Australian Government
Department of Defence
Intelligence and Security

Australian Government Information Security Manual

JUNE 2011

Foreword

Improving cyber defence is a top national security priority and the Australian Government has invested significantly in enhancing cyber security capabilities over a number of years. The *Australian Government Information Security Manual* forms an important part of the Government strategy.

Cyber threats can come from a wide range of sources, including individuals, issue motivated groups, organised criminal syndicates and nation states. The nature of the Internet makes it difficult to attribute intrusions to particular sources, but it is reasonable to assume that information held on Australian networks is attractive to intelligence services of foreign governments.

While much attention is focused on emerging threats to your information, existing traditional threats have not disappeared. We must remain vigilant in securing our information whether our networks are connected to the Internet or not. This policy provides a framework to address both new and existing security risks to your networks, enabling you to conduct your business effectively.

Implementation of the *Australian Government Information Security Manual* in your organisation will assist you to mitigate risk to your information and systems.

I encourage you to apply the security measures and procedures described here and to ensure you have effective information security governance arrangements in place; doing so will provide assurance that the information that is entrusted to you is properly protected.

Ian McKenzie
Director Defence Signals Directorate

Table of Contents

SUPPORTING INFORMATION 277

PASSWORD

About Information Security

Australian Government Information Security Manual

Using This Manual

Objective

The *Australian Government Information Security Manual* is used for the risk managed protection of information and systems.

Context

Scope
This section describes how to interpret the content and layout of this manual.

The purpose of this manual
The purpose of this manual is to apply a risk managed approach to the protection of information and systems in government.

Cyber security definition
The definition of cyber security in government is: 'measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means'.

Information security definition
Information security is a higher level of abstraction than cyber security and relates to the protection of information regardless of its form. The definition of information security in government is: 'measures relating to the confidentiality, availability and integrity of information'.

Target audience
The target audience for this manual is security personnel. This includes, but is not limited to:

- security executives, CISOs and CSOs
- ASAs and ITSAs
- ITSMs and ITSOs
- infosec-registered assessors.

Framework
This manual uses a framework to present information in a consistent manner. The framework consists of a number of headings in each section:

- Objective—the desired outcome of complying with the controls specified in the section, expressed as if the outcome has already been achieved.
- Context—the scope and applicability of the section. It can also include definitions, legislative context and background information.
- Controls—procedures with associated compliance requirements for reducing the level of security risks.
- Rationale—the reasoning behind the controls and associated compliance requirements.
- References—external sources of information that can assist in interpreting or implementing controls.

System applicability

Each control in this manual has an applicability indicator that indicates the information and systems to which the control applies. The applicability indicator has up to six elements, indicating whether the control applies to:

- U: UNCLASSIFIED information and systems
- IC: IN-CONFIDENCE information and systems
- R/P: RESTRICTED/PROTECTED information and systems
- C: CONFIDENTIAL information and systems
- S/HP: SECRET/HIGHLY PROTECTED information and systems
- TS: TOP SECRET information and systems.

Public systems

Agencies deploying public systems can determine their own security measures based on their risk appetite and security risks to their systems. However, DSD encourages such agencies to use this manual, particularly the objectives, as a guide when determining security measures for their systems.

Applicability of controls

While this manual provides controls for various technologies, not all systems will use all of the technologies mentioned. When agencies develop systems they will determine the appropriate scope of the systems and which controls in this manual are applicable.

Compliance language

The controls in this manual use language based on the IETF's RFC 2119 to indicate differing degrees of compliance.

Controls with a 'required' compliance requirement

A control with a 'required' compliance requirement is mandatory and cannot be risk managed by anyone other than DSD. These controls relate predominantly to the use of HGCE and associated key management procedures.

Controls with a 'must' or 'must not' compliance requirement

A control with a 'must' or 'must not' compliance requirement is mandatory. However, an accreditation authority and the agency head can choose to be non-compliant as long as appropriate procedures are followed.

Controls with a 'should' or 'should not' compliance requirement

A control with a 'should' or 'should not' compliance requirement is mandatory. However, valid reasons to vary from the control could exist in particular circumstances. The full implications need to be considered before an accreditation authority endorses non-compliance with such a control.

Controls with a 'recommended' compliance requirement

A control with a 'recommended' compliance requirement is optional. However, agencies are encouraged to consider implementing such controls taking into account their unique circumstances and risk appetite.

Non-compliance with multiple controls

When an agency is non-compliant with multiple controls, they may choose to logically group the areas of non-compliance when following the processes for non-compliance.

Controls

Non-compliance

Control: 1060; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: required
System owners seeking a dispensation for non-compliance with any control with a 'required' compliance requirement are required to seek the dispensation from the Director, DSD.

Control: 0001; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
System owners seeking a dispensation for non-compliance with any control with a 'must' or 'must not' compliance requirement must seek the dispensation from their accreditation authority and their agency head.

Control: 1061; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
System owners seeking a dispensation for non-compliance with any control with a 'should' or 'should not' compliance requirement must be granted the dispensation from their accreditation authority.

Justification for non-compliance

Control: 0710; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
System owners seeking a dispensation for non-compliance with any control must document:

- the reasons for non-compliance
- the alternative mitigation measures to be implemented
- an assessment of the residual security risks
- a date by which to review the decision.

Consultation on non-compliance

Control: 0711; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
If a system processes, stores or communicates information from another agency, that agency must be consulted before a decision to be non-compliant with any control is made.

Control: 0712; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
If a system processes, stores or communicates information from a foreign government, that government must be consulted before a decision to be non-compliant with any control is made.

Notification of non-compliance

Control: 0713; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must notify the Cyber Security Operations Centre at DSD when deciding to be non-compliant with any control.

Reviewing non-compliance

Control: 0876; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies review decisions to be non-compliant with any control, as well as any mitigation measures, at least annually.

Recording non-compliance

Control: 0003; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must retain a copy of decisions to be non-compliant with any control from this manual.

Rationale

Non-compliance

Controls in this manual with a 'required' compliance requirement cannot be risk managed by agencies. Only DSD can grant dispensations for these controls. In such circumstances the Director DSD will consider granting a dispensation on request from a system owner through their agency head.

Controls in this manual with a 'must' and 'must not' compliance requirement can be risk managed by agencies. In such cases the agency head in association with the accreditation authority can consider the justification for a dispensation for non-compliance and grant approval if appropriate.

Controls in this manual with a 'should' and 'should not' compliance requirement can be risk managed by agencies. As the risk for non-compliance is not as high as those with a 'must' and 'must not' compliance requirement, the accreditation authority can consider the justification for a dispensation for non-compliance and grant approval, if appropriate, without the input of the agency head.

Justification for non-compliance

Without sufficient justification and consideration of the security risk by the system owner when seeking a dispensation, the agency head or their authorised delegate will lack the appropriate information to make an informed decision on whether to accept the security risk and grant the dispensation.

Consultation on non-compliance

When an agency recieves or stores information on its system(s) that is owned by another agency or foreign government it has an obligation to inform the owner when the controls specified in this manual are not fully implemented. If the agency fails to do so the owner will be unaware that its information has been placed at a heightened risk of compromise. The owner is thus denied the opportunity to consider additional security measures for its information.

Notification of non-compliance

The purpose of notifying authorities of any decisions to be non-compliant with controls is two-fold: firstly to ensure that an accurate picture of information security across government can be maintained, and secondly as feedback to ensure the continuing refinement of this manual.

Reviewing non-compliance

An assessment of the residual security risk is conducted when providing justification for a dispensation for non-compliance. This assessment is based on the risk environment at the time the dispensation is sought. As the risk environment will evolve over time, it is important that agencies revisit the assessment annually and update it according to the current risk environment, and if necessary, reverse any decisions to grant a dispensation if the security risk is no longer acceptable.

Recording non-compliance

Without appropriate records of decisions to risk manage controls, an agency has no record of the status of its security posture. Furthermore, a lack of such records will hinder any auditing activities that may be conducted by the agency or by external parties such as ANAO.

References

This manual is updated regularly. It is therefore important that agencies ensure that they are using the latest baseline comprising the latest release, errata and interim policy releases. This manual, additional information, tools and discussion topics can be accessed from the OnSecure website at members.onsecure.gov.au.

Supplementary information to this manual can be found in the following documents.

TOPIC	DOCUMENTATION	AUTHOR
Archival of information	*The Archives Act 1983* (the Archives Act)	NAA
Business continuity	HB 221:2004, *Business Continuity Management*	Standards Australia
	HB 292-2006, *A practitioners guide to business continuity management*	Standards Australia
	HB 293-2006, *Executive guide to business continuity management*	Standards Australia
Cabinet information	*Cabinet Handbook, Security and handling of cabinet documents*	PMC
Cable security	*ACSI 61, Guidelines for the Installation of Communications and Information Processing Equipment and Systems*	DSD
Communications security roles and responsibilities	*ACSI 53, Communications Security Handbook*	DSD
Communications security incident reporting	*ACSI 107, Reporting and Evaluating COMSEC Incidents*	DSD
Emanation security	*ACSI 71, A guide to the Assessment of Electromagnetic Security in Military and High-risk Environments*	DSD
Information security	PSPF, *Information Security Protocol*	AGD
Information security management	ISO/IEC 27000:2009, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*	ISO/IEC
	AS/NZS ISO/IEC 27001:2006, *Information technology – Security techniques – Information security management systems – Requirements*	Standards Australia
	AS/NZS ISO/IEC 27002:2006, *Information technology – Security techniques – Code of practice for information security management*	Standards Australia
	ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management systems implementation guidance*	ISO/IEC
	ISO/IEC 27004:2009, *Information technology – Security techniques – Information security management – Measurement*	ISO/IEC
Key management – commercial grade	AS 11770.1-2003, *Information technology – Security techniques – Key management – Framework*	Standards Australia
Key management – high grade	*ACSI 105, Cryptographic Controlling Authorities and Keying Material Management*	DSD
Management of electronic records that may be used as evidence	HB 171-2003, *Guidelines for the management of IT evidence*	Standards Australia
Personnel security	PSPF, *Personnel Security Protocol*	AGD

Continued on next page

TOPIC	DOCUMENTATION	AUTHOR
Physical security	PSPF, *Physical Security Protocol*	AGD
Privacy requirements	*The Privacy Act 1988* (the Privacy Act)	AGD
Risk management	AS/NZS ISO 31000:2009, *Risk Management – Principles and guidelines*	Standards Australia
	HB 327:2010, *Communicating and consulting about risk (Companion to AS/NZS ISO 31000:2009)*	Standards Australia
	ISO/IEC Guide 73, *Risk Management – Vocabulary – Guidelines for use in Standards*	ISO/IEC
	ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management*	ISO/IEC
	HB 167:2006, *Security risk management*	Standards Australia
	HB 231:2004, *Information security risk management guidelines*	Standards Australia
	NIST SP 800-30, *Risk Management Guide for Information Technology Systems*	NIST

Applicability, Authority and Compliance

Objective

The requirements of the *Australian Government Information Security Manual* are complied with.

Context

Scope

The ISM is the primary policy produced by DSD relating to information security. Its role is to promote a consistent approach to information security across all Australian government, state and territory agencies and bodies for the protection of information and systems.

Applicability

This manual applies to:

- Australian Government agencies that are subject to the *Financial Management and Accountability Act 1997* (the FMA Act)
- bodies that are subject to the *Commonwealth Authorities and Companies Act 1997* (the CAC Act) and that have received notice in accordance with that Act that the ISM applies to them as a general policy of the government
- other bodies established for a public purpose under the law of the Commonwealth and other Australian Government agencies, where the body or agency has received a notice from its Portfolio Minister that the ISM applies
- state and territory agencies that hold or access classified information
- organisations that have entered a Deed of Agreement with the government to have access to classified information.

Authority

The Intelligence Services Act 2001 (the ISA) states that two functions of DSD are:

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

The ISM represents the considered advice of DSD provided in accordance with its designated functions under the ISA. Therefore agencies are not required as a matter of law to comply with the ISM, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply with it.

Compliance by smaller agencies

As smaller agencies may not always have sufficient personnel or budgets to comply with this manual, they may choose to consolidate resources with another larger host agency to undertake a joint approach to compliance.

In such circumstances smaller agencies may choose to either operate on systems fully hosted by another agency using its information security policies and security resources, or share security resources to jointly develop information security policies and systems for use by both agencies. In these cases, the requirements in this manual can be interpreted as either relating to the host agency or to both agencies, depending on the approach taken.

In situations where agencies choose a joint approach to compliance, especially when an agency agrees to fully host another agency, the agency heads may choose to seek a memorandum of understanding regarding their security responsibilities.

Legislation and legal considerations

This manual does not override any obligations imposed by legislation or law. Furthermore, if this manual conflicts with legislation or law the later takes precedence.

While this manual contains examples of when legislation or 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.

Auditing of compliance by the Australian National Audit Office

All controls in this manual, except those with a 'recommended' compliance requirement, are capable of being audited for compliance by ANAO.

Controls

Compliance

Control: 0007; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies undertaking system design activities for in-house or out-sourced projects must use the latest baseline of this manual for security requirements.

Control: 0008; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must comply with any specified compliance timeframes for information security policies that DSD determines is of particular importance.

Rationale

Compliance

By using the latest baseline of this manual for system design activities, agencies will be taking steps to protect themselves from the current threat environment for government systems.

DSD produces information security policies in addition to the ISM, such as the ACSI suite. These policies may be updated to address specific security risks to government information and systems. In such cases specific timeframes for compliance may be specified.

References

Nil.

Information Security in Government

Government Engagement

Objective

Security personnel are aware of and use security services offered in the Australian Government.

Context

Scope

This section describes the organisations involved in providing information security advice.

Defence Signals Directorate

DSD is required under the ISA to perform various functions, including the provision of material, advice and other assistance to Commonwealth and State authorities on matters relating to the security of information that is processed, stored or communicated by electronic or similar means.

DSD provides assistance to Commonwealth and State authorities in relation to cryptography, communications and computer technologies.

DSD works with industry to develop new cryptographic products. It has established the AISEP in order to deal with the increasing requirement to evaluate security products.

DSD can be contacted for advice and assistance in implementing the ISM through an ITSM or its ITSA. ITSMs and ITSAs can send questions to DSD by email at assist@dsd.gov.au or phone on 1300 CYBER1 (1300 292 371).

DSD can be contacted for advice and assistance on cyber security incidents. DSD's response will be commensurate with the urgency of the cyber security incident. There is a 24-hour, seven day a week service available if necessary. The Cyber Security Operations Centre can be contacted by email at assist@dsd.gov.au or phone on 1300 CYBER1 (1300 292 371).

DSD can be contacted for advice and assistance on the purchasing, provision, deployment, operation and disposal of HGCE. The Crypto Liaison section can be contacted by email at ISG.CryptoLiaison@defence.gov.au.

Other organisations

The table below contains a brief description of the other organisations that have a role in information security in government.

ORGANISATION	SERVICES
Attorney-General's Department – Protective Security Training Centre	Protective security training
Australasian Information Security Evaluation Program	The evaluation of security products
Australian Federal Police – Australian High Tech Crime Centre	Law enforcement in relation to electronic crime and other high tech crimes
Australian Government Information Management Office	Development, coordination and oversight of policy on electronic commerce, online services and the Internet
Australian National Audit Office	Performance audits on information security

Continued on next page

ORGANISATION	SERVICES
Australian Security Intelligence Organisation – T4 Protective Security	Protective security advice and training, technical surveillance counter-measures, physical security certifications, protective security risk reviews and physical security equipment testing
Cyber Security Policy and Coordination Committee	Coordinates cyber security initiatives for government
Defence Intelligence Organisation	Certification of SCIFs
Department of Foreign Affairs and Trade	Policy and advice for security overseas
Department of the Prime Minister and Cabinet	Protective security advice
Protective Security Policy Committee	Coordinates the development of protective security policy
Security Construction and Equipment Committee	The evaluation of security equipment

Controls

Organisations providing information security services

Control: 0879; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended that security personnel familiarise themselves with the information security roles and services provided by Australian Government organisations.

Rationale

Organisations providing information security services

If security personnel are unaware of the roles government organisations play in the information security space, they could miss out on valuable insight and assistance in developing effective security measures.

References

The following websites can be used to obtain additional information about organisations involved in the security of government systems:

- www.dsd.gov.au
- www.ag.gov.au/www/agd/agd.nsf/Page/Security_training
- www.dsd.gov.au/infosec/aisep.htm
- www.ahtcc.gov.au
- www.agimo.gov.au
- www.anao.gov.au
- www.asio.gov.au/Work/Content/ProtectiveSecurity.aspx
- www.defence.gov.au/dio
- www.dfat.gov.au
- www.pmc.gov.au
- www.scec.gov.au.

Industry Engagement and Outsourcing

Objective

Industry partners handle information appropriately and implement the same security measures as their sponsoring agency.

Context

Scope

This section describes information on outsourcing information technology services and functions to industry as well as providing them with access to information in order to undertake their duties.

Cloud computing

Cloud computing is a form of outsourcing information technology services and functions over the Internet. The requirements in this section equally apply to providers of cloud computing services.

Controls

Accrediting service providers' systems

Control: 0872; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Systems used by service providers for the provision of information technology services and functions must be accredited to the same minimum standard as the sponsoring agency's systems.

Service providers' systems

Control: 0873; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Service providers' systems should be located in Australia.

Control: 1073; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not

Service providers should not allow information to leave Australian borders unless approved by the sponsoring agency.

Service providers' ITSM

Control: 0744; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Service providers should provide a single point of contact who will act as an equivalent to an ITSM.

Developing an industry security program

Control: 1052; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies develop an industry security program to manage service providers that have been approved for the provision of information technology services and functions.

Rationale

Accrediting service providers' systems

Service providers can be provided with information as long as their systems are accredited to process, store and communicate the information. This ensures that when service providers are provided with information it receives an appropriate level of protection.

Service providers' systems

While this manual recommends against the outsourcing of information technology services and functions outside of Australia it does not preclude the use of services of foreign owned service providers in Australia. When such service providers are engaged agencies are strongly encouraged to ensure that all information provided to the service provider is hosted in Australia and does not leave Australian borders.

Service providers' ITSM

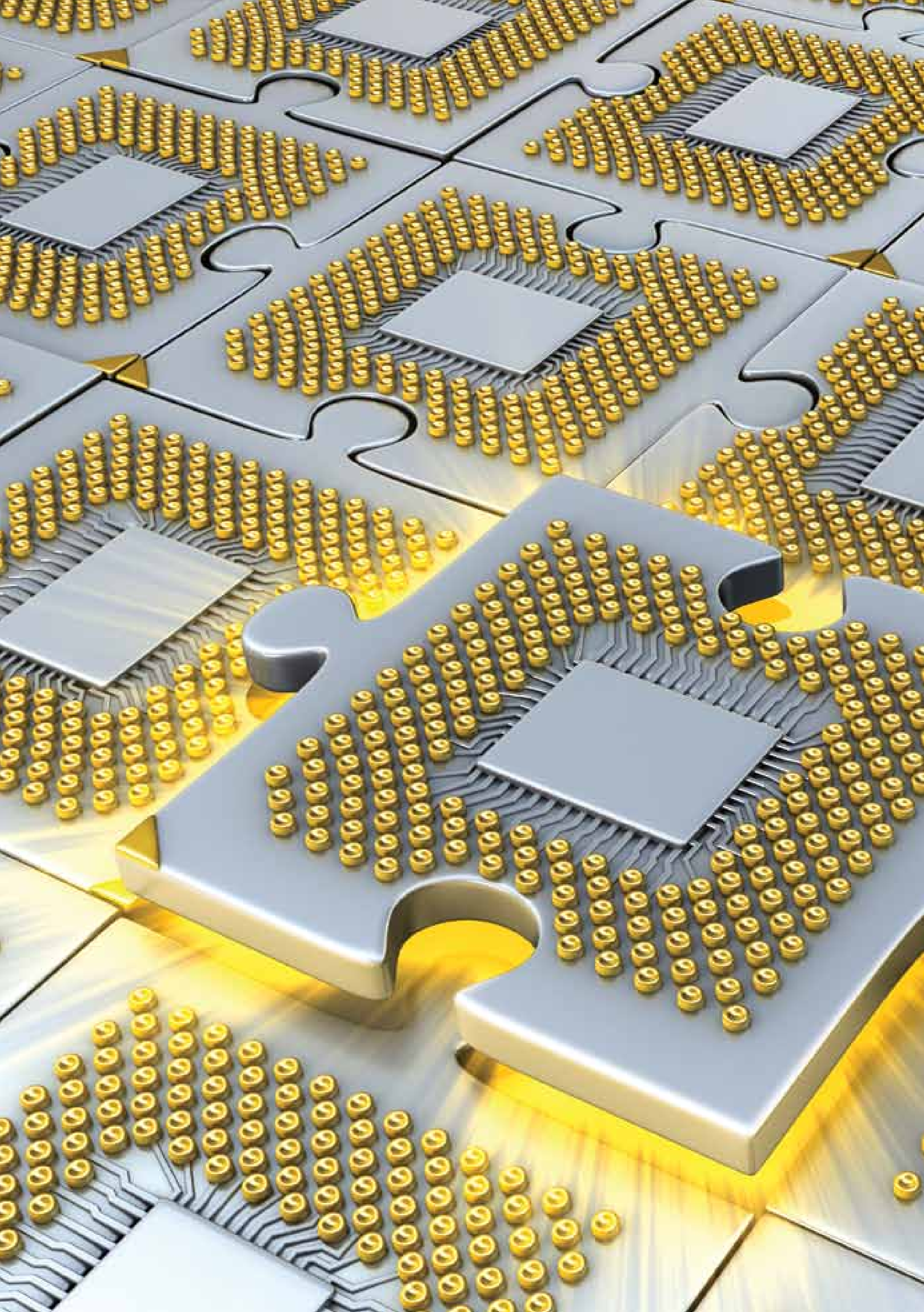
When an agency engages a service provider for the provision of information technology services and functions, having a central point of contact for information security issues will greatly assist incident response and reporting procedures.

Developing an industry security program

The development of an industry security program will assist the agency in undertaking a coordinated approach to the engagement and use of service providers for outsourcing and provision of information technology services and functions.

References

Nil.



Information Security Governance

Roles and Responsibilities

The Agency Head

Objective

The agency head endorses and is accountable for information security.

Context

Scope

This section describes the role of an agency head concerning information security.

Chief Executive Officer

In some agencies, especially those established under the CAC Act, the person responsible for the agency or body may be referred to as the CEO. In such cases the policy for the agency head is equally applicable to the CEO.

Delegating authority

When the agency head's authority in this area has been delegated to a board, committee or panel, the requirements of this section relate to the chair or head of that governing board, committee or panel.

Controls

Support for information security

Control: 0011; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

The agency head must provide support for the development, implementation and maintenance of information security processes.

Delegation of authority

Control: 0012; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Where the agency head delegates their authority, the delegate must be at least a member of the Senior Executive Service or in an equivalent management position.

