ACSI 33
Changes in the September 2005 Release

Overview

Introduction

The *Australian Government Information and Communications Technology Security Manual*, also known as *ACSI 33*, was first released in its current form in March 2004. Updates to the manual will be released twice a year. Documents covering the changes made in each update will also be published with each new release.

This document covers the changes made to the *Australian Government ICT Security Manual* in the September 2005 release, as compared to the March 2005 release.

Not included

The following types of amendments have **not** been noted in this document:

- typographical corrections,
- changes to the Index, and
- additions to the Abbreviations section.

Versions

Two versions of this document have been produced, one at UNCLASSIFIED, the other at SECURITY-IN-CONFIDENCE, consistent with the two versions of ACSI 33.

Changes that apply only to the SECURITY-IN-CONFIDENCE version of the manual will be included only in the SECURITY-IN-CONFIDENCE version of this document.

Continued on next page

Terminology

When referring to information within the manual, the following definitions are used:

- **version** refers to the classification of the manual, either UNCLASSIFIED or SECURITY-IN-CONFIDENCE,
- **release** refers to the month and year it was published,
- **block** refers to a set of information delineated by horizontal lines within the manual.

Note: Page numbers are not referenced, as they may not be consistent between versions or releases.

Feedback

Numerous comments and suggestions relating to the manual have been received. Some of the changes noted in this document are a direct result of this feedback. Many other comments will require more time to resolve effectively, and the results will be seen in future releases.

Feedback on this latest release of the manual, and on the format and/or content of this document, is also encouraged.

Contact details are in the manual, block 2.1.5.

Contents

This document contains the following topics:

Summary of Major Changes

Introduction

The following blocks summarise the most significant changes included in the September 2005 release of the manual. More detail on these changes is given in the last section, ‘Listing of Changed Blocks’.

Compliance

The compliance statement defining agencies’ responsibilities to comply with ACSI 33 within two years, previously published on the ACSI 33 Information page on DSD website, has now been incorporated into the manual with slight amendments.

Block reference: 1.0.2.1.

Definition: Accreditation

The definition of accreditation has been amended to clarify that **all** ICT systems, not just classified systems, require accreditation, and that accreditations involve approving an ICT system for information classified up to a specified level.

Block reference: 2.7.6.

Magnetic media sanitisation

A new column has been added to the table to define the requirements for overwriting magnetic media prior to release to the public domain. The major impact of this is that when, for example, auctioning previously UNCLASSIFIED computers, or throwing floppy disks in the bin, the media **MUST** be overwritten; formatting the media without overwriting it is not sufficient.

Block reference: 3.4.38.

Email protective marking policy

Policy advising agencies that they **SHOULD NOT** allow protective markings to be inserted into user-generated emails without user intervention has been added.

Block reference: 3.5.44.1.

IP telephony

Significant additions and changes to policy on the use of IP telephony have been made.

Block references: 3.8.52-59.

Continued on next page

Summary of Major Changes, Continued

Use of telephones in classified areas

Various changes have been made to the policy on recommended methods of ensuring off-hook audio protection for telephones in areas where classified conversations may be held.

Block references: 3.8.61-66.

Data transfer

Significant changes have been made to the format of this section, to improve clarity, and make it clearer that this policy applies to all forms of data transfer, from complex gateways to rarely used manual, air-gapped procedures.

The policy itself has undergone only minor changes; further changes are likely for the first ACSI 33 release of 2006.

Block references: 3.10.34-41.

Summary of Moderate Changes

Introduction

The following blocks summarise the changes included in the September 2005 release that have the potential for a moderate impact on users. More detail on these changes is given in the last section, 'Listing of Changed Blocks'.

Paragraph applicability

The statement "applies to all classifications and caveats" has been replaced with "applies to all ICT systems" in order to remove the ambiguity that could allow people to say that unlabelled blocks don't apply to UNCLASS systems.

Block reference: 1.0.8.

Definition: ICT system classification

A new block defining an ICT system classification as the highest classification for which the system is accredited has been added.

Block reference: 1.0.23.1.

Analysing the risks

The examples given for Moderate consequences were corrected, as they had been typed out incorrectly.

Block reference: 2.4.26.

Developing security SOPs

A requirement for agencies to ensure that SOPs are consistent with all relevant SSPs has been added.

Block reference: 2.6.7.

