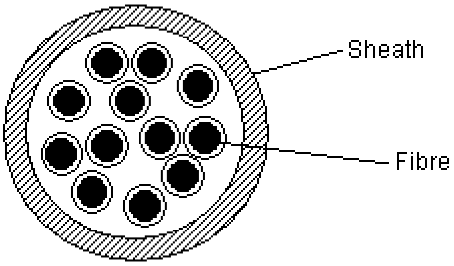


Figure 3

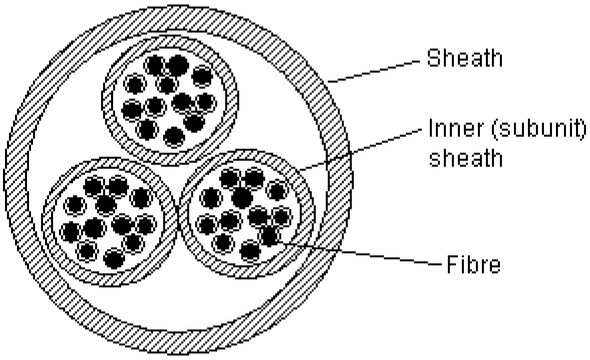


Figure 4

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 identification number,
b. classification,
c. source,
d. destination, and
e. 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

3.8.39. 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

3.8.40. The following subject is covered elsewhere:

Subject	See page
Policy for mobile and cordless telephones	'Cordless and mobile telephones' on page 3-85.

Standards

3.8.41. 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: 'Cryptographic Requirements' on page 3-92.

Pointing devices

3.8.43. As an exception to the general policy on wireless communications defined above, agencies may use wireless pointing devices.

Examples: Mice and track balls.

Infrared keyboards [U, IC, R, P]

3.8.44. As an exception to the general policy on wireless communications defined above, agencies may use infrared keyboards if the following policy is adhered to.

Agencies **SHOULD** advise users to ensure that infrared ports are positioned to prevent line of sight communications travelling into uncontrolled spaces.

Telephones and Telephone Systems

Introduction

3.8.49. This topic discusses the secure use of fixed, cordless and mobile telephones, and the systems used to transmit the information.

Policy specific to technologies such as Voice Over IP (VOIP) is covered later.
See: 'IP Telephony' on page 3-87.

Transmission over the Internet of classified information, including voice calls, is covered by encryption policy.
See: 'Requirements for transit encryption' on page 3-93.

Definition: telephone

3.8.50. A telephone is a device that converts between sound waves and electronic signals that can be transmitted over a distance.

Examples:

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

Definition: telephone system

3.8.51. For the purposes of this manual, a telephone system is defined as an ICT system designed primarily for the transmission of voice traffic.

Examples:

- a private branch exchange, and
- the Public Switched Telephone Network (PSTN).

Note: The Internet is **not** considered to be a telephone system.

User awareness

3.8.52. Agencies **MUST** advise users of the maximum permitted levels of classified conversations for both internal and external telephone connections, as determined by the accreditation of the internal telephone system and the level of the encryption, if any, on external connections.

Agencies **SHOULD** advise users of the audio risk posed by using telephones in areas where classified conversations may occur.

Continued on next page

Visual indication

3.8.53. Agencies permitting different levels of conversation for different kinds of connections **SHOULD** use telephones that give a visual indication of what kind of connection has been made.

Examples:

- If an agency has accredited their internal system to carry PROTECTED conversations, but external calls are only permitted up to IN-CONFIDENCE, then they may use telephones with displays that show a four-digit number for internal calls, and eight digits for external calls. Users would then be advised to double-check this display before talking at a classified level.
- If an agency has chosen to implement encryption on some calls, then they may use phones that display an icon to indicate when a call is encrypted.

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

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

a. the residual risks, as identified by a risk assessment, have been documented and accepted, **and either**
b. the caller and receiver are both located within Australia, **or**
c. all classified traffic that passes over external telephone systems 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 3-93.

Policy relating to the use of cordless and mobile phones is defined below.

Use of telephone systems for classified information [P]

3.8.55. Agencies intending to use 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 classified traffic that passes over external systems 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 3-93.