Control: 0880; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended that, when the agency head delegates their authority, the delegate be the CISO.

Rationale

Support for information security

Without the full support of the agency head, security personnel are less likely to have access to sufficient resources and authority to successfully implement information security.

If a cyber security incident results in the disclosure of information or a system failure due to preventable circumstances, the agency head will ultimately be held responsible.

Delegation of authority

When an agency head chooses to delegate their authority to approve non-compliance with requirements in this manual, they should consider all the risks as they remain responsible for the decisions made by their delegate.

The CISO is the most appropriate choice for delegated authority as they are a senior executive and are responsible for information security and security risk management.

References

Nil.

The Chief Information Security Officer

Objective

The chief information security officer sets the strategic direction for information security.

Context

Scope

This section describes the role of a CISO concerning information security.

The Security Executive and their CISO role

The requirement to appoint a member of the Senior Executive Service, or an equivalent management position, to the role of CISO does not require a new dedicated position be created in each agency. This role is intended to be performed by the security executive which is a position in each agency mandated by the PSPF. The introduction of the CISO role is aimed at providing a more meaningful title for a subset of the security executive's responsibilities that relate to information security.

Controls

Requirement for a CISO

Control: 0714; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must appoint a person to the role of CISO or have the role undertaken by an existing person.

Control: 0715; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

The CISO role must be undertaken by a member of the Senior Executive Service or an equivalent management position.

Control: 0716; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

The CISO must be:

- cleared for access to all information
- able to be briefed into any compartmented information.

Control: 0717; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The CISO should be responsible for overseeing the management of information security personnel.

Responsibilities – Reporting

Control: 0718; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The CISO should report to the agency head on information security issues.

Responsibilities – Security programs

Control: 0719; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The CISO should develop and maintain a comprehensive strategic-level security risk management program aimed at protecting information and systems.

Control: 0720; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The CISO should be responsible for the development of an information security communications plan.

Control: 0721; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The CISO should create and facilitate the security risk management process.

Responsibilities – Ensuring compliance

Control: 0722; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should ensure compliance with information security policies and standards.

Control: 0723; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should ensure compliance with the ISM through facilitating a continuous program of accreditation based on security risk management.

Control: 0724; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should implement information security measurement metrics and key performance indicators.

Responsibilities – Coordinating security

Control: 0725; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should facilitate information security and business alignment, and communication through an information security steering committee or advisory board which meets formally and on a regular basis.

Control: 0726; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should coordinate security risk management projects between business and information security teams.

Control: 0727; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should work with business teams to facilitate risk analysis and security risk management processes, including identifying acceptable levels of security risk consistently across the agency.

Responsibilities – Working with ICT projects

Control: 0728; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should provide strategic-level information security guidance for ICT projects and operations.

Control: 0729; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should liaise with architecture teams to ensure alignment between security and agency architectures.

Control: 0730; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should be the accreditation authority when a system undergoes accreditation; unless an external accreditation authority is mandated.

Responsibilities – Working with vendors

Control: 0731; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should coordinate the use of external information security resources including contracting and managing the resources.

Responsibilities – Budgeting

Control: 0732; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should control the information security budget.

Responsibilities – Cyber security incidents

Control: 0733; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should be fully aware of all cyber security incidents.

Responsibilities – Disaster recovery

Control: 0734; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should coordinate the development of disaster recovery policies and standards to ensure that business-critical services are supported appropriately in the event of a disaster.

Responsibilities – Training

Control: 0735; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The CISO should oversee the development and operation of information security awareness and training programs.

Responsibilities – Providing security knowledge

Control: 0881; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that the CISO provide authoritative security advice and have familiarity with a range of national and international standards and best practice.

Contacting CISOs

Control: 0736; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should maintain an email address for their CISO in the form of CISO@agency.gov.au or CISO@agency.state.gov.au.

Control: 1064; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should notify DSD when the CISO, or their contact details, change.

Rationale

Requirement for a CISO

The role of the CISO is based on industry best practice and has been introduced to ensure that information security is managed at the senior executive level.

The CISO facilitates communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives.

The CISO provides strategic-level guidance for the agency security program and ensuring compliance with national policy, standards, regulations and legislation.

Responsibilities – Reporting

As the CISO is responsible for the overall management of information security it is important that they report to the agency head on any information security issues.

Responsibilities – Security programs

Without a comprehensive strategic-level security risk management program an agency will lack high-level direction on information security issues.

Responsibilities – Ensuring compliance

Without a person responsible for ensuring compliance with the information security policies and standards, security measures of the agency are unlikely to meet minimum government requirements.

Responsibilities – Coordinating security

The CISO is to ensure appropriate communication between business and information security teams. This includes translating information security concepts and language into business concepts and language as well as ensuring that business teams consult with information security teams to determine appropriate security measures when planning new business projects for the agency.

Responsibilities – Working with ICT projects

As the CISO is responsible for the development of the strategic-level information security program they are best placed to advise ICT projects on the strategic direction of information security.

As the CISO is responsible for the overall management of information security they are the appropriate authority to accept security risks associated with the operation of agency systems.

Responsibilities – Working with vendors

The CISO coordinates the use of external security resources to ensure that a consistent approach is being applied across the agency.

Responsibilities – Budgeting

Controlling the security budget will ensure the CISO has sufficient access to funding to support information security projects and initiatives.

Responsibilities – Cyber security incidents

To ensure the CISO is able to accurately report to the agency head on information security issues it is important they remain fully aware of all cyber security incidents.

Responsibilities – Disaster recovery

Restoring business-critical services to an operational state after a disaster is an important function of business continuity. As such it will need high level support from the CISO.

Responsibilities – Training

To ensure personnel are actively contributing to the security posture of the agency, an information security awareness and training program will need to be developed. As the CISO is responsible for information security they will need to oversee the development and operation of the program.

Responsibilities – Providing security knowledge

The CISO is not expected to be a technical expert on information security issues; however, knowledge of national and international standards and best practice will help them communicate with technical experts on information security issues.

Contacting CISOs

As security agencies in government often need to communicate with security personnel of other agencies it is important that a consistent contact method is used across government. If agencies maintain a standardised email address then security agencies can pass them useful security related information.

To ensure CISOs can be contacted directly to provide warnings of threats to their systems, DSD requests agencies provide updated contact details when either the CISO or their contact details change. This information can be provided to DSD through the advice and assistance service.

References

Nil.

The Agency Security Advisor

Objective

The agency security advisor is responsible for the day-to-day performance of protective security functions.

Context

Scope

This section describes the role of an ASA concerning the protection of systems. The ASA has additional responsibilities beyond assisting in the protection of systems however these are not considered to be in the scope of this manual. Further information on responsibilities of the ASA can be found in the PSPF.

The ASA

The PSPF mandates that agencies appoint an ASA who is responsible for the day-to-day performance of protective security functions. In this regard, the ASA assists security personnel with the implementation of physical and personnel security measures for the protection of systems.

Controls

Responsibilities – Reporting

Control: 0737; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The ASA should advise the CISO on physical and personnel security issues relating to the protection of systems.

Responsibilities – Providing security knowledge

Control: 0738; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The ASA should pro-actively work with security personnel to ensure that physical and personnel security requirements are appropriately implemented for systems.

Rationale

Responsibilities – Reporting

If an ASA fails to advise the CISO of physical and personnel security issues relating to the protection of systems the CISO will not have a full picture of information security and any briefings the CISO provides to the agency head will be lacking in scope.

Responsibilities – Providing security knowledge

The ASA is the expert on physical and personnel security issues and is best placed to assist system owners with the implementation of physical and personnel security measures for their systems.

References

Nil.

The Information Technology Security Advisor

Objective

The information technology security advisor coordinates information technology security.

Context

Scope

This section describes the role of an ITSM concerning information security when designated as the ITSA. Information on the responsibilities of ITSMs can be found in the *Information Technology Security Managers* section of this chapter.

The ITSA

The ITSM who has responsibility for information technology security management across the agency is designated as the ITSA. This title reflects the responsibility this ITSM has as the first point of contact for the CISO and external agencies on any information technology security management issues.

Controls

Requirement for an ITSA

Control: 0013; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must designate an ITSM as the ITSA.

Responsibilities – Coordination of other ITSMs

Control: 0740; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Where multiple ITSMs are appointed, the ITSA should be responsible for the coordination and oversight of the other ITSMs.

Responsibilities – Reporting

Control: 0739; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The ITSA should advise the CISO on information technology issues relating to the protection of systems.

Contacting ITSAs

Control: 0025; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should maintain an email address for their ITSA in the form of ITSA@agency.gov.au or ITSA@agency.state.gov.au.

Control: 1090; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should notify DSD when the ITSA, or their contact details, change.

Rationale

Requirement for an ITSA

An ITSM, when fulfilling the designation of ITSA, still maintains full responsibilities for their role as an ITSM in addition to ITSA responsibilities.

Responsibilities – Coordination of other ITSMs

Designating an ITSM who has an additional responsibility of coordinating other ITSMs ensures that security measures and efforts are undertaken in a coordinated manner.

Responsibilities – Reporting

If an ITSA fails to advise the CISO on information technology issues relating to the protection of systems the CISO will not have a full picture of information security and any briefings the CISO provides to the agency head will be lacking in scope.

Contacting ITSAs

As security agencies in government often need to communicate with security personnel of other agencies it is important that a consistent contact method is used across government. If agencies maintain a standardised email address then security agencies can pass them useful security related information.

To ensure that ITSAs can be contacted directly to provide warnings of threats to their systems, DSD requests that agencies provide DSD with updated contact details when either the ITSA or their contact details change. This information can be provided to DSD through the advice and assistance service.

References

Nil.

Information Technology Security Managers

Objective

Information technology security managers provide information security leadership and management.

Context

Scope

This section describes the role of ITSMs concerning information security.

Information technology security managers

ITSMs are executives that coordinate the strategic directions provided by the CISO and the technical efforts of ITSOs. The main area of responsibility of an ITSM is that of the administrative controls relating to information security.

Controls

Requirement for ITSMs

Control: 0741; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must appoint at least one ITSM.

Control: 0882; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
Where spread across a number of geographical sites, it is recommended agencies appoint a local ITSM at each site.

Control: 0742; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
ITSMs should not have additional responsibilities beyond those outlined in this manual.

Control: 0743; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The ITSM role should be undertaken by personnel with an appropriate level of authority based on the size of the agency or their area of responsibility.

Control: 0024; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
ITSMs must be:

- cleared for access to all information processed by the systems under their authority
- able to be briefed into any compartmented information on the systems under their authority.

Independence of ITSMs from service providers

Control: 0016; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should be independent of service providers of information technology services and functions.

Responsibilities – Security programs

Control: 0745; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should work with the CISO to develop an information security program.

Control: 0746; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should undertake and manage projects to address identified security risks.

Responsibilities – Working with ICT projects

Control: 0747; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should identify systems that require security measures and assist in the selection of appropriate security measures for such systems.

Control: 0749; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should consult with ICT project personnel to ensure that information security is factored into the evaluation, selection, installation and configuration of ICT equipment and software.

Control: 0750; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should work with enterprise architecture teams to ensure that security risk assessments are built into system architectures and to identify, evaluate and select security solutions to meet security objectives.

Control: 0748; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should work with system owners to determine appropriate information security policies for their systems.

Control: 0023; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
ITSMs must be responsible for assisting system owners to obtain and maintain the accreditation of their systems.

Responsibilities – Working with vendors

Control: 0751; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should liaise with vendors and their purchasing and legal areas to establish mutually acceptable contracts and service-level agreements.

Responsibilities – Implementing security

Control: 0019; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
ITSMs must be responsible for ensuring the development, maintenance, updating and implementation of SRMPs, SSPs and any SOPs where higher level, multi-system or agency-wide systems are used.

Control: 0752; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should conduct security risk assessments on the implementation of new or updated ICT equipment or software on the existing environment and develop risk treatment strategies if necessary.

Control: 0753; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should recommend and coordinate the implementation of controls to support and enforce information security policies.

Control: 0754; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should provide leadership and direction for the integration of information security strategies and architecture with business and ICT strategies and architecture.

Control: 0755; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should provide technical and managerial expertise for the administration of information security management tools.

Responsibilities – Budgeting

Control: 0756; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should work with the CISO to develop information security budget projections and resource allocations based on short-term and long-term goals and objectives.

Responsibilities – Reporting

Control: 0757; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should coordinate, measure and report on technical aspects of information security management.

Control: 0758; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should monitor and report on compliance with information security policies, as well as the enforcement of information security policies.

Control: 0759; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should provide regular reports on cyber security incidents and other areas of particular concern to the CISO.

Control: 0760; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should assess and report on threats, vulnerabilities, and residual security risks and recommend remedial actions.

Responsibilities – Auditing

Control: 0761; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should assist system owners and security personnel in understanding and responding to audit failures reported by auditors.

Responsibilities – Disaster recovery

Control: 0762; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans.

Responsibilities – Training

Control: 0763; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should provide information security awareness and training for all personnel.

Control: 0764; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should develop technical information materials and workshops on information security trends, threats, best practices and control mechanisms as appropriate.

Responsibilities – Providing security knowledge

Control: 0765; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should maintain a current security knowledge base comprising of a technical reference library, security advisories and alerts, information on information security trends and practices, and laws and regulations.

Control: 0766; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should provide expert guidance on information security issues for ICT projects.

Control: 0767; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSMs should provide technical advice for the information security steering committee, change management committee and other agency and inter-agency committees as required.

Rationale

Requirement for ITSMs

Appointing local ITSMs, when an agency is spread across a number of geographic sites, will ensure the ITSA has a presence at sites to assist with monitoring information security for systems and responding to any cyber security incidents.

Independence of ITSMs from service providers

When an agency engages a service provider for the provision of information technology services and functions, from which an ITSM is also employed, the agency needs to ensure that there is no actual or perceived conflict of interest.

Responsibilities – Security programs

As ITSMs are operational managers of information security they can provide valuable input to the development of the information security program by the CISO.

Responsibilities – Working with ICT projects

As ITSMs have knowledge of all aspects of information security they are best placed to work with ICT projects to identify and incorporate appropriate security measures.

Responsibilities – Working with vendors

While the CISO will coordinate the use of external security resources to the agency, ITSMs will be responsible for establishing contracts and service-level agreements on behalf of the CISO.

Responsibilities – Implementing security

While the CISO will set the strategic direction for information security, ITSMs are responsible for managing the implementation of security measures.

Responsibilities – Budgeting

As ITSMs are operational managers of information security projects and functions they will be aware of their funding requirements and can help the CISO develop security budget projections and resource allocations.

Responsibilities – Reporting

To ensure the CISO remains aware of all information security issues, and can brief their agency head when necessary, ITSMs will need to provide regular reports on cyber security incidents and other areas of particular concern to the CISO.

Responsibilities – Auditing

As system owners may not understand the results of audits against their systems, ITSMs will need to help them understand and respond to reported audit failures.

Responsibilities – Disaster recovery

While the CISO will coordinate the development of disaster recovery policies and standards, ITSMs will need to guide the selection of appropriate strategies to achieve the direction set by the CISO.

Responsibilities – Training

While the CISO will oversee the development and operation of information security awareness and training programs, ITSMs will deliver the training to personnel.

Responsibilities – Providing security knowledge

ITSMs will often have a strong knowledge of information security issues and can provide advice for the information security steering committee, change management committee and other agency and inter-agency committees.

Responsibilities

ITSMs are generally considered the information security experts. Their core responsibilities are: to improve the security of systems, provide input to ICT projects, assist other security personnel, contribute to information security training and respond to cyber security incidents.

An ITSM is likely to have the most current and accurate understanding of the threat environment relating to systems. As such, it is essential that this information is passed to system owners to ensure that it is considered during accreditation activities.

References

Nil.

Information Technology Security Officers

Objective

Information technology security officers provide information security operational support.

Context

Scope

This section describes the role of ITSOs concerning information security.

Appointing an ITSO

The ITSO role may be combined with that of the ITSM. Small agencies may choose to assign both ITSM and ITSO responsibilities to one person under the title of the ITSA. Furthermore, agencies may choose to have this role performed by existing system administrators with an additional reporting chain to an ITSM for the security aspects of their role. Finally, agencies may choose to have the responsibilities of an ITSO undertaken externally as part of outsourcing of their ICT services.

Controls

Requirement for ITSOs

Control: 0768; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must appoint at least one ITSO.

Control: 0883; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that ITSOs do not have additional responsibilities beyond those outlined in this manual.

Control: 0769; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The ITSO role should be undertaken by personnel with an appropriate level of authority based on the size of the agency or their area of responsibility.

Control: 0770; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
ITSOs must be:

- cleared for access to all information processed by the systems for which they are responsible
- able to be briefed into any compartmented information on the systems for which they are responsible.

Responsibilities – System security administration

Control: 0771; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should validate and authorise user and access administration on systems in accordance with defined policies, standards and procedures.

Control: 0772; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should perform system security administration on designated systems, including operating systems and network devices, in accordance with defined policies, standards and procedures, as well as with industry best practice and vendor guidelines.

Control: 0773; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should perform installation and configuration management of systems, including policy assessment and compliance tools, network security applications, and host-based security systems.

Control: 0774; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should ensure patches are applied and remove known system weaknesses as a means of hardening systems in accordance with information security policies and standards.

Control: 0775; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should validate and authorise change requests; escalating such requests when appropriate as part of the change management process.

Responsibilities – Security assessments

Control: 0776; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should perform vulnerability assessments to ensure that systems are protected against known and potential threats and are free from known vulnerabilities.

Control: 0777; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should research threats and vulnerabilities and, where appropriate, take actions to mitigate threats and remediate vulnerabilities.

Control: 0778; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should assist operational personnel to locate and repair information security issues and failures on systems.

Responsibilities – Cyber security incidents

Control: 0779; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should respond to and, where appropriate, resolve or escalate reported cyber security incidents in accordance with the incident response plan.

Control: 0780; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should report unresolved network security exposures, misuse of resources or non-compliance situations to an ITSM.

Control: 0781; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should respond to and follow up on security events in system and event logs.

Control: 0782; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should collate cyber security incident and event data to produce monthly exception and management reports.

Responsibilities – Auditing

Control: 0108; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should manage and audit system event logs.

Control: 0783; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should implement or coordinate remediation activities required by audits.

Responsibilities – Disaster recovery

Control: 0784; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should develop and maintain disaster recovery plans, processes and procedures in accordance with defined policies, standards and business requirements for systems.

Responsibilities – Training

Control: 0785; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
ITSOs should communicate with system owners and personnel to increase their awareness of applicable information security policies and standards.

Rationale

Requirement for ITSOs

Appointing a person whose sole responsibility is to ensure that the technical security of systems is essential to comply with the controls in this manual.

Responsibilities – System security administration

The core responsibility of ITSOs is the implementation and monitoring of technical security measures for systems.

Responsibilities – Security assessments

As ITSOs are technical experts they are best placed to conduct vulnerability assessments and to take actions to mitigate threats and remediate vulnerabilities.

Responsibilities – Cyber security incidents

As ITSOs are responsible for system security administration they will often be the first to notice cyber security incidents on their systems. In such cases ITSOs will need to work with ITSMs to respond to the cyber security incidents in an appropriate manner.

Responsibilities – Auditing

ITSOs can assist ITSMs with technical remediation activities required as a result of audits.

Responsibilities – Disaster recovery

While the CISO will coordinate the development of disaster recovery policies and standards, ITSMs will guide the selection of appropriate strategies to achieve the direction set by the CISO, and ITSOs as technical experts will assist in the selection of security measures to achieve the strategies selected by ITSMs.

Responsibilities – Training

As ITSOs are technical experts on information security issues they are well placed to raise awareness of information security issues with system owners and personnel.

Responsibilities

ITSOs are generally considered specialists in controls for security systems, operating systems and network devices and core aspects of their work are: improving the security of systems, providing input to agency ICT projects, assisting other security personnel, contributing to information security training and responding to cyber security incidents.

References

Nil.

System Owners

Objective

System owners obtain and maintain accreditation of their systems.

Context

Scope

This section describes the role of system owners concerning information security.

Controls

Requirement for system owners

Control: 1071; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Each system must have a system owner who is responsible for the operation of the system.

Control: 1072; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
System owners should be a member of the Senior Executive Service or in an equivalent management position.

Accreditation responsibilities

Control: 0027; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
System owners must obtain and maintain accreditation for their systems.

Documentation responsibilities

Control: 0028; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
System owners must be responsible for the development, maintenance and implementation of complete, accurate and current SRMPs, SSPs and SOPs for their systems.

Rationale

Requirement for system owners

While the system owner is responsible for the operation of the system they will delegate the day-to-day management and operation of the system to a system manager or managers.

While it is strongly recommended that a system owner is a member of the Senior Executive Service, or in an equivalent management position, it does not imply that the system managers should also be at such a level.

Accreditation responsibilities

The system owner is responsible for the secure operation of their system and needs to ensure it is accredited. If modifications are undertaken to a system the system owner will need to ensure the changes are undertaken in an appropriate manner, documented adequately and that any necessary reaccreditation activities are completed.

Documentation responsibilities

While the system owner is responsible for the development, maintenance and implementation of SRMPs, SSPs and SOPs, their exposure to information security issues can be too narrowly focused and restricted to the systems with which they are familiar. Involving security personnel in the process ensures that a holistic approach to information security can be mapped to the system owner’s understanding of security risks for their specific system.

References

Nil.

System Users

Objective

System users comply with information security policies and procedures.

Context

Scope

This section describes the role of system users concerning information security.

Types of system users

This section describes responsibilities for all system users: users with general access (general users), and users with privileged access (privileged users).

Controls

Responsibilities of system users

Control: 0033; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
All system users must comply with the relevant information security policies and procedures for the systems they use.

Control: 0034; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
All system users must:

- protect account authenticators at the same classification as the system it secures
- not share authenticators for accounts without approval
- be responsible for all actions under their accounts
- use their access to only perform authorised tasks and functions.

Control: 0406; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
System users that need to bypass information security policies, procedures or mechanisms for any reason must seek formal authorisation from an ITSM.

Rationale

Responsibilities of system users

If agencies fail to develop and maintain a security culture where system users are complying with information security policies and procedures for the systems they are using, there is an increased risk of a system user unwittingly assisting with an attack against a system.

While information security policies, procedures and mechanisms aim to cover all situations, there may be legitimate reasons for a system user to bypass information security policies, procedures or mechanisms. In such cases the system user must seek formal authorisations from an ITSM before any actions are undertaken.

References

Nil.

Information Security Documentation

Documentation Fundamentals

Objective

Information security documentation is produced for systems.

Context

Scope

This section describes the information security documentation that each agency needs to develop. More detailed information about each document can be found in the relevant sections of this chapter.

Controls

Information security policy

Control: 0039; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must have an information security policy.

Security risk management plan

Control: 0040; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that every system is covered by a SRMP.

System security plan

Control: 0041; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that every system is covered by a SSP.

Standard operating procedures

Control: 0042; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that SOPs are developed for systems.