SOP contents

Some security-specific issues have been added to the list of issues the System Manager's SOPs should cover.

Block reference: 2.6.12.

Certification Authority

A definition for "Certification Authority" has been added.

Block reference: 2.7.4.1.

Continued on next page

Summary of Moderate Changes, Continued

Certification to ACSI 33

The statement defining which ACSI 33 releases were valid for certification to Australian standards, previously published on the ACSI 33 Information page on DSD website, has now been incorporated into the manual. The policy has been amended to remove the focus on March releases.

Block reference: 2.7.4.2.

Classification of system accreditations

The implied requirement not to have information classified above the level of a system's accreditation located on the system has now been formally stated.

Block reference: 2.7.10.1.

System accreditation for caveats

This block, which originally stated a requirement for systems with AUSTEO and AGAO material to be accredited as such, has been extended in scope to apply to all caveated material.

Block reference: 2.7.11.

Security incidents: standards

The requirements for security incident detection have been amended to focus on intrusion detection strategies rather than just intrusion detection system software, and to highlight the value of prevention rather than just detection.

Block reference: 2.8.12.

Timing of security reviews

The scope of the requirement to review systems has been expanded to include UNCLASSIFIED systems.

Block reference: 2.9.3.

Frequency of security reviews

The statement "Agencies **MUST** review the security of their ICT systems" has been removed, reducing the requirement to a "**SHOULD**", as stated by the previous block.

Block reference: 2.9.4.

Product selection

The requirement for agencies to acknowledge and accept the risks they take using non-DAP products has been clarified and defined as a "**MUST**".

Block reference: 3.3.12.

Continued on next page

Operation of DAPs

A requirement for agencies to operate High Grade products in accordance with all applicable DSD standards has been added.

Block reference: 3.3.22.

Off-site repairs

Changes to the intent and format of the policy for off-site repairs have been made.

Block references: 3.4.22, 3.4.22.1, 3.4.23.

Media sanitisation

Sanitisation methods for EPROMs, EEPROMs and flash memory have been updated, and a colour intensity check added to the sanitisation procedures for video screens.

Block references: 3.4.32-34.

Database search engines

The requirement to sanitise document titles that may be seen by users not entitled to access the contents has been increased from “**SHOULD”** to “**MUST”**.

Block reference: 3.5.19.

Web usage policy

Agencies are now required to have a web usage policy if they allow Internet browsing.

Block reference: 3.5.20.1.

Applications and plug-ins

The requirement to block the automatic execution of files downloaded from websites has been increased from a “**RECOMMENDS**” to a “**SHOULD**”.

Block reference: 3.5.25.

Automatic forwarding of received emails

The policy on the automatic forwarding of emails has been updated to mandate compliance with the policy on blocking of emails based on their protective markings.

Block reference: 3.5.36.

Continued on next page

Summary of Moderate Changes, Continued

Email technical standards

The standards relating to blocking emails were expanded and moved into a separate block, and a requirement to ensure that account names cannot be determined from external mail servers was added.

Block references: 3.5.40, 3.5.40.1.

Blocking of unmarked emails

The option to block unmarked emails at the server, rather than just at the user's computer, was added.

Block reference: 3.5.50.

Blocking of outbound emails

The scope of the policy was extended to apply to emails leaving any system, rather than just emails leaving an agency.

Block reference: 3.5.51.

Software development environment

The requirement to have a completely separate environment for software development has been reduced; environments may now be linked, but the information flow must be tightly controlled.

Block reference: 3.5.55.

Authentication methods: PINs

The use of PINs as the sole authentication method has been expressly prohibited.

Block reference: 3.6.9.

Protecting authentication information

A requirement to ensure that staff do not store authentication data with the system or device to which it gains access has been added.

Block reference: 3.6.9.1.

Password management

The password policy was extended to include a requirement to prevent users from reusing any of the last 8 passwords.

Block reference: 3.6.13.

Continued on next page

Summary of Moderate Changes, Continued

Group accounts

A requirement to have an alternate means of identifying the current user of a shared account has been added.

Block references: 3.6.28, 3.6.29.

Logon banners

Agencies are now required to have logon banners requiring a user response prior to gaining access to a system.

Block reference: 3.6.30.1.

Intrusion detection / Active security

Part 3, Chapter 7 has been renamed from "Intrusion Detection" to "Active Security", and much of its contents have been retitled to better fit their subject matter. A clearer distinction in terminology between logging events and auditing the results has also been made.