Cordless and mobile telephones

3.8.57. Agencies **MUST NOT** use cordless or mobile telephones for the transmission of classified information unless the security they use has been approved by DSD for that classification.
See: ‘Chapter 9 – Cryptography’ on page 3-91.

Exception: If the cordless or mobile phone user is located within Australia, and it is included in the formal acceptance of the risk assessment for the agency’s telephone system, IN-CONFIDENCE voice traffic may be transmitted.

Continued on next page

Telephones and Telephone Systems, Continued

Cordless telephones with Secure Telephony Devices

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

Definition: Off-hook audio protection

3.8.60. 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

3.8.61. 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]

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

Emergency services

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

Paging services

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

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

IP Telephony

Definition: IP Telephony

3.8.68. 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.

General guidance

3.8.69. IPT traffic may, with appropriate logical separation, flow over an agency's internal network, and be accredited to carry conversations classified up to the level of the network's accreditation if so desired.

If the internal IPT system is connected to the PSTN, then a secure voice-aware gateway is required, just as a connection from the internal data network requires a secure gateway to connect to the Internet.

In addition, users will need procedures and training to ensure that they do not exceed the maximum permitted levels of classified conversations for internal and external telephone connections.
See: 'User awareness' on page 3-84.

IPT standards

3.8.70. 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, and
b. the standards for telephones and telephone systems.
See: 'Telephones and Telephone Systems' on page 3-84.

Gateways

3.8.71. Where the gateway policy defined in this manual specifies the use of a firewall, agencies implementing IPT **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

3.8.72. 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, including management traffic, through the interface that connects to the PSTN.

Continued on next page

Network separation

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

Note: An agency’s internal IPT network may be accredited to the same classification as the internal data network if all appropriate security controls are in place for that classification, including a secure gateway.
See: ‘IPT standards’ on page 3-87.

Traffic separation

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

Vendor recommendations

3.8.77. 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 phone set up [U, IC, R, P]

3.8.78. Agencies **SHOULD:**

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

Call authentication and authorisation

3.8.80. Agencies **SHOULD** route outgoing call connection requests via a call controller for authentication and authorisation before calls can be established.

Phone to workstation connections [U, IC, R, P]

3.8.81. DSD **RECOMMENDS** that agencies do not connect workstations to IP phones unless the computer and/or the phone, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between IPT and other data traffic.

Definition: softphone

3.8.84. 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.

Continued on next page

Softphone standards [U, IC, R, P]

3.8.85. 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.

Facsimile Machines

Definition: facsimile machine

3.8.87. Within this section, 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 3-124 for additional policies and standards.

Use for the transmission of classified information

3.8.88. 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: 'Telephones and Telephone Systems' on page 3-84.
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

Use of EPL products

3.9.4. Where this manual expresses a minimum assurance requirement for a cryptographic product as an EAL, agencies **MUST** use an EPL product that has completed a DSD cryptographic evaluation in addition to meeting the stated assurance level.

See: ‘Evaluated Products List’ on page 3-20.

EPL products, DACAs and DACPs

3.9.5. Agencies **SHOULD** use an EPL product that has completed a DSD cryptographic evaluation whenever cryptography is being used to protect official information. This applies even when the use of a DACA or DACP is given as the minimum assurance level required to satisfy a “MUST” statement.

Example: An agency using an unevaluated product employing SSL to encrypt PROTECTED information travelling over an IN-CONFIDENCE network is complying with the “MUST” statement requiring the use of a DACP for this scenario, avoiding the need for a waiver. However, they are not using an EPL product, and are therefore required to complete the documentation relating to deviations from a “SHOULD” statement.

See:

- ‘DSD Approved Cryptographic Algorithms (DACAs)’ on page 3-95.
- ‘DSD Approved Cryptographic Protocols (DACPs)’ on page 3-97

Continued on next page

Requirements for storage encryption

3.9.6. 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 algorithm with the given assurance level may be stored and handled as for…**						
	Unapproved/ no encryption	**DACA**	**EAL1**	**EAL2**	**EAL3**	**EAL4**	**HG**
IC	IC	U	U	U	U	U	U
R	R	R	R	U	U	U	U
P	P	P	IC	U	U	U	U

Requirements for transit encryption [IC, R, P]

3.9.7. The table below provides the **minimum** levels of assurance that agencies **MUST** use 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. **Exception:** 'Transit encryption for email' on page 3-94.
RESTRICTED,	• public domain, or • UNCLASSIFIED,	EAL2.
	• IN-CONFIDENCE, • PROTECTED, or • HIGHLY PROTECTED,	a DACP.
PROTECTED,	• public domain, or • UNCLASSIFIED,	EAL2.
	IN-CONFIDENCE,	a DACP.