Incident response plan

Control: 0043; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must develop an IRP and supporting procedures.

Developing content

Control: 0886; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure that information security documentation is developed by personnel with a good understanding of both the subject matter and the business requirements.

Documentation content

Control: 0044; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that their SRMP, SSP, SOPs and IRP are logically connected and consistent for each system and with the information security policy.

Using a documentation framework

Control: 0786; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Where an existing, well-defined documentation framework is lacking, the document names defined in this manual should be used.

Control: 0787; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should create and maintain a document framework including a hierarchical listing of all information security documentation and their relationships.

Control: 0885; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies adopt the naming conventions provided in this manual for their information security documentation.

Outsourcing development of content

Control: 0046; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
When information security documentation development is outsourced, agencies should:

- review the documents for suitability
- retain control over the content
- ensure that all policy requirements are met.

Obtaining formal approval

Control: 0047; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
All information security documentation should be formally approved by the CISO or their delegate.

Control: 0887; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure that:

- all high-level information security documentation is approved by the agency head or their delegate
- all system-specific documentation is approved by the system owner and an ITSM.

Publication of documentation

Control: 1153; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Once information security documentation has been approved it should be published and communicated to all stakeholders.

Documentation maintenance

Control: 0048; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should regularly review all information security documentation to ensure it is kept current.

Control: 0888; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies review information security documentation:

- at least annually
- in response to significant changes in the environment, business or system.

Control: 1154; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should record the date of the most recent review on each information security document.

Rationale

Information security policy

Information security policy is a statement of high-level information security policies and is therefore an essential part of information security documentation.

Security risk management plan

The SRMP is a best practice approach to identifying and reducing potential security risks. Depending on the documentation framework chosen, multiple systems could refer to, or build upon, a single SRMP.

System security plan

The SSP is derived from the ISM and the SRMP and describes the implementation and operation of controls for a system. Depending on the documentation framework chosen, some details common to multiple systems could be consolidated in a higher level SSP.

Standard operating procedures

SOPs provide a step-by-step guide to undertaking security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by system users without strong knowledge of the system. Depending on the documentation framework chosen, some procedures common to multiple systems could be consolidated into a higher level SOP.

Incident response plan

Having an IRP ensures that when a cyber security incident occurs, a plan is in place to respond appropriately. In most situations, the aim of the response will be to preserve any evidence relating to the cyber security incident and to prevent the incident escalating.

Developing content

It is likely that the most useful and accurate information security documentation will be developed by personnel who are knowledgeable about both information security issues and the business requirements.

Documentation content

As the SRMP, SSP, SOPs and IRP form a documentation suite for a system, it is essential that they are logically connected and consistent. Furthermore, each documentation suite developed for a system will need to be consistent with the information security policy.

Using a documentation framework

Having a documentation framework for information security documents ensures that they are accounted for and maintained appropriately. Furthermore, the framework can be used to describe relationships between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

Outsourcing development of content

Agencies outsourcing the development of information security documentation still need to review and control the contents to make sure it meets their requirements.

Obtaining formal approval

If information security policy does not have formal approval, security personnel will have difficulty ensuring appropriate systems security procedures are in place. Having formal approval not only assists in the implementation of procedures, it also ensures senior managers are aware of information security issues and security risks.

Publication of documentation

If stakeholders are not made aware of new information security documentation, or changes to existing information security documentation, they will not know about any changes they may need to make to the security measures for their systems.

Documentation maintenance

The threat environment and agencies' businesses are dynamic. If an agency fails to keep their information security documentation current to reflect the changing environment, their security measures and processes may cease to be effective. In that situation, resources could be devoted to areas that have reduced effectiveness, or are no longer relevant.

References

Nil.

Information Security Policies

Objective

Information security policies set the strategic direction for information security.

Context

Scope

This section describes the development of information security policies. Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of the information security policy

Control: 0049; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The information security policy should describe information security policies, standards and responsibilities.

Control: 0890; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended the information security policy cover topics such as:

- accreditation processes
- personnel responsibilities
- configuration control
- access control
- networking and connections with other systems
- physical security and media control
- emergency procedures and cyber security incident management
- change management
- information security awareness and training.

Rationale

Contents of the information security policy

Agencies may wish to consider the following when developing their information security policy:

- the policy objectives
- how the policy objectives will be achieved
- the guidelines and legal framework under which the policy will operate
- the stakeholders
- what resourcing will be available to support the implementation of the policy
- what performance measures will be established to ensure the policy is being implemented effectively.

In developing the contents of the policy, agencies may also consult any agency-specific directives that could be applicable to information security.

Agencies should avoid including controls for systems in their policy. Instead, they should be documented in the SSP.

References

Nil.

Security Risk Management Plans

Objective

Security risk management plans identify security risks and appropriate mitigation measures for systems.

Context

Scope

This section describes the development of SRMPs, focusing on security risks related to the operation of systems. Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

System specific security risks

Control: 0009; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should determine system specific security risks that could warrant additional controls to those specified in this manual.

Contents of SRMPs

Control: 0788; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The SRMP should contain a security risk assessment and a corresponding risk treatment strategy.

Agency risk management

Control: 0893; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies incorporate their SRMP into their wider agency risk management plan.

Risk management standards

Control: 0894; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies develop their SRMP in accordance with Australian or international standards for risk management.

Rationale

System specific security risks

While a baseline of controls is provided in this manual, agencies will almost certainly have differing circumstances to those considered during the development of this manual. In such cases an agency needs to follow its own security risk management processes to determine its risk appetite and associated risk acceptance, risk avoidance and risk tolerance thresholds.

Contents of SRMPs

Security risks cannot be managed if they are not known. Even if they are known, failing to deal with them is a failure of security risk management. For this reason SRMPs consist of two components, a security risk assessment and a corresponding risk treatment strategy.

Agency risk management

If an agency fails to incorporate SRMPs for systems into their wider agency risk management plan then the agency will be unable to manage risks in a coordinated and consistent manner across the agency.

Risk management standards

For security risk management to be of true value to an agency it should relate to the specific circumstances of an agency and its systems, as well as being based on an industry recognised approach to risk management, such as those produced by Standards Australia and the ISO/IEC.

Standards Australia produces AS/NZS ISO 31000:2009, *Risk Management – Principles and guidelines* while the ISO/IEC has developed the risk management standard ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management*, as part of the ISO/IEC 27000 family of standards.

References

Information on the development of SRMPs can be found in HB 231:2004, *Information security risk management guidelines*. In particular, section 5 discusses documentation. It is available from Standards Australia at www.standards.org.au.

System Security Plans

Objective

System security plans specify the security measures for systems.

Context

Scope

This section describes the development of SSPs. Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Further information to be included in SSPs about specific functionality or technologies that could be implemented for a system can be found in the applicable areas of this manual.

Stakeholders

There can be many stakeholders involved in defining a SSP, including representatives from the:

- project, who must deliver the capability (including contractors)
- owners of the information to be handled
- system users for whom the capability is being developed
- management audit authority
- information management planning areas
- infrastructure management.

Controls

Contents of SSPs

Control: 0895; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must select controls from this manual to be included in the SSP based on the scope of the system with additional system specific controls being included as a result of the associated SRMP or higher-level SSP.

Control: 0067; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use the latest baseline of this manual when developing, and updating, their SSPs as part of accreditation and reaccreditation of their systems.

Rationale

Contents of SSPs

The ISM provides a list of controls that are potentially applicable to a system based on its classification, its functionality and the technology it is implementing. Agencies need to determine which controls are in scope of the system and translate those controls to the SSP. These controls will then be assessed on their implementation and effectiveness during the accreditation process for the system.

In performing accreditations against the latest baseline of this manual, agencies are ensuring they are taking the most recent threat environment into consideration. DSD continually monitors the threat environment and conducts research into the security impact of emerging trends. With each release of this manual, controls can be added, rescinded or modified depending on changes in the threat environment.

References

Nil.

Standard Operating Procedures

Objective

Standard operating procedures ensure security procedures are followed in an appropriate and repeatable manner.

Context

Scope

This section describes the development of security related SOPs. Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Development of SOPs

Control: 0051; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should develop SOPs for each of the following roles:

- ITSM
- ITSO
- system administrator
- system user.

ITSM SOPs

Control: 0789; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The following procedures should be documented in the ITSM's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Cyber security incidents	Reporting and managing cyber security incidents

ITSO SOPs

Control: 0790; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The following procedures should be documented in the ITSO's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Access control	Authorising access rights to applications and data
Asset musters	Labelling, registering and mustering assets, including media
Audit logs	Reviewing system audit trails and manual logs, particularly for privileged users
Configuration control	Approving and releasing changes to the system software or configurations
Cyber security incidents	Detecting potential cyber security incidents
	Establishing the cause of any cyber security incident, whether accidental or deliberate
	Actions to be taken to recover and minimise the exposure from a cyber security incident

Continued on next page

TOPIC	PROCEDURES TO BE INCLUDED
Data transfers	Managing the review of media containing information that is to be transferred off-site
	Managing the review of incoming media for viruses or unapproved software
ICT equipment	Managing the destruction of unserviceable ICT equipment and media
System integrity audit	Reviewing system user accounts, system parameters and access controls to ensure that the system is secure
	Checking the integrity of system software
	Testing access controls
	Inspecting ICT equipment and cabling
System maintenance	Managing the ongoing security and functionality of system software, including: maintaining awareness of current software vulnerabilities, testing and applying software patches/updates/signatures, and applying appropriate hardening techniques
User account management	Authorising new system users

System administrator SOPs

Control: 0055; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The following procedures should be documented in the system administrator's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Access control	Implementing access rights to applications and data
Configuration control	Implementing changes to the system software or configurations
System backup and recovery	Backing up data, including audit logs
	Securing backup tapes
	Recovering from system failures
User account management	Adding and removing system users
	Setting system user privileges
	Cleaning up directories and files when a system user departs or changes roles

System user SOPs

Control: 0056; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The following procedures should be documented in the system user's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Cyber security incidents	What to do in the case of a suspected or actual cyber security incident
End of day	How to secure systems at the end of the day
Media control	Procedures for handling and using media
Passwords	Choosing and protecting passwords
Temporary absence	How to secure systems when temporarily absent

Agreement to abide by SOPs

Control: 0057; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

ITSMs, ITSOs, system administrators and system users should sign a statement that they have read and agree to abide by their respective SOPs.

Rationale

Development of SOPs

To ensure personnel undertake their duties appropriately, with a minimum of confusion, it is important that the roles of ITSMs, ITSOs, system administrators and system users are covered by SOPs. Furthermore, ensuring that SOPs are consistent with SSPs reduces the potential for confusion resulting from conflicts in policy and procedures.

ITSM SOPs

The ITSM SOPs cover the management and leadership activities related to system operations.

ITSO SOPs

The ITSO SOPs cover the operationally focused activities related to system operations.

System administrator SOPs

The system administrator SOPs support the ITSO SOPs; however, they focus on the administrative activities related to system operations.

System user SOPs

The system user SOPs focus on day to day activities that system users need to know about, and comply with, when using systems.

Agreement to abide by SOPs

When SOPs are produced the intended audience needs to be made aware of their existence and acknowledge that they have read, understood and agree to abide by their contents.

References

Nil.

Incident Response Plans

Objective

Incident response plans outline actions to take in response to a cyber security incident.

Context

Scope

This section describes the development of IRPs to address cyber security incidents. It does not cover physical security incidents. Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of IRPs

Control: 0058; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must include, as a minimum, the following content in their IRP:

- broad guidelines on what constitutes a cyber security incident
- the minimum level of cyber security incident response and investigation training for system users and system administrators
- the authority responsible for initiating investigations of a cyber security incident
- the steps necessary to ensure the integrity of evidence supporting a cyber security incident
- the steps necessary to ensure that critical systems remain operational
- how to formally report cyber security incidents.

Control: 0059; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should include the following content in their IRP:

- clear definitions of the types of cyber security incidents that are likely to be encountered
- the expected response to each cyber security incident type
- the authority responsible for responding to cyber security incidents
- the criteria by which the responsible authority would initiate or request formal, police or ASIO investigations of a cyber security incident
- other authorities which need to be informed in the event of an investigation being undertaken
- the details of the system contingency measures or a reference to these details if they are located in a separate document.

Rationale

Contents of IRPs

The guidance provided on the content of IRPs ensures that agencies have a baseline to develop an IRP with sufficient flexibility, scope and level of detail to address the majority of cyber security incidents that could arise.

References

Nil.

Emergency Procedures

Objective

Information and systems are secured before personnel evacuate a facility in the event of an emergency.

Context

Scope

This section describes the requirements for securing information and systems as part of the procedures for evacuating a facility in the event of an emergency.

Controls

Evacuating facilities

Control: 0062; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must include in evacuation procedures the requirement to secure information and systems before the evacuation; unless the chief warden, to avoid serious injury or loss of life, authorises personnel to evacuate immediately without securing information and systems.

Preparing for the evacuation of facilities

Control: 1159; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should include in evacuation procedures the requirement to secure information and systems during the warning phase before the evacuation.

Rationale

Evacuating facilities

During the evacuation of a facility it is important that personnel secure information and systems as they would at the end of operational hours. This includes, but is not limited to, securing media and logging off workstations. This is important as an attacker could use such an opportunity to gain access to applications or databases that a system user had already authenticated to, or use another system user’s credentials, for a malicious purpose.

Preparing for the evacuation of facilities

The warning phase before the evacuation of a facility alerts personnel that they may be required to evacuate the facility. This warning phase is the ideal time for personnel to begin securing information and systems to ensure that if they need to evacuate the facility they can do so immediately.

References

Nil.

System Accreditation

Accreditation Framework

Objective

Accreditation formalises the acceptance of security risks relating to the operation of a system.

Context

Scope

This section describes the accreditation framework for systems and agencies' responsibilities.

All systems must be accredited before they can be put into operation.

Accreditation is the process by which the accreditation authority formally recognises and accepts the residual security risk to a system and the information it processes, stores and communicates.

The accreditation framework comprises three layers:

- audit:
  - reviewing the information security documentation
  - assessing the appropriateness of the controls applied to the system
  - assessing the effectiveness of the implementation of the controls
- certification:
  - providing independent assurance and acceptance of the audit
  - determining the residual security risk relating to the operation of the system
- accreditation:
  - formally accepting the residual security risk
  - awarding approval to operate the system.

Detailed information about the processes and the requirements for conducting accreditations, certification and audits is given in the *Conducting Accreditations, Conducting Certifications* and *Conducting Audits* sections of this chapter.

Controls

Accreditation framework

Control: 0791; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must develop an accreditation framework.

Accreditation

Control: 0064; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that all systems are awarded accreditation before they are used to process, store or communicate information.

Control: 0065; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that all systems are awarded accreditation before connecting them via a gateway.

Control: 0086; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure information security monitoring activities are conducted on accredited systems.

Determining authorities

Control: 0793; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
For multi-national and multi-agency systems, the certification and accreditation authorities should be determined by a formal agreement between the parties involved.

Notifying authorities

Control: 0082; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Before beginning the accreditation process the system owner should advise the certification and accreditation authorities of their intent to seek certification and accreditation for the system.

Due diligence

Control: 0071; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
If a system exchanges information with a third-party system, the agency must ensure the receiving party has appropriate security measures in place to protect their information.

Control: 0900; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies review a receiving party's accreditation deliverables when determining whether the receiving party has appropriate security measures in place to protect information.

Control: 0072; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that a third party is aware of its security requirements by defining requirements in such documentation as:

- contract provisions
- a memorandum of understanding.

Control: 0073; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure a process is in place to provide assurance to its management that a third party meets, and will continue to meet, security requirements.

Processing restrictions

Control: 0076; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not allow a system to process, store or communicate information above the classification for which the system has received accreditation.

Accrediting systems bearing a caveat or compartment

Control: 0077; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
A system that processes, stores or communicates caveated or compartmented information must be accredited for such caveated or compartmented information.

Requirement for Australian control

Control: 0078; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that systems processing, storing or communicating AUSTEO or AGAO information remain at all times under the control of an Australian national working for the government.

Reaccreditation

Control: 0069; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that the period between accreditations of systems does not exceed two years.

Control: 0070; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that the period between accreditations of systems does not exceed three years.

Rationale

Accreditation framework

Developing an accreditation framework ensures accreditation activities are conducted in a repeatable and consistent manner across the agency.

Accreditation

Accreditation of a system ensures that either sufficient security measures have been put in place or that deficiencies in such measures have been accepted by an appropriate authority. When systems are awarded accreditation, the accreditation authority accepts that the residual security risks are appropriate for the classification of the information the system processes, stores or communicates.

Once systems have been accredited, monitoring activities will assist in assessing changes to the system to determine if the security risk profile and accreditation status need to be reviewed.

Determining authorities

For multi-national and multi-agency systems, determining the certification and accreditation authorities through a formal agreement between the parties ensures the system owner has appropriate points of contact and does not receive conflicting advice from different authorities.

Notifying authorities

In advising the certification and accreditation authorities of their intent to seek certification and accreditation for a system, the system owner can seek information on the latest processes and requirements for the system.

The list of accreditation and certification authorities is given in the *Conducting Accreditations* and *Conducting Certifications* sections of this chapter.

Due diligence

When an agency is connecting a system to another party they need to be aware of the security measures the other party has implemented to protect their information. More importantly, the agency needs to know where the other party may have varied from controls in this manual.

Methods that an agency may use to ensure that third parties comply with their security requirements include:

- conducting an accreditation of the system being connected to
- seeking an information security review by an infosec-registered assessor
- seeking a copy of existing accreditation deliverables in order to make their own accreditation decision.

Ultimately, the agency needs to accept any security risks associated with connecting its system to the other party's system. This includes the other party's system potentially being used as a platform to attack its system or spilling information onto the system requiring subsequent cleanup processes.

Processing restrictions

When security is applied to systems, security measures are put in place based on the highest classification that will be processed, stored or communicated by the system. If classified information is placed on a system, and its classification is higher than the level of accreditation of the system, the information will be inadequately protected and will be exposed to a greater risk of compromise.

Accrediting systems bearing a caveat or compartment

When processing caveated or compartmented information on a system, agencies need to ensure the system has received accreditation for the information. Furthermore, when dealing with AUSTEO or AGAO information agencies need to be aware of the requirement for an Australian national to remain in control of the system at all times.

Requirement for Australian control

As AUSTEO and AGAO systems process, store and communicate information that is particularly sensitive to the Australian Government, it is essential that control of such systems is maintained by Australian citizens working for the Australian Government.

Reaccreditation

Agencies should reaccredit their systems every two years. However, an additional year's grace can be granted if procedures defined in this manual for non-compliance with 'should' requirements are followed: that is, conducting a security risk assessment and obtaining formal approval by senior management.

Once three years has elapsed since the last accreditation, the agency needs to either reaccredit the system or request a dispensation from the appropriate authorities specified in this manual.

Other reasons an agency could seek reaccreditation include:

- changes in information security policies
- detection of new or emerging threats to agency systems
- the discovery that controls are not operating as effectively as planned
- a major cyber security incident
- changes to the system or the risk profile.

References

Nil.

Conducting Accreditations

Objective

Systems are accredited before they are used operationally.

Context

Scope

This section describes conducting an accreditation for a system.

Accreditation aim

The aim of accreditation is to formally recognise and accept the residual security risk to a system and the information it processes, stores or communicates.

Accreditation authorities

For standard systems the accreditation authority is the agency head or their delegate, which is strongly recommended to be the CISO.

For systems that process, store or communicate caveated or compartmented information there may be an accreditation authority external to the agency operating the system.

For multi-national and multi-agency systems the accreditation authority is determined by a formal agreement between the parties involved.

For commercial gateway providers the accreditation authority is the agency head or their delegate, which is strongly recommended to be the CISO.

For supporting organisations the accreditation authority is the head of the supported agency or their authorised delegate, which is strongly recommended to be the CISO.

In all cases the accreditation authority will be at least a senior executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

Depending on the circumstances and practices of an agency, the agency head can choose to delegate their authority to multiple senior executives who have the authority to accept security risks for the specific business functions; for example the CISO and the business owner.

More information on delegation of the agency head's authority can be found in *The Agency Head* section of the *Roles and Responsibilities* chapter.

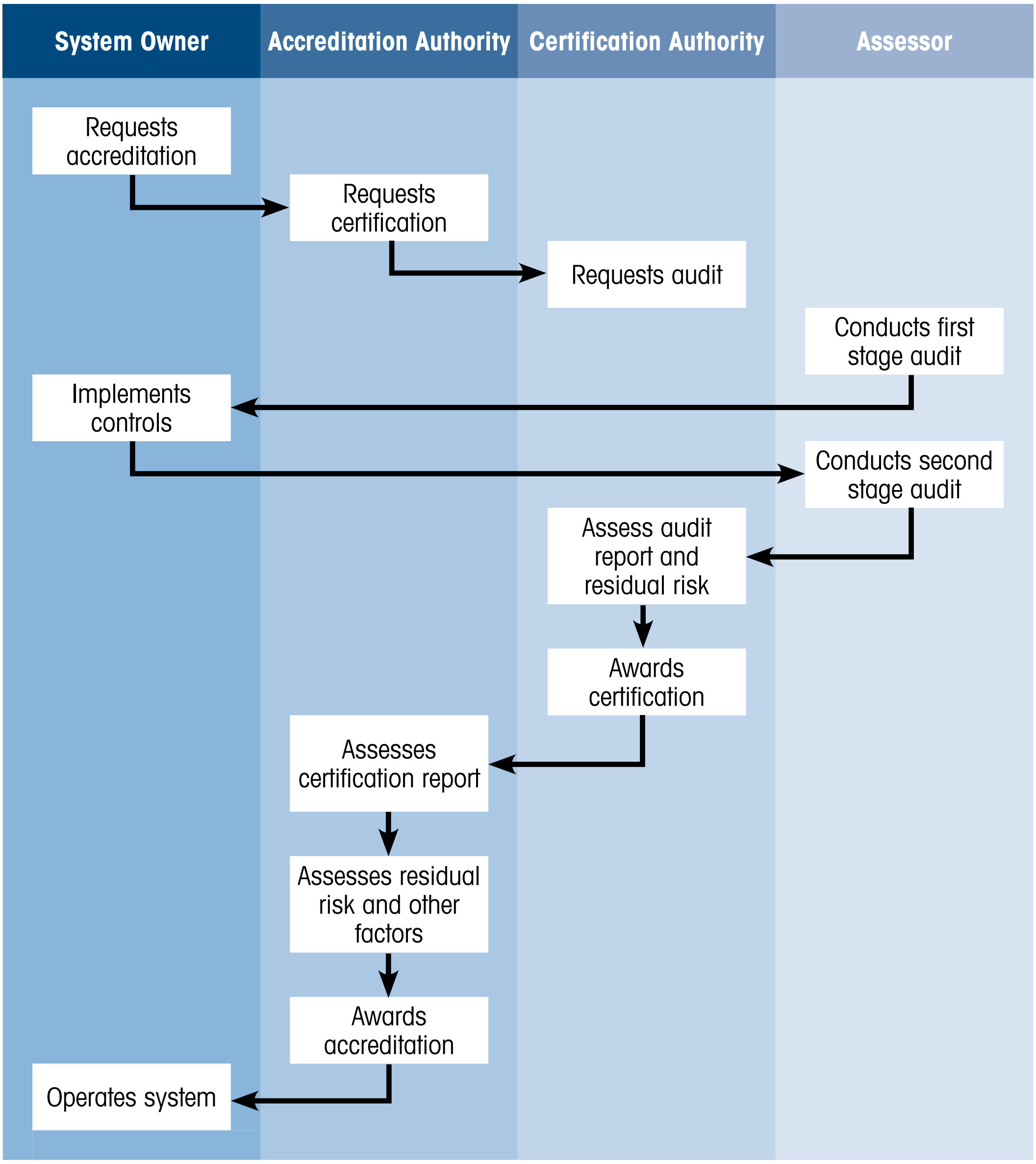
Accreditation outcomes

Accreditation is awarded when the accreditation authority accepts the residual security risk relating to the operation of the system and gives formal approval for the system to operate. However, in some cases the accreditation authority may not accept the residual security risk relating to the operation of the system. This is predominantly due to security risks being insufficiently considered and documented in the SRMP, resulting in security measures being inaccurately scoped in the SSP. In such cases the accreditation authority may request that the SRMP and SSP be amended and security measures reassessed before reconsidering the system for accreditation.