Chapter reference: 3.7.

Intrusion detection strategy

Agencies are now required to have a strategy for intrusion detection.

Block reference: 3.7.3.

Logging requirements

The list of issues that must be addressed by documented logging requirements has been amended to include availability and delivery reliability requirements, while details relating to audit requirements have been removed from this block.

Block reference: 3.7.7.

Event log facility

The list of details that must be recorded for each event has been expended to include event description, event source, and terminal location, where applicable.

Block reference: 3.7.8.

System management log

The requirement to have a system management log has been reduced to a "RECOMMENDS" for UNCLASSFIIED, X-IN-CONFIDENCE, RESTRICTED and PROTECTED systems.

Block reference: 3.7.14.1.

Continued on next page

Summary of Moderate Changes, Continued

Audit requirements

A new block defining audit requirements that must be addressed by agencies has been added.

Block reference: 3.7.16.1.

Cordless and mobile telephones

RESTRICTED conversations may no longer be conducted on unsecured cordless or mobile phones, and IN-CONFIDENCE connections are limited to voice traffic only.

Block references: 3.8.68, 3.8.69.

Requirements for storage encryption

The requirement to store authentication information separately from the device has been removed from this block, expanded and included as block 3.6.9.1.

Block reference: 3.9.5.

Network management

This block has been deleted, as the relevant policy requirements are already covered elsewhere.

Block reference: 3.10.5.

Multilevel networks

This block has been deleted, as the recommendations it contained added little value. Multilevel networks are a complex subject, and more comprehensive policy addressing their use will be developed for future releases.

Block reference: 3.10.8.

Internetwork security standards

This list of high-level requirements has been amended to better reflect the needs of all connected networks, and to delete requirements already specified elsewhere.

Block reference: 3.10.10.

Determining network classifications

Policy addressing how to determine the effective classification of external networks to which the agency is connecting has now been added.

Block reference: 3.10.10.1.

Continued on next page

Summary of Moderate Changes, Continued

Gateway standards

Gateways, which facilitate the transfer of data between networks, must comply with the policy on data transfer. This requirement has been highlighted by the inclusion here of a reference to the Data Transfer section.

Also, the requirement to deny inbound connections by default has been expanded to cover outbound connections as well.

Block reference: 3.10.15.

Remote access [U]

New requirements for the protection of remote access to UNCLASSIFIED systems have been added, including a requirement to protect privileged remote access to UNCLASSIFIED systems as if the information was classified as IN-CONFIDENCE.

Block reference: 3.10.42.1.

Virtual Private Networks

This section has been deleted, as the contents were of very limited value; the security issues relating to the use of VPNs are already addressed by policy elsewhere in the manual.

The only actual change to policy resulting from the deletion is the removal of the requirement to use a DAP for all VPN implementations. The requirement for VPN product assurance is now covered by the general assurance requirements for transit encryption.

Block references: 3.10.44-47.

Glossary changes

The following terms have been added or amended in the Glossary:

- Audit,
- Caveat,
- Host-based Intrusion Prevention System (HIPS), and
- TOP SECRET area.

Listing of Changed Blocks

Introduction

This section contains a complete listing of all blocks that have been added, deleted, or significantly amended.

Various other minor changes have been made to improve the readability, accuracy or consistency of the manual. These changes have no impact on policy, and are not included here.

Deleted blocks

Deleted blocks are indicated within the September 2005 release by a block label. The block text has been replaced with "<deleted>", and the block number is retained.

Blocks affected: 2.6.3, 3.2.14, 3.2.16, 3.3.27, 3.5.9, 3.5.16-17, 3.6.7-8, 3.7.10-11, 3.8.34, 3.10.35, 3.10.38, 3.10.44-47.

Added blocks

All added blocks have been copied in their entirety (not including unchanged tables) into this section. Added blocks are indicated by a fourth field in the block number.

Example: 2.7.4.3. is the third in a series of new blocks inserted after block 2.7.4.

Renumbered lists

Several blocks contain multiple sets of numbered list items. These lists, which were formatted to restart the numbering each time, have now been renumbered so that they are continuous within each block. This will ensure that it is no longer possible to have, for example, two unique policy requirements both referred to as 2.1.8 (a).