Continued on next page

Transit encryption for email [IC]

3.9.11. In certain limited circumstances, agencies finding the requirement to use a DACP impractical when emailing IN-CONFIDENCE information to private citizens or small businesses may decide to use either unapproved encryption, or no encryption at all. Doing so in accordance with the policy below will not require any “MUST” statements to be waived, but does require documentation addressing the deviation from the “SHOULD” statement requiring the use of EPL products.
See: ‘EPL products, DACAs and DACPs’ on page 3-92.

Where information is sent to a private entity via email, either unencrypted or encrypted using non-DSD approved cryptography, agencies **MUST** ensure that, prior to sending:

a. the sending and receiving entities are aware of and have accepted the risk,
b. the entity to whom the information relates is aware of and has accepted the risk, and
c. the agency holds documented risk acceptances of all relevant entities.

This risk acceptance may cover ongoing communications; it is not required prior to each individual email.

Important: The protection of IN-CONFIDENCE information may be subject to the *Privacy Act 1988*. DSD **RECOMMENDS** agencies seek legal advice before implementing this option.

DSD Approved Cryptographic Algorithms (DACAs)

Introduction

3.9.12. 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

3.9.13. 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

3.9.14. 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

3.9.15. 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

3.9.16. 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 DACAs and DACPs

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

a. investigate EPL products, 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 3-92 will be met, and
c. consider and accept the risks.

Some risk considerations

3.9.18. 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

DSD Approved Cryptographic Protocols (DACPs), Continued

Implementing DACPs

3.9.19. 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 3-95.

Links

3.9.20. 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)	3-99
Secure Shell (SSH)	3-100
Secure Multipurpose Internet Mail Extension (S/MIME)	3-102

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

Introduction

3.9.21. 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

3.9.22. 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

3.9.23. 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 3-97.

Securing encrypted connections

3.9.24. Agencies permitting SSL or TLS through their gateways **SHOULD** implement:

a. a product that decrypts and inspects the SSL traffic, and/or
b. a whitelist specifying the external addresses to which encrypted connections are permitted, with all other addresses blocked.
   Note: Whitelist addresses may be specified by domain name or IP address.

Secure Shell (SSH)

What is Secure Shell?

3.9.25. 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

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

Standards

3.9.27. Agencies **MUST** ensure that the standards for the use of DACPs are met. **See:** ‘DSD Approved Cryptographic Protocols (DACPs)’ on page 3-97.

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

3.9.28. 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

3.9.29. Agencies **SHOULD NOT** use “ssh-agent” or other similar key caching programs.

Secure Multipurpose Internet Mail Extension (S/MIME)

Introduction

3.9.30. 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

3.9.31. 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

3.9.32. 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 3-97.

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 3-58.

FIPS 140

What is FIPS 140?

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

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

What FIPS 140 is not

3.9.34. 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

3.9.35. 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

3.9.36. 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

3.9.37. 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

3.9.38. 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

3.9.39. 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

3.9.41. 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

3.9.42. 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

3.9.43. 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

3.9.44. 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 3-106.
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

3.9.45. 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 activities, and
e. audit activities.

Accounting

3.9.46. 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.

Audits

3.9.47. 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.

Continued on next page

Key Management, Continued

Area security and access control

3.9.48. 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

3.9.49. 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

3.9.50. 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

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

Continued on next page

KMP contents

3.9.53. The table below describes the minimum contents which **SHOULD** be documented in the KMP.

Note: The level of detail included with the KMP must be consistent with the criticality and classification of the information to be protected.