In awarding accreditation for a system, the accreditation authority may specify a shorter period before reaccreditation than that specified in this manual. The accreditation authority may also place restrictions on the use of the system which must be enforced until reaccreditation takes place or until required changes are made to the system.

Accreditation process

The following diagram shows, at a high level, the process of accreditation.



Controls

Certification

Control: 0795; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

All systems must be certified as part of the accreditation process; unless the accreditation authority is satisfied that if the system is not operated immediately it would have a devastating and potentially long lasting effect on operations.

Accreditation decision

Control: 0808; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

The accreditation authority must accept the residual security risk relating to the operation of a system in order to award accreditation.

Rationale

Certification

Certification (described in the *Conducting Certifications* section of this chapter) provides the accreditation authority with information on the security posture of a system. This allows the accreditation authority to make an informed decision on whether the residual security risk of allowing the system to operate is acceptable.

Accreditation decision

The purpose of conducting an accreditation of a system is to determine the security posture of the system and the security risk that it poses to information. In giving approval for the system to operate, the accreditation authority is accepting the residual security risk to information that is processed, stored or communicated by the system.

To assist in making an accreditation decision the accreditation authority may review:

- the SRMP for the system
- the report of compliance from the audit
- the accreditation recommendation from the certification authority
- any decisions to be non-compliant with any controls specified in this manual
- any additional security risk reduction strategies that have been implemented.

To assist in making an informed accreditation decision, the accreditation authority may also seek advice from technical experts on the technical components of information presented to them during the accreditation process.

References

Nil.

Conducting Certifications

Objective

The effectiveness of security measures for systems is accepted.

Context

Scope

This section describes conducting a certification as part of the accreditation process for a system.

Certification aim

The aim of certification is to ensure the audit for a system was conducted in an appropriate manner and to a sufficient degree of quality.

Certification outcome

The outcome of certification is a certificate to the system owner acknowledging the system has been appropriately audited and the controls identified by the system owner have been implemented effectively.

Certification authorities

For TOP SECRET systems the certification authority is DSD.

For SECRET/HIGHLY PROTECTED or below systems the certification authority is the ITSA.

For systems that process, store or communicate caveated or compartmented information there may be a mandated certification authority external to the agency operating the system.

For multi-national and multi-agency systems the certification authority is determined by a formal agreement between the parties involved.

For commercial gateway providers the certification authority is DSD.

For supporting organisations the certification authority is the ITSA of the agency sponsoring the organisation.

Controls

Audit

Control: 1141; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

All systems must undergo an audit as part of the certification process.

Certification decision

Control: 1142; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

The certification authority must accept the effectiveness of controls for the system in order to award certification.

Assessment of residual security risks

Control: 0807; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Following the audit, the certification authority should produce an assessment for the accreditation authority outlining the residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not.

Certification of commercial providers

Control: 0100; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should

Agencies should ensure commercial providers of gateway services have undergone an audit by an infosec-registered assessor and received certification from DSD.

Rationale

Audit

The aim of an audit is to assess the actual implementation and effectiveness of controls for a system. The process of conducting an audit is described in the *Conducting Audits* section of this chapter.

Certification decision

To award certification for a system the certification authority needs to be satisfied the controls identified by the system owner have been implemented and are operating effectively. However, certification only acknowledges that the identified controls were implemented and are operating effectively and not that the residual security risk is acceptable or an approval to operate has been granted.

Assessment of residual security risks

Before the certification authority can make a recommendation to the accreditation authority, an assessment of the residual security risk must be done. The purpose of the assessment is to assess the residual security risk relating to the operation of a system following the audit.

Even if, after the audit, the system is non-conformant the certification authority may be able to recommend to the accreditation authority that accreditation be awarded. For example, since the audit the system owner may have taken corrective actions to address areas of non-compliance or the residual security risk may not be great enough to preclude accreditation.

Certification of commercial providers

As commercial providers of gateway services may be used by multiple agencies across government it is strongly recommended that agencies ensure commercial providers have undergone an audit conducted by an infosec-registered assessor and received certification from DSD. Even though DSD may certify a gateway service from a commercial provider, agencies using the service still need to decide whether accreditation should be awarded or not.

References

Nil.

Conducting Audits

Objective

The effectiveness of security measures for systems is assessed.

Context

Scope

This section describes conducting an audit as part of the certification process for a system.

Audit aim

The aim of an audit is to review the system architecture (including the information security documentation) and assess the actual implementation and effectiveness of controls for a system.

Audit outcome

The outcome of an audit is a report to the certification authority describing areas of compliance and non-compliance for a system and any suggested remediation actions.

Who can conduct an audit

Audits for TOP SECRET systems can only be undertaken by DSD.

Audits for SECRET/HIGHLY PROTECTED and below systems can be undertaken by ITSMs.

Audits for RESTRICTED/PROTECTED and below systems can be undertaken by infosec-registered assessors.

Who can assist with an audit

A number of agencies and personnel are often consulted during an audit.

Agencies or personnel who can be consulted on physical security aspects of information security include:

- ASIO for TOP SECRET sites
- DIO for TOP SECRET SCIFs
- DFAT for systems located at overseas posts and missions
- the ASA for all other systems.

The ASA can be consulted on personnel security aspects of information security.

An ITSM or communications security officer can be consulted on COMSEC aspects of information security.

Independent audits

An audit can be conducted by agency assessors; however, the agency may choose to add an extra level of objectivity by engaging the services of an infosec-registered assessor to undertake the audit.

Connections to certain inter-agency systems could require an independent audit from an infosec-registered assessor as a prerequisite to certification of the system. Such requirements can be obtained from the inter-agency system owners.

Controls

Independence of assessors

Control: 0902; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended that agencies ensure assessors conducting audits are not also the system owner or certification authority.

Audit preparation

Control: 0797; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Before undertaking the audit, the system owner must approve the system architecture and associated information security documentation.

Audit (first stage)

Control: 0798; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The system architecture should be reviewed by the assessor to ensure it is based on sound security principles and meets security requirements.

Control: 0799; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The information security policies should be reviewed by the assessor to ensure policies have been developed or identified to protect information that is processed, stored or communicated by systems.

Control: 0800; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
The SRMP, SSP, SOPs and IRP must be reviewed by the assessor to ensure they are comprehensive and appropriate for the environment the system is to operate in.

Control: 0802; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
The SSP must be reviewed by the assessor to ensure all relevant controls specified in this manual are addressed.

Control: 0904; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The system owner should provide a statement of applicability for the system which includes the following topics:

- the baseline of this manual used for determining controls
- controls that are, and are not, applicable to the system
- controls that are applicable but are not being complied with
- any additional controls implemented as a result of the SRMP.

Implementing controls

Control: 0084; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Before undertaking the second stage of the audit the system owner must implement the controls for the system.

Audit (second stage)

Control: 0805; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
The implementation of controls must be assessed to determine whether they have been implemented and are operating effectively.

Control: 0806; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
The assessor must ensure, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.

Control: 0905; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that the physical security certification be less than five years old at the time of the audit.

Report of compliance

Control: 1140; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
The assessor must produce a report of compliance for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

Rationale

Independence of assessors

As there can be a perceived conflict of interest in the system owner assessing the security of their own system it is recommended that the assessor be independent of the system owner and certification authority. This does not preclude an appropriately qualified system owner from assessing the security of a system that they are not responsible for.

Audit preparation

Ensuring the system owner has approved the system architecture and associated information security documentation assists assessors in determining the scope of work for the first stage of the audit.

Audit (first stage)

The purpose of the first stage of the audit is to determine the system architecture (including information security documentation) is based on sound security principles and has addressed all applicable controls from this manual. During this stage the statement of applicability for the system will also be assessed along with any justification for non-compliance with applicable controls from this manual.

Implementing controls

Without implementing the controls for a system their effectiveness cannot be assessed during the second stage of the audit.

Audit (second stage)

The purpose of the second stage of the audit is to determine whether the controls, as approved by the system owner and reviewed during the first stage of the audit, have been implemented and are operating effectively.

Report of compliance

The report of compliance helps the certification authority assess the residual security risk relating to the operation of a system following the audit and any remediation activities the system owner may have undertaken.

References

Policy and Procedures for the InfoSec-Registered Assessor Program contains a definition of the range of activities infosec-registered assessors are authorised to perform. It can be obtained from DSD's website at www.dsd.gov.au/infosec/irap.htm.

Information Security Monitoring

Vulnerability Management

Objective

Vulnerability management activities maintain the security posture of systems.

Context

Scope

This section describes agencies' requirements for conducting vulnerability management activities for their systems.

Vulnerability assessments

A vulnerability assessment can cover anything from a single system to all of the systems that belong to the agency.

A vulnerability assessment:

- identifies any changes to the security risks faced by the target of the assessment
- assesses the effectiveness of the existing counter-measures
- reports on any changes necessary to maintain an effective security posture.

Controls

Conducting vulnerability assessments

Control: 0911; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies conduct vulnerability assessments on systems:

- before the system is first used
- after a significant change to the system
- as specified by an ITSM or the system owner.

Control: 0105; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should undertake and document vulnerability assessments of their systems at least annually.

Control: 0909; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies have vulnerability assessments conducted by personnel independent to the target of the assessment or by an independent third party.

Resolving vulnerabilities

Control: 0113; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must analyse and treat any security risks to their systems identified during a vulnerability assessment.

Vulnerability analysis strategy

Control: 0112; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should implement a vulnerability analysis strategy by:

- monitoring information about new vulnerabilities in operating systems and application software
- considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner
- running manual checks against system configurations to ensure only allowed services are active and that disallowed services are prevented
- using security checklists and hardening guides to secure operating systems and common applications.

Rationale

Conducting vulnerability assessments

Conducting vulnerability assessments prior to systems being used and after significant changes can allow the agency to establish a baseline for further information security monitoring activities.

Conducting vulnerability assessments annually can help ensure that the latest threat environment is being addressed and that systems are configured in accordance with associated information security documentation.

It is recommended that vulnerability assessments are conducted by personnel independent of the target or by an independent third party. This ensures there is no conflict of interest, perceived or otherwise, and the assessment is undertaken in an objective manner.

An agency may choose to undertake a vulnerability assessment either:

- as a result of a specific cyber security incident
- after a change to a system or its environment that significantly impacts on the agreed and implemented system architecture and information security policy
- as part of a regular scheduled assessment.

Agencies will find it useful to gather appropriate information before they start a vulnerability assessment. This will help to ensure the assessment is undertaken to a degree commensurate with the threat environment, and if applicable, the highest classification of information involved.

Depending on the scope and subject of the vulnerability assessment, agencies may gather information on areas such as:

- agency priorities and business requirements
- threat data
- likelihood and consequence estimates
- effectiveness of existing counter-measures
- other possible counter-measures
- best practices.

Resolving vulnerabilities

Agencies may wish to consider that discovered vulnerabilities could be a result of their security practices, accidental activities or malicious activities and not just as the result of a technical issue.

When an agency decides to implement changes to a system to address security risks resulting from a vulnerability assessment it will need to follow its change management processes, as for any other change.

Vulnerability analysis strategy

Agencies are encouraged to monitor information about new vulnerabilities that could affect their systems. However, they should not be complacent if no vulnerabilities are disclosed in specific products used in their systems.

Vulnerabilities can be introduced as a result of poor security practices or accidental activities. Therefore, even if no new vulnerabilities in deployed products have been disclosed there is still value to be gained from conducting regular vulnerability analyses.

Furthermore, by monitoring vulnerabilities, conducting vulnerability analyses, keeping up to date with industry and product advances, and keeping up to date with changes to the ISM, agencies will become aware of factors which may adversely impact the security risk profile of their systems.

References

Nil.

Change Management

Objective

Information security is an integral part of the change management process.

Context

Scope

This section describes the importance of maintaining the security of systems when implementing routine and urgent changes.

Identifying the need for change

The need for change can be identified in various ways, including:

- system users identifying problems or enhancements
- vendors notifying upgrades to software or ICT equipment
- vendors notifying the end of life to software or ICT equipment
- advances in technology in general
- implementing new systems that necessitate changes to existing systems
- identifying new tasks requiring updates or new systems
- organisational change
- business process change
- standards evolution
- government policy or Cabinet directives
- other incidents or continuous improvement activities.

Types of system change

A proposed change to a system could involve either:

- an upgrade to, or introduction of, ICT equipment
- an upgrade to, or introduction of, software
- major changes to access controls.

Controls

Change management

Control: 0115; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure that for routine and urgent changes:

- the change management process, as defined in the relevant information security documentation, is followed
- the proposed change is approved by the relevant authority
- any proposed change that could impact the security of a system is submitted to the accreditation authority for approval
- all associated information security documentation is updated to reflect the change.

Change management process

Control: 0117; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

The change management process must define appropriate actions to be followed before and after urgent changes are implemented.

Control: 0912; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use the following change management process:

- produce a written change request
- submit the change request for approval
- document the changes to be implemented
- implement and test the approved changes
- update the relevant information security documentation including the SRMP, SSP and SOPs
- notify and educate system users of the changes that have been implemented as close as possible to the time the change is applied
- continually educate system users in regard to changes.

Changes impacting the security of a system

Control: 0809; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
When a configuration change impacts the security of a system, and is subsequently assessed as having changed the overall security risk for the system, the system must undergo reaccreditation.

Rationale

Change management

As part of any change process it is important all stakeholders are consulted before the change is implemented. In the case of changes that will affect the security of a system, the accreditation authority will need to be consulted and approval sought.

The most likely scenario for bypassing change management processes is when an urgent change needs to be made to a system. In such cases it is essential the change management process strongly enforces appropriate actions to be taken before and after an urgent change is implemented.

Change management process

The change management process ensures changes to systems are made in an accountable manner with due consideration and with appropriate approval. Furthermore, the change management process provides an opportunity for the security impact of the change to be considered and if necessary reaccreditation processes initiated.

Changes impacting the security of a system

The accreditation for a system is the acceptance of the residual security risk relating to the operation of the system. It is important therefore that, when a change occurs that impacts the overall security risk for the system, the accreditation authority is consulted on whether the residual security risk for the system is still acceptable.

References

Nil.

Business Continuity and Disaster Recovery

Objective

Business continuity minimises the disruption to the availability of information and systems after a disaster.

Context

Scope

This section describes the role of business continuity and disaster recovery plans in ensuring continuing operation of agencies' critical systems.

Controls

Availability requirements

Control: 0118; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must determine availability requirements for their systems and implement appropriate security measures to support these requirements.

Backup strategy

Control: 0119; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should:

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

Business continuity plan

Control: 0913; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies develop a business continuity plan.

Disaster recovery plan

Control: 0914; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies develop a disaster recovery plan.

Rationale

Availability requirements

As availability requirements will vary based on business requirements they cannot be stipulated in this manual. Agencies will need to determine their own availability requirements and implement appropriate security measures to achieve them.

Backup strategy

Having a backup strategy in place is an important part of business continuity planning. The backup strategy ensures critical business information is not accidentally lost.

Business continuity plan

Developing a business continuity plan can help ensure critical functions of systems continue to operate when the system is in a degraded state. For example, when limited bandwidth is available on networks agencies may choose to strip all large attachments from emails.

Disaster recovery plan

Developing a disaster recovery plan will reduce the time between a disaster occurring and critical functions of systems being restored.

References

Additional information relating to business continuity is contained in HB 221:2004, *Business Continuity Management.*

Cyber Security Incidents

Detecting Cyber Security Incidents

Objective

Tools and appropriate procedures detect cyber security incidents.

Context

Scope

This section describes controls aimed at detecting cyber security incidents. It does not cover detecting physical and personnel security incidents.

Additional information relating to detecting cyber security incidents can be found in the following chapters and sections:

- *Information Security Monitoring: Vulnerability Management*
- *Personnel Security for Systems: Information Security Awareness and Training*
- *Access Control: Event Logging and Auditing*
- *Network Security: Intrusion Detection and Prevention.*

Controls

Preventing and detecting cyber security incidents

Control: 0120; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must develop, implement and maintain tools and procedures covering the detection of potential cyber security incidents, incorporating:

- counter-measures against malicious code
- intrusion detection strategies
- audit analysis
- system integrity checking
- vulnerability assessments.

Control: 0121; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention as opposed to detection of cyber security incidents.

Rationale

Preventing and detecting cyber security incidents

The activities listed for assisting in detecting cyber security incidents will assist in mitigating the most common methods of attack used to exploit systems.

Many potential cyber security incidents are noticed by personnel rather than software tools. However for this to happen, personnel must be well trained and aware of information security issues and know how to recognise possible cyber security incidents.

Automated tools are only as good as the quality of the analysis they provide. If tools are not adequately configured to assess potential security risks then it will not be evident when a weakness emerges. Additionally, if the tools are not regularly updated to include knowledge of new vulnerabilities their effectiveness will be reduced.

Agencies may consider some of the tools described in the table below for detecting potential cyber security incidents.

TOOL	DESCRIPTION
Anomaly detection systems	Monitor network and host activities that do not conform to normal system activity.
Intrusion prevention systems	Some IDSs 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.
Log analysis	Involves collecting and analysing event logs using pattern recognition to detect anomalous activities.
Network and host IDSs	Monitor and analyse network and host activity, usually relying on a list of known attack signatures to recognise potential cyber security incidents.
System integrity verification	Used to detect changes to critical system components such as files, directories or services. These changes may alert a system administrator to unauthorised changes that could signify an attack on the system and inadvertent system changes that render the system open to attack.

References

Nil.

Reporting Cyber Security Incidents

Objective

Reported cyber security incidents assist in maintaining an accurate threat environment picture for government systems.

Context

Scope

This section describes agencies' responsibilities for reporting cyber security incidents. It does not cover reporting physical or personnel security incidents.

Cyber security incidents and outsourcing

The requirement to lodge a cyber security incident report applies even when an agency has outsourced some or all of its information technology functions and services.

Categories of cyber security incidents

The Cyber Security Event Reporting scheme defines two categories of cyber security incidents: red and yellow. Red cyber security incidents are considered to be significant while yellow cyber security incidents are considered to be non-significant.

Controls

Reporting cyber security incidents

Control: 0123; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must direct personnel to report cyber security incidents to an ITSM as soon as possible after the cyber security incident is discovered.

Control: 0124; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should:

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

Reporting significant cyber security incidents to DSD

Control: 0139; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies, through an ITSM, must report significant cyber security incidents to DSD.

Reporting non-significant cyber security incidents to DSD

Control: 0918; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended that agencies, through an ITSM, report non-significant cyber security incidents to DSD.

How to report cyber security incidents to DSD

Control: 0140; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should formally report cyber security incidents using the CSER scheme.

Outsourcing and cyber security incidents

Control: 0141; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies that outsource their information technology services and functions must ensure the service provider consults with the agency when a cyber security incident occurs.

Cryptographic keying material

Control: 0142; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

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

High grade cryptographic keying material

Control: 0143; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: required

Agencies are required to notify DSD of any suspected loss or compromise of keying material associated with HGCE in accordance with *ACSI 107*.

Rationale

Reporting cyber security incidents

Reporting cyber security incidents to an ITSM as soon as possible provides management with a means to assess the overall damage to a system and to take remedial action including seeking advice from DSD if necessary.

Reporting significant cyber security incidents to DSD

DSD uses significant cyber security incident reports as the basis for identifying and responding to cyber security events across government. Significant incidents are also used for developing new policies, procedures, techniques and training measures to prevent the recurrence of similar cyber security incidents across government.

Reporting non-significant cyber security incidents to DSD

DSD uses non-significant cyber security incident reports as the basis for identifying trends in cyber security incidents and for developing new policies, procedures, techniques and training measures to prevent the recurrence of similar cyber security incidents across government.

How to report cyber security incidents to DSD

Reporting cyber security incidents to DSD through the appropriate channels ensures appropriate and timely assistance can be provided. In addition, it allows DSD to maintain an accurate threat environment picture for government systems.

Outsourcing and cyber security incidents

When an agency outsources information technology services and functions, they are still responsible for reporting of cyber security incidents. The agency must ensure the service provider informs them of all cyber security incidents to allow them to formally report these to DSD.

Cryptographic keying material

Reporting any cyber security incident involving the loss or misuse of cryptographic keying material is particularly important. Systems users rely on the use of cryptographic keying material for the confidentiality and integrity of their secure communications.

High grade cryptographic keying material

ACSI 107 applies to all agencies including contractors. Its requirements cover all HGCE used to process classified information.

For cyber security incidents involving the suspected loss or compromise of HGCE keying material, DSD will investigate the possibility of compromise, and where possible, initiate action to reduce the impact of the compromise.

References

Further information on reporting cyber security incidents is located on the DSD website at www.dsd.gov.au/infosec/reportincident.htm.

Further information on the categories of cyber security incidents can be found in www.dsd.gov.au/_lib/pdf_doc/isir_categories.pdf.

Managing Cyber Security Incidents

Objective

Appropriate remedies assist in preventing future cyber security incidents.

Context

Scope

This section describes procedures for managing cyber security incidents. The management of physical and personnel security incidents is out of scope unless it directly impacts on the protection of systems (for example, breaching physical protection for a server room).

Controls

Cyber security incident management documentation

Control: 0122; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must detail cyber security incident responsibilities and procedures for each system in the relevant SSP, SOPs and IRP.

Recording cyber security incidents

Control: 0125; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that all cyber security incidents are recorded in a register.

Control: 0126; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should include, at minimum, the following information in their register:

- the date the cyber security incident was discovered
- the date the cyber security incident occurred
- a description of the cyber security incident, including the personnel and locations involved
- the action taken
- to whom the cyber security incident was reported
- the file reference.