Blocks affected: 2.1.8, 2.8.35, 3.3.26, 3.6.6, 3.6.18, 3.8.22, 3.9.44, 3.10.15.

Format

From this point onward, all blocks are presented as they appear in the September 2005 release, with the exception that any unchanged tables within a block have not been shown, and unchanged rows within tables have been labelled as such.

Continued on next page

Compliance

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

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

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

Paragraph applicability and system classifications

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

Definition: ICT system classification

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

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

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…
<unchanged>	catastrophic.
<unchanged>	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.
<unchanged>	minor.
<unchanged>	insignificant.

Continued on next page

Relationship between SSP and SOPs

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

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

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

System Manager SOPs

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

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

Topic	Procedures that SHOULD be included
System maintenance	Managing the ongoing security and functionality of system software and hardware, including: a. maintaining awareness of current software vulnerabilities, b. applying appropriate hardening techniques, and c. updating anti-virus software.
Hardware destruction	Managing the destruction of unserviceable equipment and media.
User account management	<unchanged>
Configuration control	<unchanged>
Access control	<unchanged>
System backup and recovery	<unchanged>

Certification Authority

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

Continued on next page

Certification to Australian Government standards

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

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

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

Reviewing certification reports

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

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

Definition: accreditation

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

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

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

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

Continued on next page

System accreditation: classification

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

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

System accreditation: caveats

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

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

Examples:

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

Standards

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

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

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.

Continued on next page

User awareness

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

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

Tools used

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

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

Handling malicious code infection

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

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

Step	Action
1	<unchanged>
2	Scan all connected systems, and any media used within a set period leading up to the incident, for malicious code. **Note:** Consider the infected date of the machine, and the possibility that the record may be inaccurate, when determining the appropriate period. **Result:** Infected systems and media are identified.
3	<unchanged>
4	<unchanged>
5	Report the incident and perform any other activities required by the incident response plan. **See:** • 'Reporting of incidents' on page 2-xx for information on reporting requirements and additional assistance available from DSD. • 'Incident Response Plan' on page 2-xx.

Continued on next page

Developing the plan – additional standards

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

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

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.

Contact details

3.1.7. T4 can be contacted via:

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

T4 Protective Security
GPO Box 2176
Canberra ACT 2601

Continued on next page

Storage authority

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

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

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-xx.

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

Degree and content of security training

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

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

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

Continued on next page

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

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

See: Part D of the *PSM*.

Standards

3.3.10. Agencies **SHOULD** use a DAP when they are relying on the product to enforce security functionality for the protection of classified Australian Government information and systems. Policy stated elsewhere in this manual may specify more rigorous requirements for particular technology types.

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

Other options

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

a. products that are listed on DSD's EPL as either a Certified Product or as a product currently in evaluation,
b. products that are in evaluation by a foreign scheme with which the AISEP has a recognition agreement, and
c. products that have had no formally recognised evaluation.

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

Continued on next page

Listing of Changed Blocks, Continued

Operation of DAPs

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

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

Secure disposal

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

See: ‘Disposing of Hardware’ on page 3-xx.

Classifying hardware

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

Labelling hardware and media

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

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

Off-site repairs [IC, R, P]

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

a. use a repair company approved for that purpose by the agency, or
b. use any other company if:
    1) the media within the hardware is sanitised and declassified, or
    2) the hardware is escorted at all times by an appropriately cleared and briefed escort and due care is taken to ensure that official information is not compromised.

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

Continued on next page

Approved media sanitisation methods [IC, R, P]

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

Media type	Sanitisation method
Magnetic media	<unchanged>
Erasable Programmable ROM (EPROM)	Erase as per the manufacturer's specification, increasing the specified UV erasure time by a factor of three.
Electrically Erasable Programmable ROM (EEPROM)	Erase as per the manufacturer's specification.
Flash memory **Example:** • Memory sticks • Thumb drives	Erase as per the manufacturer's specification, or using a third party tool. Agencies **SHOULD** verify the effectiveness of the erasure process before approving it for use as a sanitisation method. If no effective process is available, then the media **SHOULD** be destroyed. **Note:** Many manufacturers' "erasure" processes merely obscure the data, and tools designed to recover such data are readily available.
<unchanged>	<unchanged>
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

Overwriting procedure: determining *X*

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

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

Storage and handling

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

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-xx.