Topic	Content
Objectives	Objectives of the cryptographic system and KMP, including organisational aims.
References	• Relevant ACSIs. • Vendor documentation. • Related policies.
Classification	Classification of the cryptographic system: • hardware, • software, and • documentation.
System Description	• Maximum classification of information protected. • The use of keys. • The environment. • Administrative responsibilities. • Key algorithm. • Key length. • Key lifetime.
Topology	Diagram(s) and description of the cryptographic system topology including data flows.
Key Management	• Who generates keys. • How keys are delivered. • How keys are received. • Key distribution, including local, remote, central. • How keys are installed. • How keys are transferred. • How keys are stored. • How keys are recovered. • How keys are revoked. • How keys are destroyed.
Accounting	• How accounting will be undertaken for the cryptographic system. • What records will be maintained. • How records will be audited.

Continued on next page

Key Management, Continued

KMP contents (continued)

Topic	Content
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 securing connections between networks.

Contents

3.10.2. This chapter contains the following topics:

Not included

3.10.3. The following subject is covered elsewhere:

Subject	See
Data transfer	'Chapter 11 – Data Transfer' on page 3-126.

Additional references

3.10.4. Additional information relating to network security is contained in the AS/NZS ISO/IEC 17799:2006:

- 10.6 Network security management, and
- 11.4 Network access control.

Network Management

Configuration management

3.10.5. Agencies **SHOULD** keep the network configuration under the control of a central network management authority.

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.

Network diagrams [U, IC, R, P]

3.10.6. Agencies **MUST** have, for each network they manage:
a. a high level diagram showing all connections into the network, and
b. a logical network diagram showing all network devices.

These diagrams **SHOULD**:
c. be updated as network changes are made, and
d. include a "Current as at <date>" on each page.

LAN configuration

3.10.8. Agencies **SHOULD** configure networks to limit opportunities for unauthorised access to information transiting the network infrastructure.

Options to achieve this include the use of:

- switches rather than hubs,
- routers and firewalls isolating parts of the network on a need-to-know basis,
- encryption on the LAN, and
- application-level encryption.

Management traffic

3.10.9. Agencies **SHOULD** ensure that all ICT management traffic travelling across a network is transmitted securely, protected from unauthorised access.

Continued on next page

Limiting network access [U, IC, R]

3.10.10. Where no system within a physical location is classified above IN-CONFIDENCE or RESTRICTED, DSD **RECOMMENDS** that agencies implement network access controls on all networks.

Examples:

- Use of network access control protocols such as 802.1x on all network ports.
- For networks using Dynamic Host Configuration Protocol (DHCP), implement static MAC to IP address assignments.
- Implement port security on network switches to limit access based on MAC address and disable all unused ports.

Internetwork Connections

Internetwork connections

3.10.12. Internetwork policies and standards enable controlled secure information flow and/or access between networks.

Internetwork security standards

3.10.14. Agencies **MUST** 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, and
d. all users operate over the connection within the limits of their required rights and privileges.

Determining the classification of other networks

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

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

3.10.16. 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

3.10.17. When intending to connect an agency network to another non-public domain network, agencies **SHOULD:**

a. obtain 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, particularly where a connection to a public domain network such as the Internet may exist.

Once connectivity is established, agencies **SHOULD** become information stakeholders in the change management process for the other network in order to retain visibility of any increase in the level of risk introduced by changes to the other network.

Gateways

Definition: gateway

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

Definition: one-way gateway

3.10.19. 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 in the less trusted system from entering the more trusted system.

Gateway standards

3.10.20. Agencies **MUST** ensure that:

a. all agency networks are protected from other networks by gateways,

b. all gateways contain a network device to control the data flow that meets the relevant standards, and
See:
- 'Firewalls' on page 3-116 for bi-directional gateways, and
- 'Diodes' on page 3-119 for one-way gateways.

c. for gateways between networks of different classifications, any shared components are managed by the owners of the more highly classified network,

d. the data flow is controlled in accordance with the relevant standards, and
See: 'Chapter 11 – Data Transfer' on page 3-126.

e. all gateway components are physically located within a server room.
See: 'Separation using a server room' on page 3-6.