Control: 0916; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies use their register as a reference for future security risk assessments.

Handling data spills

Control: 0129; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

When a data spill occurs agencies must assume the information has been compromised.

Control: 0130; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must include in standard procedures for all personnel with access to systems a requirement that they notify an ITSM of any data spillage and access to any data which they are not authorised to access.

Control: 0131; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must document procedures for dealing with data spills in their IRP.

Control: 0132; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must treat any data spill as a cyber security incident and follow the IRP to deal with it.

Control: 0133; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

When a data spill occurs agencies must report the details of the data spill to the information owner.

Containing data spills

Control: 0134; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
When information is introduced onto a system not accredited to handle the information, personnel must not delete the information until advice is sought from an ITSM.

Control: 0135; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
When information is introduced onto a system not accredited to handle the information, personnel should not copy, view, print or email the information.

Control: 0136; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
When information is introduced onto a system not accredited to handle the information, agencies should segregate the affected system from the network.

Handling malicious code infection

Control: 0917; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies follow the steps described below when malicious code is detected:

- isolate the infected system
- decide whether to request assistance from DSD, and if such assistance is requested and agreed to, delay any further action until advised by DSD to continue
- scan all previously connected systems, and any media used in a set period leading up to the cyber security incident, for malicious code
- isolate all infected systems and media to prevent reinfection
- change all passwords and key material stored or potentially accessed from compromised systems
- advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems
- use current antivirus software to remove the infection from the systems or media
- report the cyber security incident and perform any other activities specified in the IRP.

Allowing continued attacks

Control: 0137; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies considering allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence should seek legal advice.

Integrity of evidence

Control: 0138; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should:

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

Seeking assistance

Control: 0915; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure any requests for DSD assistance are made as soon as possible after the cyber security incident is detected and that no actions, which could affect the integrity of the evidence, are carried out before DSD’s involvement.

Rationale

Cyber security incident management documentation

Documenting responsibilities and procedures for cyber security incidents in relevant SSPs, SOPs and the IRP ensures that when a cyber security incident does occur, personnel can respond in an appropriate manner. In addition, ensuring system users are aware of reporting procedures assists in capturing any cyber security incidents that an ITSM, ITSO or system owner fail to notice.

Recording cyber security incidents

The purpose of recording cyber security incidents in a register is to highlight the nature and frequency of the cyber security incidents so that corrective action can be taken. This information can subsequently be used as an input into future security risk assessments of systems.

Handling data spills

Assuming information is compromised as a result of a cyber security incident allows an agency to apply procedures in response to a worst case scenario.

Containing data spills

The spillage of information onto a system not accredited to handle it is considered a significant cyber security incident under the DSD CSER scheme.

An affected system can be segregated by powering off the system, removing network connectivity to the device or applying access controls on information associated with the data spill to prevent access. However it should be noted that powering off the system could destroy information that would be useful for forensics activities at a later date.

Handling malicious code infection

The guidance for handling malicious code infections is provided to help prevent the spread of the infection and to prevent reinfection. An important consideration is the infection date of the machine. However when determining the infection date it is important to bear in mind that the record could be inaccurate as a result of the infection.

A complete operating system reinstallation, or an extensive comparison of characterisation information, is the only reliable way to ensure malicious code is eradicated.

Allowing continued attacks

Agencies allowing an attacker to continue an attack against a system in order to seek further information or evidence will need to establish with their legal advisors whether the actions are breaching the *Telecommunications (Interception and Access) Act 1979* (the TIA Act*).*

Integrity of evidence

While gathering evidence it is important to maintain the integrity of the information. Even though in most cases an investigation does not directly lead to a police prosecution, it is important the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs is protected.

Seeking assistance

If the integrity of evidence of a cyber security incident is compromised it reduces DSD's ability to assist agencies. DSD therefore requests that no actions which could affect the integrity of the evidence be carried out before DSD's involvement.

References

Further information relating to the management of ICT evidence is contained in HB 171:2003, *Guidelines for the management of information technology* evidence.

Physical Security

Physical Security for Systems

Facilities

Objective

Physical security measures applied to facilities protect systems and their infrastructure.

Context

Scope

This section describes the requirements for the physical security of facilities. Information on servers and network devices, network infrastructure and ICT equipment can be found in other sections of this chapter.

Physical security requirements for storing classified information

Many of the physical controls in this manual are derived from the *Physical Security Protocol* of the PSPF. In particular the minimum standard of security container, secure room or lockable commercial cabinet needed for storing classified information outside of operational hours.

Physical security requirements for processing classified information

In addition to the physical security requirements for storing classified information, the requirements for processing classified information are specified under the definitions for Secure Area, Partially Secure Area and Intruder Resistant Area in the *Physical Security Protocol* of the PSPF.

Secured and unsecured spaces

In the context of this manual a secured space is a facility that has security measures in place for the processing of classified information. These secured spaces can be constructed with assistance from two different ASIO technical notes. These are the *Secure/Partial Secure Area* technical note and the *Intruder Resistant Area* technical note. Areas that are not certified as meeting the requirements for a secured space are known as unsecured spaces.

Facilities

In the context of this manual a facility is an area that facilitates government business. For example, a facility can be a building, a floor of a building or a designated space on the floor of a building.

Physical security certification authorities

The certification of physical security measures is undertaken by:

- the ASA for areas processing up to SECRET/HIGHLY PROTECTED information
- ASIO for areas processing up to TOP SECRET information
- DIO for TOP SECRET SCIFs.

Facilities located outside of Australia

Agencies operating sites in posts or missions located outside of Australia can contact DFAT to determine any additional requirements which may exist.

Controls

Facility physical security

Control: 0810; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure any facility containing a system or its associated infrastructure, including deployable systems, is certified against minimum physical security requirements in the *Physical Security Protocol* of the PSPF.

Preventing observation by unauthorised people

Control: 0164; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should prevent unauthorised people from observing systems, in particular displays and keyboards.

Control: 0919; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies position screens and keyboards so they cannot be seen by unauthorised people, or fix blinds or drapes to the inside of windows.

Bringing non-agency owned devices into secured spaces

Control: 0172; Revision: 1; Updated: Sep-09; Applicability: TS; Compliance: must not
Agencies must not permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the accreditation authority.

Technical surveillance counter-measure testing

Control: 0173; Revision: 1; Updated: Sep-09; Applicability: TS; Compliance: must
Agencies must ensure technical surveillance counter-measure tests are conducted as determined by the outcomes of a security risk assessment and as a part of the physical security certification.

Rationale

Facility physical security

The application of defence-in-depth to the protection of systems and infrastructure is enhanced through the use of successive layers of physical security. The first layer of security is the use of a secured facility, the second layer is the use of a secured server room (when appropriate) and the final layer is the use of security containers or lockable commercial cabinets. All layers are designed to limit access to those with the appropriate authorisation to access the system and infrastructure.

Deployable platforms need to meet physical security certification requirements as per any other system. Physical security certification authorities dealing with deployable platforms can have specific requirements that supersede the requirements of this manual and as such security personnel should contact their appropriate physical security certification authority to seek guidance.

In the case of deployable platforms, physical security requirements may also include perimeter controls, building standards and personnel levels.

Preventing observation by unauthorised people

Facilities without sufficient perimeter security are often exposed to the potential for observation through windows. Ensuring information on workstation screens is not visible will assist in reducing this security risk.

Bringing non-agency owned devices into secured spaces

At the request of the accreditation authority for TOP SECRET areas, non-agency owned devices are not to be brought into such facilities without approval.

Technical surveillance counter-measure testing

Technical surveillance counter-measure testing is conducted as part of the physical security certification to ensure facilities do not have any unauthorised listening devices.

References

Further information relating to physical security, including technical surveillance counter-measure testing, is also contained in the *Physical Security Protocol* of the PSPF.

Further information on endorsed blinds and drapes is available in the *Security Equipment Catalogue* produced by SCEC.

Servers and Network Devices

Objective

Secured server and communications rooms protect servers and network devices.

Context

Scope

This section describes the requirements for the physical security of servers and network devices. Information relating to network infrastructure and ICT equipment can be found in other sections of this chapter.

Secured server and communications rooms

Agencies can certify the physical security of a server or communications room to the requirements of the *Physical Security Protocol* of the PSPF to provide an additional layer of physical security for servers and network devices. In such cases, because of the additional layer of security, the requirements for physical storage specified in the *Physical Security Protocol* can be lowered.

Agencies choosing not to use a server or communications room, or using a server or communications room that does not meet the requirements of the *Physical Security Protocol* of the PSPF, will still need to meet the storage requirements as set out in the *Physical Security Protocol* of the PSPF based on the physical security certification of the surrounding facility.

Controls

Securing servers and network devices

Control: 1053; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure servers and network devices are secured in cabinets as shown in the tables below.

SECURE FACILITY						
CLASSIFICATION	SECURE ROOM	INTRUDER RESISTANT ROOM	UNSECURED ROOM / NO ROOM	A CLASS VAULT	B CLASS VAULT	C CLASS VAULT
TOP SECRET	Class C	Class B	Class B	Lockable Commercial	Lockable Commercial	Prohibited
SECRET/HIGHLY PROTECTED	Lockable Commercial	Lockable Commercial	Class C	Lockable Commercial	Lockable Commercial	Lockable Commercial
CONFIDENTIAL	Lockable Commercial	Lockable Commercial	Class C	Lockable Commercial	Lockable Commercial	Lockable Commercial
PROTECTED	Lockable Commercial	Lockable Commercial	Class C	Lockable Commercial	Lockable Commercial	Lockable Commercial
RESTRICTED	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial
IN-CONFIDENCE	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial
UNCLASSIFIED	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial

PARTIALLY SECURE FACILITY						
CLASSIFICATION	SECURE ROOM	INTRUDER RESISTANT ROOM	UNSECURED ROOM / NO ROOM	A CLASS VAULT	B CLASS VAULT	C CLASS VAULT
TOP SECRET	Class C	Class A	Class A	Lockable Commercial	Prohibited	Prohibited
SECRET/HIGHLY PROTECTED	Lockable Commercial	Class B	Class B	Lockable Commercial	Lockable Commercial	Prohibited
CONFIDENTIAL	Lockable Commercial	Class C	Class C	Lockable Commercial	Lockable Commercial	Lockable Commercial
PROTECTED	Lockable Commercial	Class C	Class C	Lockable Commercial	Lockable Commercial	Lockable Commercial
RESTRICTED	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial
IN-CONFIDENCE	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial
UNCLASSIFIED	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial

INTRUDER RESISTANT FACILITY						
CLASSIFICATION	SECURE ROOM	INTRUDER RESISTANT ROOM	UNSECURED ROOM / NO ROOM	A CLASS VAULT	B CLASS VAULT	C CLASS VAULT
TOP SECRET	Class B	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
SECRET/HIGHLY PROTECTED	Lockable Commercial	Class A	Class A	Lockable Commercial	Prohibited	Prohibited
CONFIDENTIAL	Lockable Commercial	Class B	Class B	Lockable Commercial	Lockable Commercial	Prohibited
PROTECTED	Lockable Commercial	Class B	Class B	Lockable Commercial	Lockable Commercial	Prohibited
RESTRICTED	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial
IN-CONFIDENCE	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial
UNCLASSIFIED	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial	Lockable Commercial

Extending alarm coverage

Control: 0812; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: must

Agencies choosing to use a secured server or communications room certified as an Intruder Resistant Area in a secured facility certified as a Secure Area must extend the type one alarm system coverage for the facility into the server or communications room.

Securing server rooms, communications rooms and security containers

Control: 0813; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not leave server rooms, communications rooms or security containers in an unsecured state.

Control: 1074; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

No-lone zones

Control: 0150; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies operating no-lone zones must suitably signpost the area and have all entry and exit points appropriately secured.

Administrative measures

Control: 0151; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must develop a site security plan for each server and communications room covering:

- a summary of the security risk review for the facility
- roles and responsibilities of facility and security personnel
- the administration, operation and maintenance of the electronic access control system or security alarm system
- key management, the enrolment and culling of system users and issuing of personal identification number codes
- personnel security clearances, information security awareness training and regular briefings
- inspection of the generated audit trails and logs
- end of day checks and lockup
- reporting of cyber security incidents
- activities to undertake in response to security alarms.

Rationale

Securing servers and network devices

When an agency chooses to implement a security container for a server or network device in a non-secured server or communications room, or outside a server or communications room, it needs to comply with the requirements of the *Physical Security Protocol* of the PSPF. However, when an agency stores a server or network device in a secured server or communications room, the storage requirements for the server or network device can be lowered in some situations due to the multiple layers of physical security.

While this manual aims to equate the security measures for PROTECTED and RESTRICTED systems, the physical security requirements in the *Physical Security Protocol* of the PSPF differ. However, when agencies with RESTRICTED systems meet the physical security requirements for PROTECTED systems they can treat the systems as equal. For example, certifying a server room containing RESTRICTED servers as a Secure Room will also meet the requirements for a server room containing PROTECTED servers. However, certifying a server room as an Intruder Resistant Room will not unless it is within a larger Secure Facility.

Extending alarm coverage

When a server or communications room certified as an Intruder Resistant Area is constructed in a facility certified as a Secure Area the type one alarm system for the facility still needs to cover the interior of the server or communications room.

Securing server rooms, communications rooms and security containers

If personnel decide to leave server rooms, communications rooms or security containers with keys in locks, unlocked or with security functions disabled, it negates the purpose of providing security. Such activities will compromise the security efforts and should not be permitted.

No-lone zones

Areas containing particularly sensitive materials or ICT equipment can be provided with additional security through the use of a designated no-lone zone. The aim of this designation is to enforce two-person integrity, where all actions are witnessed by at least one other person.

Administrative measures

Site security plans, the physical security equivalent of the SSP and SOPs for systems, are used to document all aspects of physical security for systems. Formally documenting this information ensures that standards, controls and procedures can easily be reviewed by security personnel.

The development of the security risk review is a requirement specified in the *Physical Security Protocol* of the PSPF and is the responsibility of the ASA.

References

Nil.

Network Infrastructure

Objective

Network infrastructure is protected by secured facilities and the use of encryption technologies.

Context

Scope

This section describes the physical security of network infrastructure. Information relating to servers, network devices and ICT equipment can be found in other sections of this chapter. Additionally, information on using encryption for infrastructure in unsecured spaces can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Controls

Network infrastructure in secured spaces

Control: 0156; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must certify the physical security of facilities containing network infrastructure to the highest classification of information being communicated over the network infrastructure.

Control: 1070; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended that agencies communicating information over infrastructure in secured spaces encrypt classified information with at least a DACP.

Protecting network infrastructure

Control: 0152; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should

Agencies should locate patch panels, fibre distribution panels and structured wiring enclosures in at least lockable commercial cabinets.

Control: 0153; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must locate patch panels, fibre distribution panels and structured wiring enclosures in at least lockable commercial cabinets.

Network infrastructure in unsecured spaces

Control: 0157; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies communicating classified information over public network infrastructure or over infrastructure in unsecured spaces must use encryption to lower requirements to that for unclassified and public networks.

Rationale

Network infrastructure in secured spaces

Network infrastructure processes information being communicated across it and therefore needs to meet the minimum physical security requirements for processing classified information as specified in the *Physical Security Protocol* of the PSPF. The requirements for physical security of network infrastructure can be lowered if encryption is being applied to classified information communicated over the infrastructure (data in transit encryption).

While secured spaces may provide adequate physical protection for classified information being communicated over infrastructure in the space, they do not provide any protection against a malicious entity that may be residing on the network. If classified information being communicated over the infrastructure is not encrypted, the malicious entity can capture the traffic and use it to exploit the network and the information being communicated across it.

Protecting network infrastructure

Patch panels, fibre distribution panels and structure wiring enclosures need to be placed in at least lockable commercial cabinets, to prevent tamper with them. Furthermore, keys for such cabinets should not be kept in locks as this defeats the purpose of using lockable commercial cabinets.

Network infrastructure in unsecured spaces

Agencies lose control over classified information when it is communicated over unsecured public network infrastructure or over infrastructure in unsecured spaces, they must ensure information is encrypted to a sufficient level that if it was captured it would not be cost-effective to retrieve the original information.

References

Nil.

ICT Equipment

Objective

ICT equipment is secured during non-operational hours.

Context

Scope

This section describes the physical security of ICT equipment containing media. This includes but is not limited to workstations, printers, photocopiers, scanners and multifunction devices.

Additional information relating to ICT equipment and media can be found in the *Fax Machines and Multifunction Devices* section of the *Communications Systems and Devices* chapter as well as in the *Product Security* and *Media Security* chapters.

Handling ICT equipment containing media

During non-operational hours, media that resides in ICT equipment and that contains classified information needs to be stored in accordance with the *Physical Security Protocol* of the PSPF. This can be achieved by doing one of the following:

- ensuring ICT equipment always reside in an appropriate class of secure room
- storing ICT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet
- using ICT equipment with removable non-volatile media which is stored during non-operational hours in an appropriate class of security container or lockable commercial cabinet as well as securing its volatile media
- using ICT equipment without non-volatile media as well as securing its volatile media
- using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media
- configuring ICT equipment to prevent the storage of classified information on the non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown as well as securing its volatile media.

The intent of security measures such as cryptography, preventing the storage of classified information on non-volatile media, scrubbing temporary data at logoff or shutdown, and securing volatile media, is to treat media used in ICT equipment as per the storage requirements of a lower classification during non-operational hours.

The security measures described in the previous paragraph do not constitute sanitisation and reclassification of the media. Therefore, the media retains its classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal as specified in this manual.

ICT equipment using hybrid hard drives or solid state drives

When hybrid hard drives and solid state drives are used, the practices preventing the storage of classified information on non-volatile media and enforced scrubbing of temporary data at logoff or shutdown are not approved as a method of lowering the storage requirements specified in the *Physical Security Protocol* of the PSPF.

Controls

Accounting for ICT equipment

Control: 0159; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must account for all ICT equipment containing classified media.

Physical security for facilities containing ICT equipment

Control: 0160; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must certify the physical security of facilities containing ICT equipment to the highest classification of information being processed, stored or communicated by the equipment in the facilities.

Securing ICT equipment during non-operational hours

Control: 0161; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that during non-operational hours ICT equipment with classified media is secured in accordance with the minimum physical security requirements for storing classified information as specified in the *Physical Security Protocol* of the PSPF.

Securing non-volatile media for storage

Control: 0162; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies choosing to prevent the storage of classified information on non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown should:

- assess the security risks associated with such a decision
- specify in the systems' SSP the processes and conditions for their application.

Securing volatile media for storage

Control: 0163; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies securing volatile media for ICT equipment during non-operational hours should:

- remove power from the equipment the media resides in
- assess the security risks if not sanitising the media
- specify in the systems' SSP any additional processes and controls that will be applied.

Encrypting media in ICT equipment

Control: 1056; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies encrypt media in ICT equipment with at least a DACA.

Rationale

Accounting for ICT equipment

Ensuring ICT equipment containing media is accounted for by using asset registers and regular audits will assist in preventing theft or alerting appropriate authorities if theft occurs.

Physical security for facilities containing ICT equipment

Media used in ICT equipment takes on the classification of the information it processes. Therefore the area in which the media is used needs to be certified to a level appropriate to the classification of the information that is accessible.

Securing ICT equipment during non-operational hours

The *Physical Security Protocol* of the PSPF states that Class C, B or A secure rooms; Class C, B or A security containers; or lockable commercial cabinets can be used to meet physical security requirements for storing ICT equipment containing media. The class of secure room or security container depends on the physical security certification of the surrounding area and the classification of the information.

Securing non-volatile media for storage

Techniques such as preventing the storage of classified information on non-volatile media and scrubbing temporary data at logoff or shutdown may sound secure. However there is no guarantee that they will always work effectively or will not be bypassed due to unexpected circumstances such as a loss of power from a computer being switched off at the power point. Therefore these security risks need to be considered when implementing such a solution.

Securing volatile media for storage

If agencies need to conduct a security risk assessment as part of the procedure for storing ICT equipment containing media during non-operation hours, they should consider security risks such as:

- an attacker gaining access to the ICT equipment immediately after power is removed and accessing the contents of volatile media to recover encryption keys or parts thereof
- extreme environmental conditions causing data to remain in volatile media for extended periods after the removal of power.

Encrypting media in ICT equipment

Current industry best practice is to encrypt all media in ICT equipment. Newer operating systems provide this functionality and older operating systems can be made to provide it through the use of open source applications.

References

Nil.

Tamper Evident Seals

Objective

Tamper evident seals and associated auditing processes identify attempts to bypass the security of systems and their infrastructure.

Context

Scope

This section describes tamper evident seals on assets.

Controls

Recording seal usage

Control: 0174; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Agencies should record the usage of seals in a register that is appropriately secured.

Control: 0175; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Agencies should record in a register information on:

- issue and usage details of seals and associated tools
- serial numbers of all seals purchased
- the location or asset on which each seal is used.

Control: 0176; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: must
Agencies must record the usage of seals in a register that is appropriately secured.

Control: 0177; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must
Agencies must record in a register information on:

- issue and usage details of seals and associated tools
- serial numbers of all seals purchased
- the location or asset on which each seal is used.

Purchasing seals

Control: 0178; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should consult with the seal manufacturer to ensure that, if available, any purchased seals and sealing tools display a unique identifier or image appropriate to the agency.

Control: 0179; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow contractors to independently purchase seals and associated tools on behalf of the government.

Reviewing seal usage

Control: 0180; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should review seals for differences with a register at least annually.

Rationale

Recording seal usage

Keeping a register of seals and which assets they are used on helps reduce the risk of seals being replaced without the knowledge of security personnel.

Purchasing seals

Using uniquely numbered seals ensures a seal can be uniquely mapped to an asset. This helps security personnel reduce the risk of seals being replaced without anyone being aware of it.

Reviewing seal usage

Users of assets with seals should be encouraged to randomly check the integrity of the seals and to report any concerns to security personnel. In addition, conducting reviews at least annually will allow detection of any tampering to an asset and ensure that the correct seal is located on the correct asset.

References

The SCEC endorses seals to be used for various sealing requirements. Further information on endorsed seals is available in the *Security Equipment Catalogue* produced by SCEC.

Personnel Security

Personnel Security for Systems

Information Security Awareness and Training

Objective

A security culture is fostered through continual security education tailored to roles and responsibilities.

Context

Scope

This section describes the training that should be provided to personnel on information security issues.

Controls

Information security awareness and training

Control: 0252; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must provide ongoing information security awareness and training for personnel on information security policies including topics such as responsibilities, consequences of non-compliance, and potential security risks and counter-measures.

Information security awareness and training responsibility

Control: 0251; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure all personnel who have access to a system have sufficient information security awareness and training.

Degree and content of information security awareness and training

Control: 0253; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should align the exact degree and content of information security awareness and training to system user responsibilities.