Operation

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

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

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

Continued on next page

Device configuration

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

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

Standards for malicious code counter-measures

3.5.8. Agencies **MUST**:

a. develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering how to:
   1) minimise the likelihood of malicious software being introduced into the system(s),
   2) detect any malicious software installed on the system(s),
b. make their users aware of the agency's policies, plans and procedures
c. <deleted, see 3.5.9.1.>
d. <deleted>, and
e. ensure that all instances of detected malicious code outbreaks are handled according to the procedures.

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

Anti-virus scanners

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

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

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

Host based intrusion prevention systems

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

Continued on next page

Integrity checking

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

Active content blocking

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

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

Data labelling

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

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

Database files

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

Accountability

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

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

Search engines

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

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

Web usage policy

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

Continued on next page

Applications and plug-ins

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

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

Servers and clients

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

Automatic forwarding of received emails

3.5.36. Agencies **MUST** ensure that the standards for blocking unmarked and outbound emails are also applied to automatically forwarded emails.
See:

- 'Blocking of unmarked emails' on page 3-xx.
- 'Blocking of outbound emails' on page 3-xx.

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.

Email security documentation standards

3.5.39. Agencies **MUST**:

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

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

Continued on next page

Email technical standards

3.5.40. Agencies **SHOULD:**

a. harden and patch email servers and clients,
b. restrict access to email servers to administrative users,
c. <deleted, see 3.5.40.1.>
d. configure auditing to produce logs and analyse the logs for any security issues,
e. ensure that email servers available to the public are separated from the agency's internal systems,
f. disable open mail relaying so that mail servers will only relay messages destined for the agency's domain(s) and those originating from within the domain, and
g. ensure that account names cannot be determined from external mail servers.

Technical standards for blocking emails

3.5.40.1. Agencies **SHOULD** block:

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

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

Marking tools

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

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

Blocking of unmarked emails

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

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

Continued on next page

Blocking of outbound emails

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

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

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

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

Blocking of inbound emails

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

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

Software development environments

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

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

Continued on next page

Methods for user identification and authentication

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

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

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

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

Protecting authentication information

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

Password management

3.6.13. Agencies **SHOULD**:

a. require passwords to be changed at least every 90 days,
b. prevent users from changing their password more than once a day,
c. check passwords for poor choices,
d. force the user to change an expired password on initial logon or if reset, and
e. **NOT** allow passwords to be reused within 8 password changes.

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

Reset passwords **SHOULD NOT** be predictable.
Examples: “password” or a user’s SID should not be used.

Continued on next page

Screen and session locking

3.6.15. Agencies **SHOULD:**

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

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.

Definition: privileged access

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

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

Note: Users with privileged access are called privileged users.

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

See: ‘Chapter 1 – ICT Security Roles and Responsibilities’ on page 2-xx.

Continued on next page

Use of privileged accounts

3.6.20. Agencies **SHOULD**:

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

Group accounts

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

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

Logon banner

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

The banner may cover issues such as:

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

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.

Definition: intrusion detection system

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

Continued on next page

Intrusion detection strategy

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

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

Event management and correlation

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

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

IDSs on Internet gateways

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

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

IDSs on other gateways

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

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

Configuring the IDS

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

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

Continued on next page

Logging requirements

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

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

Event log facility

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

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

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

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

Continued on next page

Event logs for software components

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

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

If the software component is a(n)…	Then the RECOMMENDED events to log include…
database	• user access to the database, • attempted user access that is denied, **Example:** Access denial due to incorrect password. • changes to user roles or database rights, • addition of new users, especially privileged users, • modifications to the data, and • modifications to the format of the database.
<unchanged>	<unchanged>

User logs

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

a. maintain a secure log of all authorised users, their user identification and who provided the authorisation and when, and
   Note: In many cases this could be achieved by retaining the account application form filled in by the user and/or their supervisor.
b. maintain the log for the life of the system.
   Important: The retention of user logs may be subject to the *Archives Act 1983*.

System management log information

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

a. sanitisation activities,
b. system startup and shutdown,
c. component or system failures,
d. maintenance activities,
e. housekeeping activities,
   Examples: Backup and archival runs.
f. system recovery procedures, and
g. special or out-of-hour activities.

Continued on next page

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

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

Purpose

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

Responsibilities

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

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

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

Audit requirements

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

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

How to audit an event log

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

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

Continued on next page

Resources

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

Vulnerability analysis strategy

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

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

When to perform

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

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

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

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).