Agencies **SHOULD** ensure that gateways:

f. are the only communications routes into and out of internal networks,

g. by default, deny all connections into and out of the network,

h. allow only explicitly authorised connections,

i. are managed via a secure path,

j. provide sufficient audit capability to detect gateway security breaches and attempted network intrusions, and

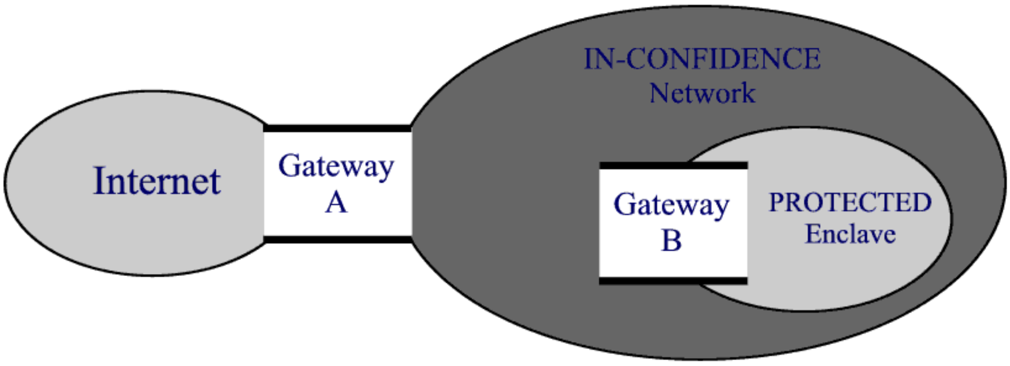
k. provide real-time alarms.

Continued on next page

Cascaded connections

3.10.23. 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 from the IN-CONFIDENCE network 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 a PROTECTED network and the Internet would require an EAL4 firewall, therefore a firewall of this assurance level must be included 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

3.10.25. 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

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

Definition: traffic flow filter

3.10.27. A traffic flow filter is a device configured to automatically filter and control the flow of network data.

Selecting a traffic flow filter

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

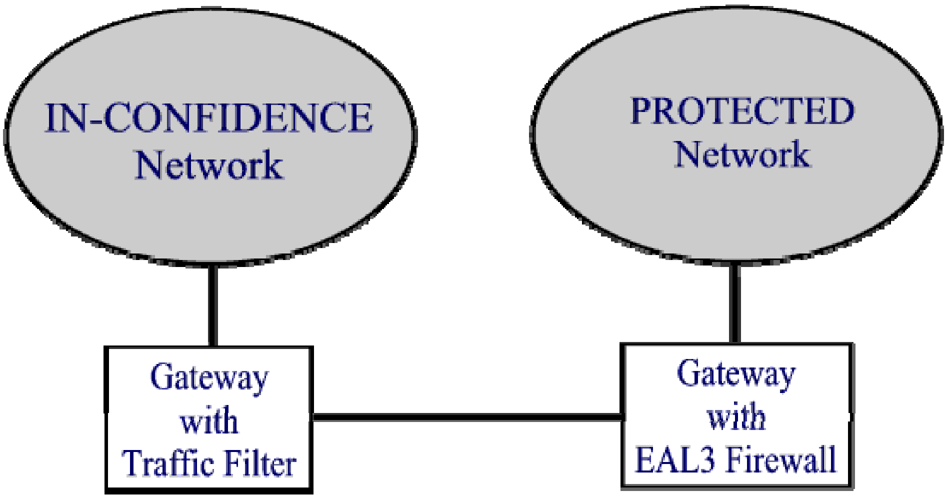
1. A firewall selected from the EPL.
2. A firewall or proxy that is not listed on the EPL.
3. A router with appropriate access control lists configured.

See: 'Product Selection' on page 3-21.

Firewall assurance level example

3.10.29. The following tables define firewall assurance level requirements. They are formulated on the assumption that the policy requiring all networks to be protected from other networks by gateways has been followed.
See: 'Gateway standards' on page 3-114.

Example: (Using the information in the following table.) A gateway exists between your IN-CONFIDENCE network and another agency's PROTECTED network (and you have confirmed that their network meets the security requirements for a network of that classification). Since their network is relatively secure, you only require a traffic flow filter to control the flow of data from it into your network. The other agency, however, requires an EAL3 firewall to control data flowing into its network from yours.