Control: 0922; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies ensure information security awareness and training includes:

- the purpose of the training or awareness program
- security appointments and contacts
- the legitimate use of system accounts, software and information
- the security of accounts, including shared passwords
- authorisation requirements for applications, databases and data
- the security risks associated with non-agency systems, particularly the Internet
- reporting any suspected compromises or anomalies
- reporting requirements for cyber security incidents, suspected compromises or anomalies
- classifying, marking, controlling, storing and sanitising media
- protecting workstations from unauthorised access
- informing the support section when access to a system is no longer needed
- observing rules and regulations governing the secure operation and authorised use of systems.

Control: 0255; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure information security awareness and training includes advice to system users not to attempt to:

- physically damage the system
- bypass, strain or test security measures
- introduce or use unauthorised ICT equipment or software on a system
- assume the roles and privileges of others
- attempt to gain access to information for which they have no authorisation
- relocate ICT equipment without proper authorisation.

System familiarisation training

Control: 0256; Revision: 1; Updated: Sep-09; Applicability: TS; Compliance: must
Agencies must provide all system users with familiarisation training on the information security policies and procedures and the secure operation of the system before being granted unsupervised access to the system.

Disclosure of information while on courses

Control: 0257; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should advise personnel attending courses along with non-government personnel not to disclose any details that could be used to compromise security.

Rationale

Information security awareness and training

Information security awareness and training programs are designed to help system users:

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

Information security awareness and training responsibility

Agencies are responsible for ensuring an appropriate information security awareness and training program is provided to personnel. Without management support, security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

Personnel will naturally lose awareness or forget training over time. Providing ongoing information security awareness and training helps keep personnel aware of issues and their responsibilities.

Methods that can be used to continually promote awareness include logon banners, system access forms and departmental bulletins or memoranda.

Degree and content of information security awareness and training

The exact degree and content of information security awareness and training depends on the objectives of the organisation. Personnel with responsibilities beyond that of a general user should have tailored training to meet their needs.

Guidance provided to system users should include sufficient emphasis on activities that are not allowed on systems. The minimum list of content given in the control ensures that personnel are sufficiently exposed to issues that, if they are ignorant of them, could cause a cyber security incident.

System familiarisation training

A TOP SECRET system needs increased awareness by personnel. Ensuring familiarisation with information security policies and procedures, the secure operation of the system and basic information security training, provides personnel with specific knowledge relating to these types of systems.

Disclosure of information while on courses

Government personnel attending courses with non-government personnel may not be aware of the consequences of disclosing information relating to the security of their systems. Raising awareness of such consequences should prevent any disclosure that could lead to a targeted attack being launched against their systems.

References

Nil.

Authorisations, Security Clearances and Briefings

Objective

Only appropriately authorised, cleared and briefed personnel are allowed access to systems.

Context

Scope

This section describes the authorisations, security clearances and briefings required by personnel to access systems. Information on the technical implementation of access controls for systems can be found in the *System Access* section of the *Access Control* chapter.

Security clearances – Australian and foreign

Where this manual refers to security clearances, the reference applies to Australian security clearances or security clearances from a foreign government which is recognised by Australia under a security of information arrangement.

Controls

Documenting authorisations, security clearance and briefing requirements

Control: 0432; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must specify in the SSP any authorisations, security clearances and briefings necessary for system access.

Authorisation and system access

Control: 0404; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should

Agencies should:

- limit system access on a need-to-know basis
- have any requests for access to a system by personnel authorised by their supervisor or manager
- provide system users with the least amount of privileges needed to undertake their duties
- have system access and privileges reassessed at regular intervals by the supervisor or manager of the system user, including when a change of duties occurs, and remove system access or privileges if necessary.

Control: 0405; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must:

- limit system access on a need-to-know basis
- have any requests for access to a system by personnel authorised by their supervisor or manager
- provide system users with the least amount of privileges needed to undertake their duties
- have system access and privileges reassessed at regular intervals by the supervisor or manager of the system user, including when a change of duties occurs, and remove system access or privileges if necessary.

Recording authorisation for personnel to access systems

Control: 0407; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should:

- maintain a secure record of:
  - all authorised system users
  - their user identification
  - who provided the authorisation to access the system
  - when the authorisation was granted
- maintain the record for the life of the system to which access is granted.

Security clearance for system access

Control: 0434; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

All system users must either:

- hold a security clearance at least equal to the system classification
- have been granted access in accordance with the requirements in this manual for limited higher access or emergency access.

System access briefings

Control: 0435; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

All system users must have received any necessary briefings before being granted access to a system.

Access by foreign nationals to AUSTEO systems

Control: 0409; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not allow foreign nationals, including seconded foreign nationals, to have access to systems that process, store or communicate AUSTEO information unless effective controls and procedures are in place to ensure AUSTEO information is not passed to, or made accessible by, foreign nationals, including seconded foreign nationals.

Access by foreign nationals to AGAO systems

Control: 0411; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not allow foreign nationals, excluding seconded foreign nationals, to have access to systems that process, store or communicate AGAO information unless effective controls and procedures are in place to ensure AGAO information is not passed to, or made accessible by, foreign nationals, excluding seconded foreign nationals.

Access by foreign nationals to Australian systems

Control: 0816; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not

Where systems process, store or communicate information with nationality releasability markings, agencies must not allow foreign nationals, including seconded foreign nationals, to have access to such information that is not marked as releasable to their nation.

Granting limited higher access

Control: 0440; Revision: 2; Updated: Nov-10; Applicability: R/P, C, S/HP, TS; Compliance: must

Agencies granting limited higher access to a system must ensure:

- the requirement to grant limited higher access is temporary in nature and is an exception rather than the norm
- an ITSM has approved the limited higher access
- a cessation date for limited higher access has been set
- the access period does not exceed two months
- the limited higher access is granted on a non-ongoing basis
- the system user only accesses information at one security clearance level higher than currently held
- the system user is not granted privileged access to the system
- the system user's access is formally documented
- the system user's access is reported to the CISO.

Controlling limited higher access

Control: 0441; Revision: 2; Updated: Nov-10; Applicability: R/P, C, S/HP, TS; Compliance: must

Agencies granting limited higher access to a system must ensure that either:

- effective controls are in place to restrict access to only information that is necessary to undertake the system user's duties
- the system user is continually supervised by another system user who has the appropriate security clearances to access the system.

Granting emergency access

Control: 0442; Revision: 2; Updated: Nov-10; Applicability: R/P, C, S/HP, TS; Compliance: must

Agencies granting emergency access to a system must ensure:

- the requirement to grant emergency access is due to an immediate and critical need to access information
- the agency head or their delegate has approved the emergency access
- the system user's access is formally documented
- the system user's access is reported to the CISO
- the security clearance process is completed as soon as possible.

Accessing systems without necessary security clearances and briefings

Control: 0443; Revision: 1; Updated: Sep-09; Applicability: R/P, C, S/HP, TS; Compliance: must not

Agencies must not grant limited higher access or emergency access to systems that process, store or communicate caveated or compartmented information.

Rationale

Documenting security clearance and briefing requirements

Ensuring the requirements for access to a system are documented and agreed upon helps determine if system users have appropriate authorisations, security clearances and need-to-know to access the system.

Types of system users for which access requirements need to be documented include general users, privileged users, contractors and visitors.

Authorisation and system access

Personnel seeking access to a system need to have a genuine business requirement to access the system as verified by their supervisor or manager. Once a requirement to access a system is established the system user should only be given the privileges they need to undertake their duties. Providing all system users with privileged access when there is no requirement for privileged access can cause significant vulnerabilities in a system.

Recording authorisation for personnel to access systems

In many cases the requirement to maintain a secure record of all personnel authorised to access a system, their user identification, who provided the authorisation and when the authorisation was granted, can be met by retaining a completed system account request form signed by the supervisor or manager of the system user.

Security clearance for system access

A security clearance provides assurance that personnel can be trusted with access to classified information that is processed, stored or communicated by a system.

System access briefings

Some systems may contain caveated or compartmented information. There may be unique briefings that system users need before being granted access to such systems.

Access by foreign nationals to AUSTEO systems

AUSTEO information is restricted to Australian nationals.

Access by foreign nationals to AGAO systems

AGAO information is restricted to Australian nationals, with the exception of seconded foreign nationals, who may access such information to undertake their assigned duties.

Access by foreign nationals to Australian systems

When information from foreign nations is entrusted to the Australian Government care needs to be taken to ensure foreign nationals do not have access to such information unless it has also been released to their country.

Granting limited higher access

Under strict circumstances access to systems may be granted to personnel who lack the appropriate security clearance.

Controlling limited higher access

When personnel are granted access to a system under the provisions of limited higher access they need to be closely supervised or have their access controlled such that they only have access to information they require to undertake their duties.

Granting emergency access

Emergency access to a system may be granted where there is an immediate and critical need to access information for which personnel do not have the appropriate security clearances. Such access will need to be granted by the agency head or their delegate and formally documented.

Accessing systems without necessary security clearances and briefings

The ability to grant limited higher access or emergency access to systems processing, storing or communicating caveated or compartmented information is not permitted.

References

The *Physical Security Protocol* of the PSPF contains policy on granting and maintaining security clearances.

Privileged Access

Objective

Only trusted personnel are granted privileged access to systems.

Context

Scope

This section describes personnel who are granted privileged access to systems.

Privileged access

In this section, privileged access is considered to be access which can give a system user one or more of:

- the ability to change key system configurations
- the ability to change control parameters
- access to audit and security monitoring information
- the ability to circumvent security measures
- access to data, files and accounts used by other system users, including backups and media
- special access for troubleshooting the system.

Controls

Use of privileged accounts

Control: 0444; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should

Agencies should:

- ensure the use of privileged accounts is controlled and accountable
- ensure system administrators are assigned an individual account for the performance of their administration tasks
- keep privileged accounts to a minimum
- allow the use of privileged accounts for administrative work only.

Control: 0445; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: must

Agencies must:

- ensure the use of privileged accounts is controlled and accountable
- ensure system administrators are assigned an individual account for the performance of their administration tasks
- keep privileged accounts to a minimum
- allow the use of privileged accounts for administrative work only.

Privileged system access by foreign nationals

Control: 0446; Revision: 1; Updated: Sep-09; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate AUSTEO information.

Control: 0447; Revision: 1; Updated: Sep-09; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not allow foreign nationals, excluding seconded foreign nationals, to have privileged access to systems that process, store or communicate AGAO information.

Control: 0448; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate classified information.

Maintaining system management logs

Control: 0982; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: recommended
It is recommended agencies maintain system management logs for the life of a system.

Control: 0451; Revision: 1; Updated: Nov-10; Applicability: C, S/HP; Compliance: should
Agencies should maintain system management logs for the life of a system.

Control: 0452; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Agencies must maintain system management logs for the life of a system.

Content of system management logs

Control: 0450; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
System management logs should be updated to record the following information:

- system startup and shutdown
- component or system failures
- maintenance activities
- backup and archival activities
- system recovery activities
- special or out of hours activities.

Security clearances for privileged users

Control: 0984; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies involved in frequent transfers of data from another system to their system with a lesser classification clear at least one privileged user to the classification of the higher system.

Rationale

Use of privileged accounts

Inappropriate use of any feature or facility of a system that enables a privileged user to override system or application controls can be a major contributory factor to failures or cyber security incidents on systems.

Privileged access rights allow system-wide changes to be made. An appropriate and effective mechanism to log privileged users will provide greater accountability and auditing capability.

Privileged system access by foreign nationals

As privileged users often have the ability to bypass controls on a system it is strongly encouraged that foreign nationals are not given privileged access to systems processing particularly sensitive information.

Maintaining system management logs

Having thorough information on the operations of a system can better assist system administrators in their role, potentially having a positive flow-on effect for the security of the system.

Content of system management logs

The recommended content of system management logs assists in logging key management activities conducted on systems.

Security clearances for privileged users

When frequent data transfers occur between systems of different classifications, having a privileged user from the lesser system cleared to the classification of the higher system will assist in any actions that need to be taken resulting from a data spill from the higher system onto the lesser system.

References

Nil.

Using the Internet

Objective

Personnel use Internet services in a responsible and security conscience manner.

Context

Scope

This section describes responsibilities of personnel using Internet services such as the Web, web-based email and peer-to-peer applications. While this section does not address Internet services such as IM, IRC, IP telephony and video conferencing, agencies need to be aware that unless applications using these communications methods are evaluated and approved by DSD they are not approved for communicating classified information over the Internet.

Additional information on using applications that can be used with the Internet can be found in the *Web Applications* and *Email Applications* sections of the *Software Security* chapter.

Controls

Using the Internet

Control: 0817; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure personnel are instructed to report any suspicious contact when using the Internet to an ITSM.

Awareness of web usage policies

Control: 0818; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must make their system users aware of their web usage policies.

Monitoring web usage

Control: 0819; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should implement measures to monitor their personnel's compliance with their web usage policies.

Posting information on websites

Control: 0820; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure personnel are instructed to take special care not to post classified information on public websites.

Control: 1146; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure personnel posting information on websites maintain separate professional accounts from any personal accounts they have for websites.

Control: 1147; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should monitor websites on which personnel post information and, if necessary, remove any inappropriate information.

Posting personal information on websites

Control: 0821; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.

Control: 0924; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Personnel should avoid posting personal information, such as the following, on websites:

- past and present employment details
- personal details
- schools/institutions
- clubs/hobbies
- educational qualifications
- current work duties
- work contact details.

Control: 1148; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Personnel should use privacy settings for websites to restrict access to personal information they post to only those they authorise to view it.

Control: 0923; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that personnel undertake a web search on their name to see what personal information is available and contact an ITSM if they need assistance in determining if the information is appropriate to be viewed by the general public or potential adversaries.

Awareness of email usage policies

Control: 0266; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must make their system users aware of their email usage policies.

Monitoring email usage

Control: 0822; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should implement measures to monitor their personnel's compliance with email usage policies.

Public web-based email services

Control: 0267; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow personnel to send and receive emails using public web-based email services.

Peer-to-peer applications

Control: 0823; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow personnel to use peer-to-peer applications over the Internet.

Receiving files via the Internet

Control: 0824; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow personnel to receive files via peer-to-peer, IM or IRC applications.

Rationale

Using the Internet

Agencies need to determine what constitutes suspicious contact in their own work environment. Suspicious contact may relate to the work duties of personnel or the specifics of projects being undertaken by personnel.

Awareness of web usage policies

There is little value in having web usage policies for system users if they are not made aware of their existence.

Monitoring web usage

Agencies may choose to monitor breaches of web usage policies—for example attempts to access blocked websites such as pornographic and gambling websites—as well as compiling a list of system users who excessively download or upload data without a legitimate business requirement.

Posting information on websites

Personnel need to take special care not to accidentally post classified information on public websites, especially in forums and blogs. Even unclassified information that appears to be benign in isolation could, along with other information, have a considerable security impact on the government.

To ensure personal opinions of personnel are not interpreted as official policy, personnel will need to maintain separate professional and personal accounts when using websites, especially when using online social networks.

Posting personal information on websites

Personnel need to be aware that any personal information they post on websites could be used to develop a detailed profile of their lifestyle and hobbies in order to attempt to build a trust relationship with them or others. This relationship could then be used to attempt to elicit government information from them or implant malicious software on systems by inducing them to, for example, open emails or visit websites with malicious content.

Awareness of email usage policies

There is little value in having email usage policies for system users if they are not made aware of their existence.

Monitoring email usage

Agencies may choose to monitor breaches of email usage policies—for example, attempts to send prohibited file types or executables, attempts to send excessively sized attachments or attempts to send classified information without appropriate protective markings.

Public web-based email services

Using public web-based email services allows personnel to bypass security measures that agencies will have put in place to protect against malicious code or phishing attempts distributed via email.

Peer-to-peer applications

Personnel using peer-to-peer file sharing applications are often unaware of the extent of files that are being shared from their workstation. In most cases peer-to-peer file sharing applications will scan workstations for common file types and share them automatically for public consumption. Examples of peer-to-peer file sharing applications include Shareaza, KaZaA, Limewire, eMule and uTorrent.

Some peer-to-peer IP telephony applications, such as Skype, use proprietary protocols and make heavy use of encrypted tunnels to bypass firewalls. Because of this their use cannot be regulated or monitored. It is important that agencies implementing an IP telephony solution over the Internet choose applications that use protocols that are open to inspection by intrusion detection systems.

Receiving files via the Internet

When personnel receive files via peer-to-peer file sharing, IM or IRC applications they are often by passing security measures put in place to detect and quarantine malicious code. Personnel should be encouraged to send files via established methods such as email to ensure they are appropriately scanned for malicious code.

References

Nil.

Escorting Uncleared Personnel

Objective

Uncleared personnel are escorted in secured areas.

Context

Scope

This section describes the escorting of uncleared personnel in secured spaces.

Controls

Unescorted access

Control: 0166; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must ensure all personnel with unescorted access to TOP SECRET areas have appropriate security clearances and briefings.

Maintaining an unescorted access list

Control: 0167; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must maintain a current unescorted access list listing all personnel entitled to enter a TOP SECRET area without an escort.

Displaying the unescorted access list

Control: 0168; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: should

Agencies should display unescorted access lists in TOP SECRET areas.

Recording visits in a visitor log

Control: 0169; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not

Agencies must not permit personnel not on the unescorted access list to enter a TOP SECRET area unless their visit is recorded in a visitor log and they are escorted by a person on the unescorted access list.

Content of the visitor log

Control: 0170; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must, at minimum, record the following information in a visitor log for each entry:

- name
- organisation
- person visiting
- contact details for person visiting
- date and time in and out.

Separate visitor logs

Control: 0171; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies with a TOP SECRET area in a larger facility must maintain a separate log from any general visitor log.

Rationale

Unescorted access

It is widely considered a standard security practice to ensure personnel have correct security clearances to access sensitive areas and that access by escorted personnel is recorded for auditing purposes.

Maintaining an unescorted access list

Maintaining an unescorted access list reduces the administrative overhead of determining if personnel can enter a TOP SECRET area without an escort.

Displaying the unescorted access list

Displaying an unescorted access list allows people to quickly verify if personnel are entitled to be in a TOP SECRET area without an escort.

Recording visits in a visitor log

Recording visitors to a TOP SECRET area ensures there is a record of visitors should an investigation into an incident need to take place in the future.

Contents of the visitor log

The contents of the visitor log ensures security personnel have sufficient details to conduct an investigation into an incident should they need to.

Separate visitor logs

Maintaining a separate visitor log for TOP SECRET areas assists in enforcing the need-to-know principle. General visitors do not have a need-to-know about details of personnel who have visited TOP SECRET areas.

References

Nil.

Communications Security

Communications Infrastructure

Cable Management Fundamentals

Objective

Cable management systems are implemented to allow easy integration of systems across government.

Context

Scope

This section describes cable distribution systems used in facilities in Australia. When designing cable management systems, the *Cable Labelling and Registration*, and *Cable Patching* sections of this chapter also apply.

Applicability of controls in this section

The controls in this section are applicable to all facilities. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Common implementation scenarios

This section provides common requirements for non-shared government facilities, shared government facilities and shared non-government facilities. Further specific requirements for each scenario can be found in the other sections of this chapter.

TOP SECRET cabling

For TOP SECRET cabling the cable's protective sheath is not considered to be a conduit. For TOP SECRET fibre optic cables with subunits, the cable's outer protective sheath is considered to be a conduit.

Controls

Cabling standards

Control: 0181; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must install all cabling in accordance with the relevant Australian standards as directed by the Australian Communications and Media Authority.

Cable colours

Control: 0926; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: recommended

It is recommended agencies comply with the cable colours specified in the following table.

CLASSIFICATION	CABLE COLOUR
SECRET/HIGHLY PROTECTED	Pink
CONFIDENTIAL	Green
RESTRICTED/PROTECTED	Blue
IN-CONFIDENCE	Blue
UNCLASSIFIED	Black or grey

Control: 0186; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
In TOP SECRET areas, agencies must comply with the cable colours specified in the following table.

CLASSIFICATION	CABLE COLOUR
TOP SECRET	Red
SECRET/HIGHLY PROTECTED	Pink
CONFIDENTIAL	Green
RESTRICTED/PROTECTED	Blue
IN-CONFIDENCE	Blue
UNCLASSIFIED	Black or grey

Cable colours for foreign systems in Australian facilities

Control: 0825; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP; Compliance: should not
Agencies should not allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

Control: 0826; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP; Compliance: should
The cable colour to be used for foreign systems should be agreed between the host agency, the foreign system owner and the accreditation authority.

Control: 0827; Revision: 0; Updated: Sep-09; Applicability: TS; Compliance: must not
Agencies must not allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

Control: 0828; Revision: 0; Updated: Sep-09; Applicability: TS; Compliance: must
The cable colour to be used for foreign systems must be agreed between the host agency, the foreign system owner and the accreditation authority.

Cable groupings

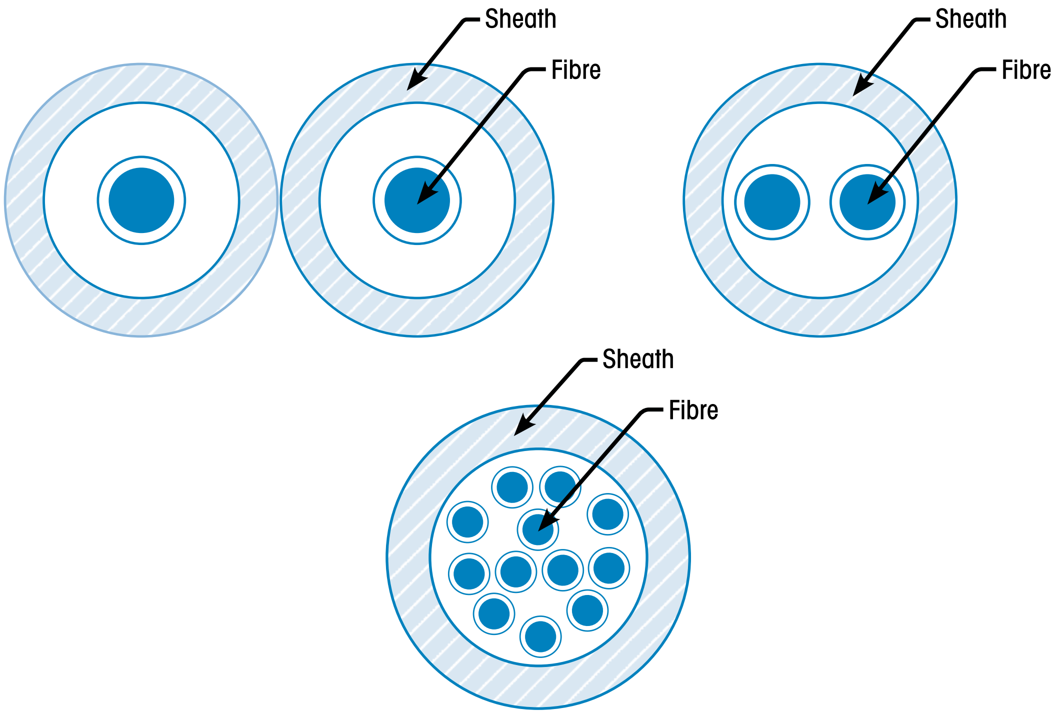
Control: 0187; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not deviate from the approved group combinations for cable classifications as indicated below.