Definition: IP Telephony

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

Continued on next page

Standards

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

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

Gateways [U, IC, R, P]

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

See: 'Gateways' on page 3-xx.

Connection to the PSTN

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

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

Network separation

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

Traffic separation [U, IC, R, P]

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

Infrastructure hardening [U, IC, R, P]

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

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

Continued on next page

Call authentication and authorisation

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

Vendor recommendations

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

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

IP phones

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

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

3.8.59.2. Agencies **SHOULD:**

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

DSD **RECOMMENDS** that agencies:

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

Securing IP phone firmware upgrades

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

Definition: softphone

3.8.59.5. A softphone is a software application that allows a computing device, such as a desktop computer, to act as an IP phone, using either a built-in or an externally connected microphone and speaker. It may also be known as a software IP phone.

Continued on next page

Softphone standards [U, IC, R, P]

3.8.59.6. Agencies **SHOULD NOT** use software phones.

If an agency deviates from this standard, then DSD **RECOMMENDS** that the agency have a separate, dedicated Network Interface Card (NIC) on the host for voice network access.

Use of telephones near classified conversations

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

Definition: Off-hook audio protection

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

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

Definition: Push-to-Talk

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

Requirement for off-hook audio protection [P]

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

Cordless and mobile telephones [IC]

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

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

Continued on next page

Cordless and mobile telephones [R, P]

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

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

Requirements for storage encryption

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

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

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

Internetwork security standards

3.10.10. Agencies **SHOULD** ensure that:

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

Continued on next page

Determining the classification of other networks

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

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

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

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

Gateway standards

3.10.15. Agencies **MUST** ensure that:

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

Agencies **SHOULD** ensure that gateways:

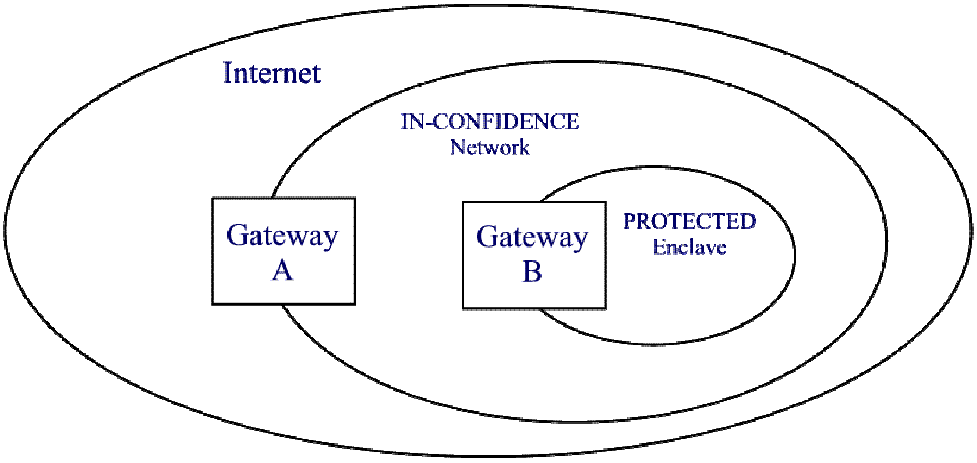
a. are the only communications routes into and out of internal networks,
b. by default, deny all connections into and out of the network,
c. allow only explicitly authorised connections,
d. are managed via a secure path,
e. provide sufficient audit capability to detect gateway security breaches and attempted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

Continued on next page

Cascaded connections

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

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



See:
- 'Definition: cascaded connections' on page 3-xx.
- 'Firewalls' on page 3-xx.
- 'Diodes' on page 3-xx.

Selecting a traffic flow filter

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

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

Continued on next page

Introduction

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

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

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

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

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

Media

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

a. previously unused piece of media, or
b. pool of media items created **only** for transfer.

Agencies **SHOULD NOT** transfer data using media that has previously contained data of a higher classification than the systems between which the data is being transferred.

Definition: filter

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

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

Filtering standards [U, IC, R, P]

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

Continued on next page

Filtering techniques

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

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

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

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

a. protective marking checks.

Data import from a less classified system

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

Continued on next page

User responsibilities

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

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

Definition: remote access

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

Standards [U]

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

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

Continued on next page

Connectivity standards

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

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

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