Continued on next page

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

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

See:

- 'Firewall assurance level example' on page 3-116 if you need help interpreting this table.
- 'Selecting a traffic flow filter' on page 3-116 if, according to the table, your gateway requires a traffic flow filter.
- 'Inter-connecting 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

Inter-connecting networks within an agency

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

- either network if the networks are of the same classification and are accredited for the same set of caveats, or
- the less classified of the networks, if it is accredited for the same or fewer caveats than the more highly classified network.
  Note: the requirements for the protection of the more highly classified network from the less classified network must still be met.

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

Personal firewalls

3.10.35. Wherever it is practical to do so, DSD **RECOMMENDS** that agencies implementing firewalls for the protection of individual machines use separate hardware devices in preference to software-based personal firewall applications.

Example: Home-based workers who require remote access to agency systems.

Diodes

Definition: diode

3.10.36. A device that allows data to flow in only one direction.

Content and volume checks

3.10.37. Agencies deploying a diode to control data flow within a one-way gateway **SHOULD** monitor the volume of the data being transferred to ensure that it conforms to expectations.

In addition, data transfer controls are required to manage the data flow.
See: ‘Chapter 11 – Data Transfer’ on page 3-126.

Assurance requirements [PD, U, IC, R, P]

3.10.38. 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.

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]

3.10.43. 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 3-93.

Standards for classified systems

3.10.44. 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 3-92.

Peripheral Switches

Definition: peripheral switch

3.10.45. 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

3.10.46. 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

3.10.48. 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

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

Exceptions:

- A single network, managed in accordance with a single SSP, for which some separation is required for administrative or similar reasons, may use VLANs to achieve that separation.
- 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

3.10.50. 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

3.10.52. 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

3.10.53. Within this manual, the term "multifunction devices" (MFDs) refers to the class of devices that combines 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:

- 'Telephones and Telephone Systems' on page 3-84, and
- 'Facsimile Machines' on page 3-90.

Risks with MFDs

3.10.54. 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.

Copying documents

3.10.55. Agencies **MUST NOT** permit network-connected MFDs to be used to copy documents classified above the level of the connected network.

Usage [IC, R]

3.10.56. Agencies **SHOULD NOT** enable a connection from an MFD to a telephone network of a lower classification unless the MFD:

a. has been evaluated to EAL2, and the scope of the evaluation includes:
   1) information flow control functions to prevent unintended and unauthorised data flows,
   2) data export controls capable of blocking information based on protective markings,
   3) authentication, and
   4) audit data generation and protection,

b. is configured to use the evaluated functionality in accordance with the relevant policies.

   See:
   - 'User Identification and Authentication' on page 3-61,
   - 'Event Logging' on page 3-70, and
   - 'Chapter 11 – Data Transfer' on page 3-126.

Usage [P]

3.10.57. Agencies **SHOULD NOT** enable the facsimile functionality of MFDs unless the telephone network is accredited to at least the same classification as the computer network.

Continued on next page

Policies, plans and procedures

3.10.59. Agencies deploying MFDs **MUST** develop a set of policies, plans and procedures governing the use of the equipment.

Chapter 11 – Data Transfer

Overview

Introduction

3.11.1. 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]

3.11.2. 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.

User responsibilities

3.11.4. Agencies **MUST** ensure that users:

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

Definition: trusted source

3.11.5. A trusted source is:

- a person or system formally identified as being capable of reliably producing information meeting certain defined parameters, such as a maximum data classification, or
- a person formally identified as being capable of reliably reviewing information produced by others to confirm compliance with certain defined parameters.

Examples: Trusted sources may include:

- trained sanitisation officers tasked with sanitising data for release to less classified systems,
- competent releasing officers tasked with reviewing data submitted by others for release to less classified systems,
- an accredited system that automatically generates messages designed for release to less classified systems, and
- an automated database replication tool known to operate in an assured manner.

Continued on next page

Overview, Continued

Contents

3.11.6. This chapter contains the following topics:

Content Filtering

Definition: filter

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

Examples: Email content scanners and “dirty word” checkers.

Filtering techniques

3.11.8. The table below identifies some 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 all 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 header to determine the 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 to 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 over-classified information and other suspicious content that an automated system may miss; particularly important for the transfer of image files.