GROUP	APPROVED COMBINATION
1	UNCLASSIFIED
	IN-CONFIDENCE
	RESTRICTED/PROTECTED
2	CONFIDENTIAL
	SECRET/HIGHLY PROTECTED
3	TOP SECRET

Fibre optic cables sharing a common conduit

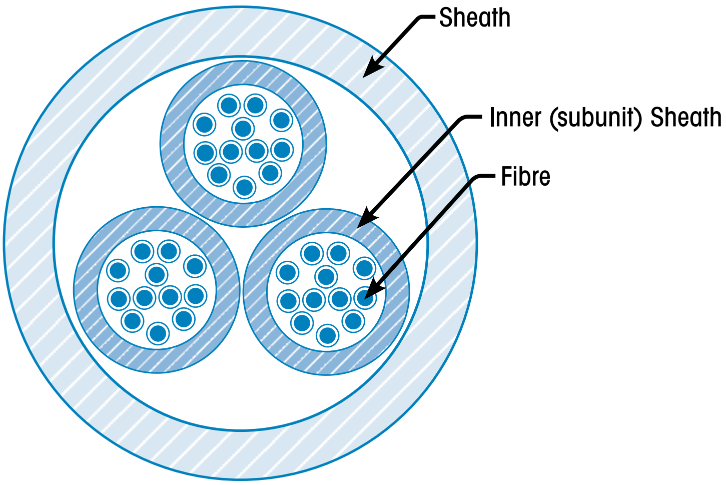
Control: 0189; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

With fibre optic cables the fibres in the sheath, as shown below, must only carry a single group.



Control: 0190; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

If a fibre optic cable contains subunits, as shown below, each subunit must only carry a single group; however, each subunit in the cable can carry a different group.



Terminating cabling in cabinets

Control: 1098; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Cabling should terminate in either:

- individual cabinets
- one cabinet with a division plate to delineate classifications for small systems.

Control: 1099; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: must
In TOP SECRET areas, cabling must terminate in either:

- individual cabinets
- one cabinet with a division plate to delineate classifications for small systems.

Control: 1100; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must
TOP SECRET cabling must terminate in an individual TOP SECRET cabinet.

Connecting cable reticulation systems to cabinets

Control: 1101; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Reticulation systems leading into cabinets in secured communications and server rooms should terminate as close as possible to the cabinet.

Control: 1102; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Reticulation systems leading into cabinets not in a secure communications or server room should terminate as close as possible to the cabinet.

Control: 1103; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
In TOP SECRET areas, reticulation systems leading into cabinets not in a secure communications or server room must terminate at the boundary of the cabinet.

Audio secure spaces

Control: 0198; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
When penetrating an audio secured space agencies must consult with ASIO and comply with all directions provided.

Wall outlet terminations

Control: 1104; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: must
Cable groups sharing a wall outlet must:

- use fibre optic cabling
- use different connectors on opposite sides of the wall outlet for each group.

Control: 1105; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must not
TOP SECRET cabling must not share a wall outlet with another classification.

Control: 1106; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must
In areas containing outlets for both TOP SECRET systems and systems of other classifications, agencies must ensure that the connectors for the TOP SECRET systems are different to those of the other systems.

Wall outlet colours

Control: 1107; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: must not
Wall outlets must not be coloured red.

Control: 1108; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must
In TOP SECRET areas, wall outlets must be coloured red.

Wall outlet covers

Control: 1109; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Faceplates on wall outlets should be clear plastic.

Control: 1110; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
In TOP SECRET areas, faceplates on wall outlets must be clear plastic.

Rationale

Cabling standards

Unauthorised personnel could inadvertently or deliberately access system cabling. This could result in loss or compromise of information. Non-detection of covert tampering or access to system cabling may result in long term unauthorised access to information by a hostile entity.

Cable colours

The use of defined cable colours provides an easily recognisable cable management system.

Cable colours for foreign systems in Australian facilities

Different cable colours for foreign systems in Australian facilities helps prevent unintended patching of Australian and foreign systems together.

Cable groupings

Grouping cables provides a method of sharing conduits and cable reticulation systems in the most efficient manner.

Fibre optic cables sharing a common conduit

Fibre optic cables of various cable groups can share a common conduit to reduce installation costs.

Terminating cabling in cabinets

Having individual or divided cabinets for each classification prevents accidental or deliberate cross patching and makes visual inspection of cabling and patching easier.

Connecting cable reticulation systems to cabinets

Strictly controlling the routing from cable management systems to cabinets prevents unauthorised modifications and tampering and provides easy inspection of cabling.

Audio secure spaces

Audio secure spaces are strictly designed to prevent audio conversation from being heard outside the walls. Penetrating an audio secure space in an unapproved manner can degrade this. Consultation with ASIO needs to be undertaken before any modifications are done to audio secure spaces.

Wall outlet terminations

Wall outlet boxes are the main method of connecting cable infrastructure to workstations. They allow the management of cabling and the type of connectors allocated to various classifications.

Wall outlet colours

The colouring of wall outlets makes it easy to identify TOP SECRET infrastructure.

Wall outlet covers

Transparent covers on wall outlets allows for inspection of cabling for cross patching and tampering.

References

Australian Standards for cabling can be obtained from the Australian Communications and Media Authority at www.acma.gov.au/WEB/STANDARD/pc=PC_2459.

Cable Management for Non-Shared Government Facilities

Objective

Cable management systems are implemented in non-shared government facilities.

Context

Scope

This section describes cabling installed in facilities where the entire facility and personnel are cleared to the highest classification of information processed in the facility. This section is to be applied in addition to common requirements for cabling as outlined in the *Cable Management Fundamentals* section of this chapter.

Applicability of controls in this section

The controls in this section are applicable to all facilities that process classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre optic cabling

Control: 1111; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use fibre optic cabling.

Cabling inspectability

Control: 1112; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: recommended
It is recommended cabling be inspectable at a minimum of five-metre intervals.

Control: 1113; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
In TOP SECRET areas, cabling should be inspectable at a minimum of five-metre intervals.

Cables sharing a common reticulation system

Control: 1114; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Approved cable groups can share a common reticulation system but should have either a dividing partition or a visible gap between the differing cable groups.

Cabling in walls

Control: 1115; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended flexible or plastic conduit be used in walls to run cabling from cable trays to wall outlets.

Cabinet separation

Control: 1116; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: should
TOP SECRET cabinets should have a visible gap to lower classified cabinets.

Rationale

Use of fibre optic cabling

Fibre optic cabling does not produce, and is not influenced by, electromagnetic emanations, and therefore offers the highest degree of protection from electromagnetic emanation effects.

Fibre cabling is more difficult to tap than copper cabling.
Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre cable is the best method to future proof cabling infrastructure—it protects against unforseen threats and facilitates upgrading secure cabling to higher classifications in the future.

Cabling inspectability
Regular inspections of cable installations are necessary to detect any illicit tampering or degradation.

Cables sharing a common reticulation system
Laying cabling in a neat and controlled manner that allows for inspections reduces the need for individual cable trays for each classification.

Cabling in walls
Cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements.

Cabinet separation
Having a definite gap between cabinets allows for ease of inspections for any illicit cabling or cross patching.

References

Nil.

Cable Management for Shared Government Facilities

Objective

Cable management systems are implemented in shared government facilities.

Context

Scope

This section describes cabling installed in facilities where the facility and personnel are cleared at different classification levels. This section is to be applied in addition to common requirements for cabling as outlined in the *Cable Management Fundamentals* section of this chapter.

Applicability of controls in this section

The controls in this section are applicable to all facilities that process classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre optic cabling

Control: 1117; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use fibre optic cabling.

Cabling inspectability

Control: 1118; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: should
Cabling should be inspectable at a minimum of five-metre intervals.

Control: 1119; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
In TOP SECRET areas, cables should be fully inspectable for their entire length.

Cables sharing a common reticulation system

Control: 1120; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Approved cable groups can share a common reticulation system but should have either a dividing partition or a visible gap between the individual cable groups.

Cabling in walls

Control: 1121; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Cabling from cable trays to wall outlets should run in flexible or plastic conduit.

Wall penetrations

Control: 1122; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: should
For wall penetrations that exit into a lower classified space, cabling should be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

Control: 1123; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: should
TOP SECRET facilities should have a power distribution board located in the TOP SECRET area with a feed from a UPS to power all ICT equipment.

Cabinet separation

Control: 1124; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: should
TOP SECRET cabinets should have a visible gap to lower classified cabinets.

Rationale

Use of fibre optic cabling

Fibre optic cabling does not produce, and is not influenced by, electromagnetic emanations, and therefore offers the highest degree of protection from electromagnetic emanation effects.

Fibre cabling is more difficult to tap than copper cabling.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre cable is the best method to future proof cabling infrastructure—it protects against unforseen threats and facilitates upgrading secure cabling to higher classifications in the future.

Cabling inspectability

In a shared government facility it is important that cabling systems be inspected for illicit tampering and damage on a regular basis and they have tighter controls than in a non-shared government facility.

Cables sharing a common reticulation system

In a shared government facility, tighter controls are placed on sharing reticulations systems.

Cabling in walls

In a shared government facility, cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements. Controls are slightly more stringent than in a non-shared government facility.

Wall penetrations

Penetrating a wall to a lesser-classified space by cabling requires the integrity of the classified space to be maintained. All cabling is encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure space.

Power reticulation

In a shared government facility with lesser-classified systems, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cabling or cross patching.

References

Nil.

Cable Management for Shared Non-Government Facilities

Objective

Cable management systems are implemented in shared non-government facilities.

Context

Scope

This section describes cabling installed in facilities shared by agencies and non-government organisations. This section is to be applied in addition to common requirements for cabling as outlined in the *Cable Management Fundamentals* section of this chapter.

Applicability of controls in this section

The controls in this section are applicable to all facilities that process classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre optic cabling

Control: 1125; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: should
Agencies should use fibre optic cabling.

Control: 0182; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
In TOP SECRET areas, agencies must use fibre optic cabling.

Cabling inspectability

Control: 1126; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: should
Cabling should be inspectable at a minimum of five-metre intervals.

Control: 0184; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
In TOP SECRET areas, cables must be fully inspectable for their entire length.

Cables sharing a common reticulation system

Control: 1127; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: should
Approved cable groups can share a common reticulation system but should have either a dividing partition or a visible gap between the differing cable groups.

Control: 1128; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: must
In TOP SECRET areas, approved cable groups can share a common reticulation system but must have either a dividing partition or a visible gap between the differing cable groups.

Control: 1129; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must
TOP SECRET cabling must run in a non-shared, enclosed reticulation system.

Enclosed cable reticulation systems

Control: 1130; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: should
Cables should be run in an enclosed cable reticulation system where the front covers of conduits, ducts and cable trays in floors, ceiling and of associated fittings should be clear plastic.

Control: 1131; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
In TOP SECRET areas, cables must be run in an enclosed cable reticulation system where the front covers of conduits, ducts and cable trays in floors, ceiling and of associated fittings must be clear plastic.

Cabling in walls

Control: 1132; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Cabling from cable trays to wall outlets must run in flexible or plastic conduit.

Cabling in party walls

Control: 1133; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must not

Cabling must not run in a party wall.

Sealing conduits

Control: 0194; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must use a visible smear of conduit glue to seal:

- all plastic conduit joints
- conduit runs connected by threaded lock nuts.

Sealing reticulation systems

Control: 0195; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must use SCEC endorsed tamper evident seals to seal all removable covers on reticulation systems, including:

- conduit inspection boxes
- outlet and junction boxes
- T-pieces.

Sealing reticulation systems

Control: 0196; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must

Tamper evident seals must be uniquely identifiable.

Wall penetrations

Control: 1134; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must

For wall penetrations that exit into a lower classified space, cabling must be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

Control: 1135; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must

TOP SECRET facilities must have a power distribution board located in the TOP SECRET area with a feed from a UPS to power all ICT equipment.

Cabinet separation

Control: 1136; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must

TOP SECRET cabinets must have a visible gap to lower classified cabinets.

Rationale

Use of fibre optic cabling

Fibre optic cabling is essential in a shared non-government facility. Fibre optic cabling does not produce, and is not influenced by, electromagnetic emanations, and therefore offers the highest degree of protection from electromagnetic emanation effects.

Fibre cabling is more difficult to tap than copper cabling.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre cable is the best method to future proof cabling infrastructure—it protects against unforseen threats and facilitates upgrading secure cabling to higher classifications in the future.

Cabling inspectability

In a shared non-government facility it is imperative that cabling systems be inspected for illicit tampering and damage on a regular basis and that they have tighter controls where the threats are closer and unknown.

Cables sharing a common reticulation system

In a shared non-government facility, tighter controls are placed on sharing reticulation systems as the threats to tampering and damage are increased.

Enclosed cable reticulation systems

In a shared non-government facility, TOP SECRET cabling is enclosed in a sealed reticulation system to prevent access and control cable management.

Cabling in walls

In a shared non-government facility, cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements. Controls are more stringent than in a non-shared government facility or a shared government facility.

Cabling in party walls

In a shared non-government facility, cabling is not allowed in a party wall. A party wall is a wall shared with an unsecured space where there is no control over access. An inner wall can be used to run cabling where the space is sufficient for inspection of the cabling.

Sealing conduits

In a shared non-government facility, where the threat of access to cabling is increased, all conducts are sealed with a visible smear of glue to prevent access to cabling.

Sealing reticulation systems

In a shared non-government facility, where the threats of access to cable reticulation systems is increased, SCEC endorsed seals are required to provide evidence of any tampering or illicit access.

Wall penetrations

Penetrating a wall to a lesser-classified space by cabling requires the integrity of the classified space be maintained. All cabling is encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure space.

Power reticulation

In a shared non-government facility, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means. The addition of a UPS is required to maintain availability of the TOP SECRET systems.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cabling or cross patching.

References

Nil.

Cable Labelling and Registration

Objective

Cable registers are used to record cables and labels.

Context

Scope

This section describes the labelling of cabling infrastructure installed in secured spaces.

Applicability of controls in this section

The controls in this section are applicable to all facilities that process classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Conduit label specifications

Control: 0201; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Labels for TOP SECRET conduits must be:

- a minimum size of 2.5cm x 1cm
- attached at 5m intervals
- marked as 'TS RUN'.

Control: 0202; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Conduit labels in areas where uncleared personnel could frequently visit must have red text on a clear background.

Control: 0203; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Conduit labels in areas that are not clearly observable must have red text on a white background.

Installing conduit labelling

Control: 0204; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Conduit labels installed in public or visitor areas should not draw undue attention from people who do not have a need-to-know of the existence of such cabling.

Labelling wall outlet boxes

Control: 1095; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Wall outlet boxes should denote the classification, cable number and outlet number.

Control: 0205; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Wall outlet boxes must denote the classification, cable number and outlet number.

Standard operating procedures

Control: 0206; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The SOPs should record the site conventions for labelling and registration.

Labelling cables

Control: 1096; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Agencies should label cables at each end, with sufficient source and destination details to enable the physical identification and inspection of the cable.

Control: 0207; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Agencies must label cables at each end, with sufficient source and destination details to enable the physical identification and inspection of the cable.

Cable register

Control: 0208; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Agencies should maintain a register of cables.

Control: 0210; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Agencies must maintain a register of cables.

Cable register contents

Control: 0209; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
The cable register should record at least the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers if applicable.

Control: 1097; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
For cables in TOP SECRET areas, the cable register must record at least the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers if applicable.

Cable inspections

Control: 0211; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should inspect cables for inconsistencies with the cable register in accordance with the frequency defined in the SSP.

Rationale

Conduit label specifications

Conduit labelling of a specific size and colour is required to easily identify secure conduits carrying cables.

Installing conduit labelling

Conduit labelling in public or reception areas could draw undue attention to the level of classified processing and lead to a disclosure of capabilities.

Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching ICT equipment of a lesser classification to the wrong outlet.

Standard operating procedures

Recording labelling conventions in SOPs makes cabling and fault finding easier.

Labelling cables

Labelling cables with the correct source and destination information minimises the likelihood of cross patch and aids in fault finding and configuration management.

Cable register

Cable registers provide a source of information that assessors can view to verify compliance.

Cable register contents

Cable registers allow installers and assessors to trace cabling for inspections, malice or accidental damage. It tracks all cable management changes through the life of the system.

Cable inspections

Cable inspections, at pre-defined periods, are a method of checking the cable management system with the cable register.

References

Nil.

Cable Patching

Objective

Communications systems are designed to prevent patching between different classifications.

Context

Scope

This section describes the configuration and installation of patch panels, patch cables and fly leads associated with communications systems.

Applicability of controls in this section

The controls in this section are applicable to all facilities that process classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Terminations to patch panels

Control: 0213; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure only approved cable groups terminate on a patch panel.

Patch cable and fly lead connectors

Control: 1093; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should

In areas containing cabling for systems of different classifications, agencies should ensure the connectors for each system are different to those of the other systems; unless the length of the higher classified patch cables is less than the distance between the higher classified patch panel and any patch panel of a lower classification.

Control: 0214; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

In areas containing cabling for both TOP SECRET systems and systems of other classifications, agencies must ensure the connectors for the TOP SECRET systems are different to those of the other systems.

Control: 1094; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should

In areas containing cabling for systems of different classifications, agencies should document the selection of connector types.

Control: 0215; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

In areas containing cabling for both TOP SECRET systems and systems of other classifications, agencies must document the selection of connector types for TOP SECRET systems.

Physical separation of patch panels

Control: 0216; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: should

Agencies should physically separate TOP SECRET and non-TOP SECRET patch panels by installing them in separate cabinets.

Control: 0217; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

Where spatial constraints demand patch panels of a lower classification than TOP SECRET be located in the same cabinet, agencies must:

- provide a physical barrier in the cabinet to separate patch panels
- ensure only personnel cleared to TOP SECRET have access to the cabinet
- obtain approval from the relevant accreditation authority prior to installation.

Fly lead installation

Control: 0218; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: should

Agencies should ensure the fibre optic fly leads used to connect wall outlets to ICT equipment either:

- do not exceed 5m in length
- if they exceed 5m in length:
  - are run in the facility's fixed infrastructure in a protective and easily inspected pathway
  - are clearly labelled at the equipment end with the wall outlet designator
  - are approved by the accreditation authority.

Rationale

Terminations to patch panels

Connecting a system to another system of a lesser classification will result in a data spill. A data spill could result in the following issues:

- inadvertent or deliberate access by non-cleared personnel
- the lesser system not meeting the appropriate requirements to secure the classified information from unauthorised access or tampering.

Patch cable and fly lead connectors

Ensuring cables are equipped with connectors of a different configuration to all other cables prevents inadvertent connection to systems of lower classifications.

Physical separation of patch panels

Appropriate physical separation between a TOP SECRET system and a system of a lesser classification:

- reduces or eliminates the chances of cross patching between the systems
- reduces or eliminates the possibility of unauthorised personnel gaining access to TOP SECRET system elements.

Fly lead installation

Keeping the lengths of fly leads to a minimum prevents clutter around desks, prevents damage to fibre optic cabling and reduces the chance of cross patching and tampering. If lengths become excessive, cabling needs to be treated as infrastructure and run it in conduit or fixed infrastructure such as desk partitioning.

References

Nil.

Emanation Security Threat Assessments

Objective

A valid threat assessment is used to determine the appropriate counter-measures to minimise compromising emanations.

Context

Scope

This section describes emanation security threat assessment advice, so agencies can implement appropriate counter-measures to minimise the loss of classified information through compromising emanations.

This section is only applicable to:

- agencies located outside of Australia
- facilities in Australia that have transmitters
- mobile platforms and deployable assets that process classified information.

Controls

Emanation security threat assessments in Australia

Control: 0247; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies designing and installing systems with RF transmitters inside or co-located with their facility must:

- contact DSD for an emanation security threat assessment in accordance with the latest version of *ACSI 71*
- install cabling and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 0248; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP; Compliance: must

Agencies designing and installing systems with RF transmitters that co-locate with systems of a higher classification must:

- contact DSD for an emanation security threat assessment in accordance with the latest version of *ACSI 71*
- install cabling and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 1137; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies designing and installing systems in shared facilities with non-Australian government entities must:

- contact DSD for an emanation security threat assessment in accordance with the latest version of *ACSI 71*
- install cabling and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Emanation security threat assessments outside Australia

Control: 0932; Revision: 2; Updated: Nov-10; Applicability: IC, R/P; Compliance: recommended

It is recommended that agencies deploying systems overseas:

- contact DSD for emanation security threat advice
- install cabling and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 0249; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies deploying systems overseas in military and fixed locations must:

- contact DSD for an emanation security threat assessment in accordance with the latest version of *ACSI 71*
- install cabling and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Early identification of emanation security issues

Control: 0246; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies needing an emanation security threat assessment should do so as early as possible in project lifecycles as emanation security controls can have significant cost implications.

ICT equipment in highly sensitive areas

Control: 0250; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must
Agencies must ensure that ICT equipment in TOP SECRET areas meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

Rationale

Emanation security threat assessments in Australia

Obtaining the current threat advice from DSD on potential adversaries and applying the appropriate counter-measures is vital in maintaining the confidentiality of classified systems from an emanation security attack.

Failing to implement recommended counter-measures against an emanation security attack can lead to compromise. Having a good cable infrastructure and installation methodology will provide a strong backbone that will not need updating if the threat increases. Infrastructure costs are very expensive and time consuming to retro-fit.

Emanation security threat assessment outside Australia

Fixed sites and deployed military platforms are more vulnerable to emanation security attack and require a current threat assessment and countermeasure implementation. Failing to implement recommended counter-measures and standard operating procedures to reduce threats could result in the platform emanating compromising signals, which if intercepted and analysed, could lead to platform compromise with serious consequences.

Early identification of emanation security issues

It is important to identify the need for emanation security controls for a system early in the project lifecycle as this can reduce costs for the project. Costs are much greater if changes have to be made once the system has been designed and deployed.

ICT equipment in highly sensitive areas

While ICT equipment in a TOP SECRET area in Australia may not need certification to TEMPEST standards, the equipment still needs to meet applicable industry and government standards.

References

Additional information on cabling and separation standards, as well as the potential dangers of operating RF transmitters near systems is documented in the latest version of *ACSI 61.*

Additional information on conducting an emanation security threat assessment is found in the latest version of *ACSI 71*.

Communications Systems and Devices

Radio Frequency and Infrared Devices

Objective

Only approved radio frequency and infrared devices are brought into secured areas.

Context

Scope

This section describes the use of RF and infrared devices in secured spaces. Information on the use of RF devices outside secured spaces can be found in the *Working Off-Site* chapter.

Exemptions for the use of infrared devices

An infrared device can be used in a secured space provided it does not communicate classified information.