Limiting transfers by file types [U, IC, R, P]

3.11.9. Agencies **SHOULD** strictly define and limit the types of files that may be transferred, based on business requirements and the results of a risk assessment.

The level of risk will be affected by the degree of assurance agencies can place in the ability of their data transfer filters to:

- confirm the file type by examination of the contents of the file,
- confirm the absence of malicious content,
- confirm the absence of inappropriate content,
- confirm the classification of the content, and
- handle compressed files appropriately.

Blocking suspicious data

3.11.11. Agencies **MUST** block or drop any data identified by a data filter as suspicious until/unless reviewed and approved for transfer by a trusted source other than the originator.

Temporary Connections

Introduction

3.11.12. Interconnecting networks are protected from each other by secure connections known as gateways. In general, however, the temporary connection of a single device will not occur through a traditional gateway. Security controls are therefore needed to ensure that only authorised information flows over the connection.

In addition to the policy defined here, data transfer controls are required.
See: ‘Data Import’ on page 3-131, and ‘Data Export’ on page 3-132.

Definition: temporary connection

3.11.13. A temporary connection occurs when a system can communicate directly with another device or removable media item via a temporary, human-initiated link.

Examples:

- reading to and writing from removable media inserted into a workstation,
- connecting a PED to a system to update information, and
- connecting a laptop to a network to send a few emails.

Airgapped transfers

3.11.14. Agencies transferring data manually between two agency systems **SHOULD** use:

a. a previously unused piece of media,
b. a pool of media items used **only** for data transfer between the two relevant systems, or
c. a media item which has been sufficiently sanitised to permit its reuse on the less classified of the systems between which the data transfer is occurring.
See: ‘Media Sanitisation’ on page 3-32.

Over-classification of media

3.11.15. Agencies **MUST NOT** insert media of any classification into a system of a lower classification.

Classification of media [IC, R, P]

3.11.16. Agencies intending to classify a media item below the classification of the system in which it is inserted **SHOULD** ensure that:

a. the media is read-only,
b. the media is inserted into a read-only device, or
c. all data transfers to the media are performed in accordance with agency policy on data export.
See: ‘Data Export’ on page 3-132.

Agencies not meeting the above requirement **SHOULD** classify all removable media interacting with a system at the classification of that system.

Continued on next page

Connection of portable computers and PEDs [U, IC, R, P]

3.11.19. Agencies intending to allow portable computers or PEDs to be temporarily connected to a system of a different classification **MUST** ensure that a firewall of the appropriate assurance is used to protect the more highly classified side of the connection.

This requirement does not apply when a device is using a network purely as a carrier for appropriately encrypted traffic to a remote system.
Example: An IN-CONFIDENCE laptop does not require a firewall when it is using the Internet to carry only an approved VPN connection back to the agency's IN-CONFIDENCE network.

If the high side is…	And the low side is…	Then the minimum firewall assurance is…
UNCLASSIFIED,	public domain,	a traffic flow filter.
IN-CONFIDENCE,	• public domain, • UNCLASSIFIED,	an EAL2 firewall.
RESTRICTED,	• public domain, • UNCLASSIFIED, or • IN-CONFIDENCE,	an EAL2 firewall.
PROTECTED,	• public domain, or • UNCLASSIFIED,	an EAL4 firewall.
	• IN-CONFIDENCE, or • RESTRICTED,	an EAL3 firewall.

Unaccredited devices

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

Data Import

Additional policy

3.11.23. Where the data import occurs via a connection between networks, as opposed to a temporary connection, policy relating to gateways, firewalls and diodes also applies.

See: ‘Chapter 10 – Network Security’ on page 3-109.

Data import [U]

3.11.24. Agencies importing data to an UNCLASSIFIED system **SHOULD** ensure that the data is scanned for malicious and active content.

Data import to a classified system

3.11.25. Agencies importing data to a classified system **MUST** ensure that the data is scanned for malicious and active content.

Exceptions:

- Malicious content may be imported to isolated systems specifically designed for the storage, analysis and/or transmission of such content.
- Where the type of data cannot be effectively scanned, and the source and/or content of the data is strictly limited to known safe states, the Accreditation Authority may choose to approve the importation of unscanned data.
  Example: Importing automatically generated image files from a fully certified and accredited system known to operate in an assured manner.

Data Export

Additional policy

3.11.27. Where the data export occurs via a connection between networks, as opposed to a temporary connection, policy relating to gateways, firewalls and diodes also applies.

See: ‘Chapter 10 – Network Security’ on page 3-109.

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

3.11.28. Agencies **SHOULD** restrict the export of data to a less classified system by filtering data using at least protective marking checks.

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
DMZ	Demilitarised Zone
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
EPL	Evaluated Products List
FIPS	Federal Information Processing Standard
GSM	Global System for Mobile communications
HG	High Grade
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
LAN	Local Area Network

Continued on next page

Abbreviations, Continued

MAC	Media Access Control
MFD	Multifunction Device
MMS	Multimedia Messaging Service
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
SOE	Standard Operating Environment
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.

Availability Ensures that authorised users have access to information and associated assets when required.

Business continuity Ensures the ongoing availability of identified processes and resources in support of critical business objectives.

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.

Continued on next page

Certification

The assertion by a Certification Authority that compliance with a standard has been achieved, based on a comprehensive evaluation. Certification is generally a prerequisite for accreditation.

Certification authority

An entity with the authority to assert that ICT systems comply with the required standards.

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: 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.

Communications security

See: Comsec.

Control

A measure that is taken to mitigate risks.

Continued on next page

Control register

A document used in the RMP to record the controls required for a site.

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

DSD Approved Product. The term is now obsolete.

Declassification, media

The administrative decision to remove all classifications from the media, based on an assessment of relevant issues including the consequences of damage from disclosure or misuse, the effectiveness of any sanitisation procedure used, and the intended destination of the media.

Degaussing

The process of applying a magnetic force to remove information from media.

Continued on next page

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.

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.

Emanations security

Emanations security includes, but is not limited to, consideration of:

- audio,
- visual,
- infrared, and
- electromagnetic emissions.

TEMPEST security is a subset of emanations security.

Encryption

The art or science concerning the principles, means, and methods for rendering plain information unintelligible.

EPL

The Evaluated Products List identifies products that:

- have completed a CC, ITSEC and/or some other DSD approved evaluation,
- are currently undergoing CC or ITSEC evaluation within the AISEP, or some other form of evaluation within DSD, or
- have completed a CC or ITSEC evaluation through a recognized overseas scheme

It is available on the DSD website.
URL: www.dsd.gov.au/infosec/evaluation_services/epl/epl.html

Continued on next page

Evaluation assurance level

See: EAL.

Firewall

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

Firmware

Software embedded in a hardware device.

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.

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.

Hardware

The physical components of computer equipment including peripheral equipment.

Examples:

- personal and mainframe computers,
- laptops,
- printers,
- routers,
- personal digital assistants (PDAs), and
- mobile phones.

Continued on next page

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: 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.

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.

Continued on next page

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.

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.

Continued on next page

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.

Provisional certification

Provisional certification may be granted by a Certification Authority when the system is lacking compliance in some non-critical aspect(s) of the design, policy or management.

It is issued to indicate that full certification can be expected, subject to successful completion of the provisions identified in the certification report.

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.

Reclassification, media

The administrative decision to change the classification of the media, based on an assessment of relevant issues including the consequences of damage from unauthorised disclosure of misuse, the effectiveness of any sanitisation procedure used, and the intended destination of the media.

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.

Traffic flow filter

A device that has been configured to automatically filter and control the flow of network data.

Continued on next page

Trusted source

A trusted source is:

- a person or system formally identified as being capable of reliably producing information meeting certain defined parameters, such as a maximum data classification, or
- a person formally identified as being capable of reliably reviewing information produced by others to confirm compliance with certain defined parameters.

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.

Whitelist

A whitelist defines a set of accepted items. This set is inclusive, confirming that the item being analysed is acceptable. It is the opposite of a blacklist which confirms that items are not acceptable.

Examples:

- A spam filter may use an email whitelist to specify email addresses, IP addresses or domain names from which emails will be accepted.
- A locked down computer may have a software whitelist defining which programs may be executed on the system.

Index