Exemptions for the use of RF devices

The following devices, at the discretion of the accreditation authority, can be exempted from the controls associated with RF transmitters:

- pagers that can only receive messages
- garage door openers
- car lock/alarm keypads
- medical and exercise equipment that uses RF to communicate between sub-components
- communications radios that are secured by approved cryptography.

Controls

Pointing devices

Control: 0221; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not

Wireless RF pointing devices must not be used in TOP SECRET areas unless used in a RF screened building.

Infrared keyboards

Control: 0222; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P; Compliance: should

Agencies using infrared keyboards should ensure infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecured space.

Control: 0223; Revision: 2; Updated: Nov-10; Applicability: C, S/HP; Compliance: must not

Agencies using infrared keyboards must not allow:

- line of sight and reflected communications travelling into an unsecured space
- multiple infrared keyboards at different classifications in the same area
- other infrared devices to be brought into line of sight of the keyboard or its receiving device/port
- infrared keyboards to be operated in areas with unprotected windows.

Control: 0224; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not
Agencies using infrared keyboards must not allow:

- line of sight and reflected communications travelling into an unsecured space
- multiple infrared keyboards at different classifications in the same area
- other infrared devices in the same area
- infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.

Bluetooth and wireless keyboards

Control: 1058; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should not
Agencies should not use Bluetooth and wireless keyboards unless in a RF screened building.

Control: 1155; Revision: 0; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must not
Agencies must not use Bluetooth and wireless keyboards unless in a RF screened building.

RF devices in secured spaces

Control: 0830; Revision: 0; Updated: Sep-09; Applicability: C, S/HP; Compliance: should
Agencies should prevent RF devices from being brought into secured spaces unless authorised by the accreditation authority.

Control: 0225; Revision: 1; Updated: Sep-09; Applicability: TS; Compliance: must
Agencies must prevent RF devices from being brought into TOP SECRET areas unless authorised by the accreditation authority.

Detecting RF devices in secured spaces

Control: 0928; Revision: 1; Updated: Nov-10; Applicability: C, S/HP; Compliance: recommended
It is recommended agencies deploy security measures to detect and respond to active RF devices in secured spaces.

Control: 0829; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: should
Agencies should deploy security measures to detect and respond to active RF devices in TOP SECRET areas.

RF controls

Control: 0929; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies limit the effective range of communications outside their area of control by either:

- minimising the output power level of wireless devices
- RF shielding.

Rationale

Pointing devices

Since wireless RF pointing devices can pose an emanation security risk they are not to be used in TOP SECRET areas unless in a RF screened building.

Infrared keyboards

When using infrared keyboards with CONFIDENTIAL or SECRET/HIGHLY PROTECTED systems, drawn opaque curtains are an acceptable method of protecting windows.

When using infrared keyboards with a TOP SECRET system, windows with curtains that can be opened are not acceptable as a method of permanently blocking infrared transmissions.

Bluetooth and wireless keyboards

As the Bluetooth protocol provides little security and wireless keyboards often provide no security they cannot be relied upon to protect information.

RF devices in secured spaces

RF devices pose an audio security threat to secured spaces as they are capable of picking up and transmitting classified background conversations. Furthermore, many RF devices can connect to ICT equipment and act as unauthorised data storage devices.

Detecting RF devices in secured spaces

As RF devices are prohibited in highly classified environments it is encouraged that agencies deploy security measures to detect and respond to the unauthorised use of such devices.

RF controls

Minimising the output power of wireless devices and using RF shielding on facilities will assist in limiting the wireless communications to areas under the control of the agency.

References

Nil.

Fax Machines and Multifunction Devices

Objective

Fax machines and multifunction devices are used in a secure manner.

Context

Scope

This section describes fax machines and MFDs connected to the PSTN, HGCE or computer networks. Further information on MFDs communicating via network gateways can be found in the *Data Import and Export* section of the *Gateway Security* chapter.

Controls

Fax machine and MFD usage policy

Control: 0588; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must develop a policy governing the use of fax machines and MFDs.

Sending fax messages

Control: 1092; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must have separate fax machines or MFDs for sending classified and unclassified fax messages.

Control: 0241; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies sending classified fax messages must ensure the fax message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the public switched telephone network.

Sending fax messages using HGCE

Control: 0242; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: required

Agencies intending to use fax machines or MFDs to send classified information are required to comply with additional requirements in *ACSI 129* and *ACSI 131*.

Receiving fax messages

Control: 1075; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The sender of a fax message should make arrangements for the receiver to:

- collect the fax message as soon as possible after it is received
- notify the sender if the fax message does not arrive in an agreed amount of time.

Connecting MFDs to telephone networks

Control: 0244; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should not

Agencies should not enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.

Control: 0245; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must not

Agencies must not enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.

Connecting MFDs to computer networks

Control: 0590; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies must ensure:

- each MFD applies user identification, authentication and audit functions for all information communicated by that device
- these mechanisms are of similar strength to those specified for workstations on that network
- each gateway can identify and filter the information in accordance with the requirements for the export of data via a gateway.

Copying documents on MFDs

Control: 0589; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not permit MFDs connected to computer networks to be used to copy documents above the classification of the connected network.

Observing fax machine and MFD use

Control: 1036; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure fax machines and MFDs are located in an area where use can be observed.

Rationale

Fax machine and MFD usage policy

As fax machines and MFDs are capable of communicating classified information, and are a potential source of cyber security incidents, it is important that agencies develop a policy governing their use.

Sending fax messages

Once a fax machine or MFD has been connected to cryptographic equipment and used to send a classified fax message it can no longer be trusted when connected directly to unsecured telecommunications infrastructure or the public switched telephone network. For example, if a fax machine fails to send a classified fax message the device will continue attempting to send the fax message even if it has been disconnected from the cryptographic device and connected directly to the public switched telephone network. In such cases the fax machine could then send the classified fax message in the clear causing a cyber security incident.

Sending fax messages using HGCE

Using the correct procedure for sending a classified fax message will ensure that it is sent securely to the correct recipient.

Using the correct memory erase procedure will prevent a classified fax message being communicated in the clear.

Implementing the correct procedure for establishing a secure call will prevent sending a classified fax message in the clear.

Witnessing the receiving of a fax message and powering down the receiving machine or clearing the memory after transmission will prevent someone without a need-to-know accessing the fax message.

Ensuring fax machines and MFDs are not connected to unsecured phone lines will prevent accidentally sending classified messages stored in memory.

Receiving fax messages

While the communications path between fax machines and MFDs may be appropriately protected, personnel need to be aware of the need-to-know of the information that is being communicated. It is therefore important fax messages are collected from the receiving fax machine or MFD as soon as possible. Furthermore, if an expected fax message is not received it may indicate that there was a problem with the original transmission or the fax message has been taken by an unauthorised person.

Connecting MFDs to telephone networks

When a MFD is connected to a computer network and a telephone network the device can act as a bridge between the networks. The telephone network therefore needs to be accredited to the same classification as the computer network the MFD is connected to.

Connecting MFDs to computer networks

As network connected MFDs are considered to be devices that reside on a computer network they need to be able to process the same classification of information that the network is capable of processing.

Copying documents on MFDs

As networked MFDs are capable of sending scanned or copied documents across a connected network, personnel need to be aware that if they scan or copy documents at a classification higher than that of the network the device is connected to they could be causing a data spill onto the connected network.

Observing fax machine and MFD use

Placing fax machines and MFDs in public areas can help reduce the likelihood of any suspicious use of fax machines and MFDs going unnoticed.

References

Specific information regarding the procedures for fax machines and MFDs attached to HGCE is found in *ACSI 129* and *ACSI 131*.

Telephones and Telephone Systems

Objective

Telephone systems are prevented from communicating unauthorised information.

Context

Scope

This section describes the secure use of fixed telephones, including cordless telephones, as well as the systems they use to communicate information. Information regarding mobile phones and smartphones is covered in the *Mobile Devices* section of the *Working Off-Site* chapter while information regarding VoIP and encryption of data in transit is covered in the *Internet Protocol Telephony* section of the *Network Security* chapter and the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Controls

Telephones and telephone systems usage policy

Control: 1078; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must develop a policy governing the use of telephones and telephone systems.

Personnel awareness

Control: 0229; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must advise personnel of the maximum permitted classification for conversations using both internal and external telephone connections.

Control: 0230; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should advise personnel of the audio security risk posed by using telephones in areas where classified conversations can occur.

Visual indication

Control: 0231; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

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.

Use of telephone systems

Control: 0232; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies intending to use telephone systems for the transmission of classified information must ensure:

- the system has been accredited for the purpose
- all classified traffic that passes over external systems is appropriately encrypted.

Cordless telephones

Control: 0233; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not use cordless telephones for classified conversations.

Cordless telephones with secure telephony devices

Control: 0234; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not use cordless telephones in conjunction with secure telephony devices.

Speakerphones

Control: 0235; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not

Agencies must not use speakerphones on telephones in TOP SECRET areas unless:

- it is located in a room rated as audio secure
- the room is audio secure during any conversations
- only personnel involved in discussions are present in the room.

Off-hook audio protection

Control: 0930; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C; Compliance: recommended

It is recommended agencies ensure off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

Control: 0236; Revision: 2; Updated: Nov-10; Applicability: S/HP; Compliance: should

Agencies should ensure off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

Control: 0931; Revision: 2; Updated: Nov-10; Applicability: S/HP; Compliance: recommended

It is recommended agencies use push-to-talk handsets in open areas, and where telephones are shared.

Control: 0237; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must ensure off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

Control: 0238; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: should

Agencies should use push-to-talk handsets to meet the requirement for off-hook audio protection.

Rationale

Telephones and telephone systems usage policy

All non-secure telephone networks are subject to interception. Accidentally or maliciously revealing classified information over a public telephone network can lead to interception.

Personnel awareness

As there is a high risk of unintended disclosure of classified information when using telephones it is important personnel are made aware of what levels of classified information they can discuss on particular telephone systems as well as the audio security risk associated with the use of telephones.

Visual indication

When single telephone systems are approved to hold conversations at different classifications, alerting the user to the classification level they can speak at when using their phone will assist in the reducing the risk of unintended disclosure of classified information.

Use of telephone systems

When classified conversations are to be held using telephone systems the conversation needs to be appropriately protected through the use of encryption measures.

Cordless telephones

Cordless telephones have minimal transmission security, therefore should not be used for classified communications.

Cordless telephones with secure telephony devices

As the data between cordless handsets and base stations is not appropriately secured, cordless telephones must not be used for classified communications even if the device is connected to a secure telephony device.

Speakerphones

As speakerphones are designed to pick up and transmit conversations in the vicinity of the device they must not be used in TOP SECRET areas as the audio security risk is too high. However, if the agency is able to reduce the audio security risk through the use of an audio secure room that is secured during conversations then they may be used.

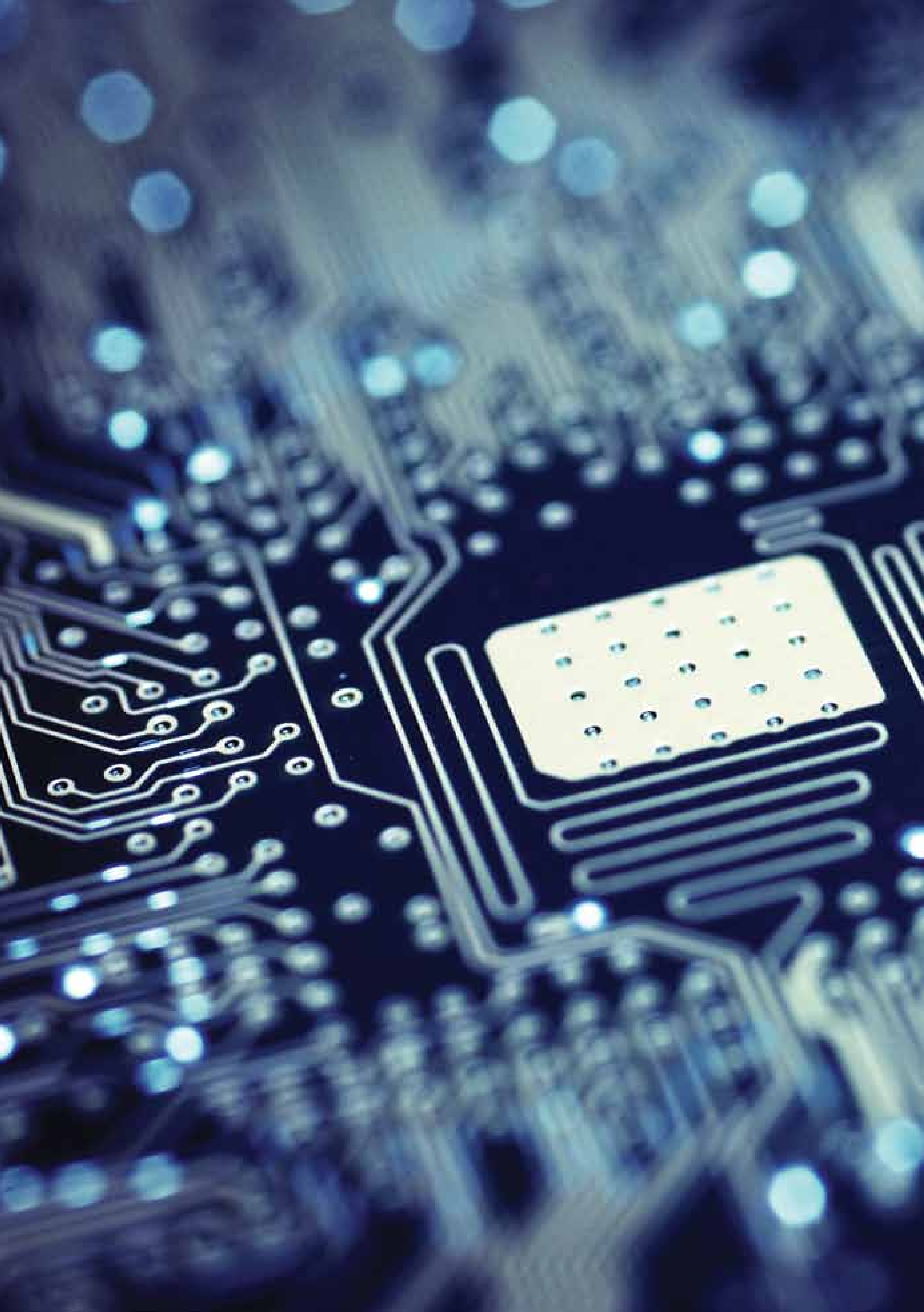
Off-hook audio protection

Providing off-hook security minimises the chance of classified conversation being accidentally coupled into handsets and speakerphones. Limiting the time an active microphone is open limits this threat.

Simply providing an off-hook audio protection feature is not sufficient to meet the requirement for its use. To ensure that the protection feature is used appropriately personnel need to be made aware of the protection feature and trained in its proper use.

References

Nil.



Information Technology Security

Product Security

Product Selection and Acquisition

Objective

Products providing security functions for the protection of information are formally evaluated.

Context

Scope

This section describes selecting and acquiring products that provide security functionality for the protection of information. It does not describe selecting or acquiring products that do not provide security functionality or physical security products.

Selecting products without security functions

Agencies selecting products that do not provide a security function, or selecting products whose security functions will not be used, are free to follow their own acquisition guidelines.

Product specific requirements

Where consumer guides exist for evaluated products, the requirements in the consumer guides take precedence over those in this manual.

Convergence

Convergence is the integration of a number of discrete technologies into one product. Converged solutions can include the advantages and disadvantages of each discrete technology. When products have converged elements, the relevant areas of this manual for each of the discrete elements are applicable.

Evaluated Products List

The EPL consists of products that have been, or are in the process of being, evaluated through one or more of the following schemes:

- Common Criteria
- high assurance evaluation
- another DSD approved evaluation.

The EPL is maintained by DSD and provides a listing of approved products for the protection of information.

Australasian Information Security Evaluation Program

The AISEP exists to ensure that a range of evaluated products are available to meet the needs of the Australian and New Zealand Government.

The AISEP performs the following functions:

- evaluation and certification of products using the Common Criteria
- continued maintenance of the assurance of evaluated products
- recognition of products evaluated by a foreign scheme with which the AISEP has a mutual recognition agreement.

Recognition arrangements

DSD has a number of recognition arrangements regarding evaluated products. Before choosing a product that has not been evaluated by the AISEP or DSD, agencies are encouraged to investigate whether the product will be recognised for Australian use once it has completed an evaluation in a foreign scheme.

Controls

Evaluated product selection preference order

Control: 0280; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must select products in the following order of preference:

- products which have completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement, a high assurance evaluation by DSD, or another DSD approved evaluation
- products in evaluation in the AISEP or DSD
- products in evaluation in a scheme where the outcome will be recognised by DSD when the evaluation is completed; then
- products that have not completed any evaluation.

Control: 0282; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

When choosing a product agencies must document the justification for any decision to choose a product that has not completed an evaluation and accept any security risk introduced by the use of such a product.

Evaluated product selection

Control: 0279; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should select products that have their desired security functionality in the scope of the product's evaluation and are applicable to the intended environment.

Product specific requirements

Control: 0463; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must check consumer guides for products, where available, to determine any product specific requirements.

Control: 0464; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Where product specific requirements exist in a consumer guide, agencies must comply with the requirements outlined in the consumer guide.

Control: 0283; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies selecting high assurance products and HGCE must contact DSD and comply with any product specific requirements.

Sourcing non-evaluated software

Control: 0936; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: recommended

It is recommended agencies:

- obtain software from verifiable sources and verify its integrity using vendor supplied checksums
- validate the software's interaction with the operating systems and network in a test environment prior to use on operational systems.

Control: 0284; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should

Agencies should:

- obtain software from verifiable sources and verify its integrity using vendor supplied checksums
- validate the software's interaction with the operating systems and network in a test environment prior to use on operational systems.

Delivery of evaluated products

Control: 0285; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

Control: 0286; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies procuring high assurance products and HGCE must contact DSD and comply with any product specific delivery procedures.

Delivery of non-evaluated products

Control: 0937; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended 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 that they expect to receive in an unaltered state.

Leasing arrangements

Control: 0287; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that leasing agreements for ICT equipment take into account the:

- difficulties that could be encountered when the equipment needs maintenance
- difficulties that could be encountered in sanitising equipment before returning it
- the possible requirement for destruction if sanitisation cannot be performed.

Ongoing maintenance of assurance

Control: 0938; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies choose products from developers that have made a commitment to the continuing maintenance of the assurance of their product.

Rationale

Evaluated product selection preference order

In selecting products for use, agencies should note that completed evaluations provide greater assurance than products that are still undergoing evaluation or have not completed any evaluation activity. This is reflected in the preference order for selecting security products.

For products that are currently in evaluation, agencies should select those that are undergoing evaluation through AISEP in preference to those being conducted in a recognised foreign scheme. If a major vulnerability is found during the course of an AISEP evaluation, DSD might be able to provide advice on appropriate risk treatment strategies.

Agencies should be aware that while this section provides a product selection preference order, policy stated elsewhere in this manual, or product specific advice from DSD, could override this requirement by specifying more rigorous requirements for particular functions and device use.

Additionally, where a product performs a cryptographic function for the protection of data at rest or in transit, the product will need to complete a DCE before it satisfies the requirement for a product from the EPL.

Evaluated product selection

A product listed on the EPL might not meet security requirements. This could occur for a number of reasons, including that the scope of the evaluation is inappropriate for the intended use or the operational environment differs from that assumed in the evaluation. An agency should therefore ensure that a product is suitable by reviewing all available documentation. In the case of Common Criteria certified products, this documentation includes the security target (the security requirements of an identified target of evaluation), certification report, consumer guide and any caveats contained in the entry on the EPL.

Products that are in evaluation will not have a certification report and may not have a published security target. A draft security target can be obtained from DSD for products that are in evaluation through AISEP. For products that are in evaluation through a foreign scheme, the vendor can be contacted directly for further information.

Product specific requirements

Not all evaluated products may be found suitable for their intended purpose—even those they may pass their Common Criteria evaluation. Typically such products will have cryptographic functionality that is not covered in sufficient depth under the Common Criteria. Where products have specific usage requirements in addition to this manual, or supersede requirements in this manual, they will be outlined in the product's consumer guide.

Sourcing non-evaluated software

Software downloaded from websites on the Internet could contain malicious code or malicious content that is installed along with the legitimate software. Agencies need to confirm the integrity of the software they are installing before deploying it on a system to ensure that no unintended software is installed at the same time.

Delivery of evaluated products

It is important that agencies ensure that the product that is intended for use is the actual product that is received. If the product differs from the evaluated version, then no assurance can be gained from any evaluation that has been performed.

For products that do not have evaluated delivery procedures, it is recommended agencies assess whether the vendor's delivery procedures are sufficient to maintain the integrity of the product.

Other factors to consider when assessing delivery procedures include:

- the intended environment of the product
- the types of attackers that the product will defend against
- the resources of any potential attackers
- the likelihood of an attack
- the importance of maintaining confidentiality of the product purchase
- the importance of ensuring adherence to delivery timeframes.

Delivery procedures can vary greatly from product to product. For most products the standard commercial practice for packaging and delivery could be sufficient for agencies' requirements. More secure delivery procedures can include security measures to detect tampering or masquerading. Some examples of specific security measures include tamper evident seals, cryptographic checksums and signatures, and secure transportation.

Delivery of non-evaluated products

When a non-evaluated product is purchased agencies are still recommended to take the time to determine if the product has arrived in a state that they were expecting it to and that there are no obvious signs of tampering.

Leasing arrangements

Agencies should consider security and policy requirements when entering into a leasing agreement for ICT equipment in order to avoid potential cyber security incidents during maintenance, repairs or disposal processes.

Ongoing maintenance of assurance

Developers that have demonstrated a commitment to ongoing maintenance or evaluations are more likely to be responsive to ensuring that security patches are independently assessed.

A developer's commitment to continuity of assurance can be gauged through the number of evaluations undertaken and whether assurance maintenance has been performed on previous evaluations.

References

Additional information on the EPL, AISEP and the Common Criteria can be found at:

- www.dsd.gov.au/infosec/epl.htm
- www.dsd.gov.au/infosec/aisep.htm
- www.commoncriteriaportal.org
- www.commoncriteriaportal.org/schemes.html.

Product Installation and Configuration

Objective

Evaluated products use evaluated configurations.

Context

Scope

This section describes installing and configuring products providing security functionality. It does not describe installing and configuring general products or physical security products.

Evaluated configuration

A product is considered to be operating in its evaluated configuration if:

- functionality that it uses was in the scope of the evaluation and implemented in the specified manner
- only patches that have been assessed through a formal assurance continuity process have been applied
- the environment complies with assumptions or organisational security policies stated in the product's security target or similar document.

Unevaluated configuration

A product is considered to be operating in an unevaluated configuration when it does not meet the requirements of an evaluated configuration.

Controls

Installation and configuration of evaluated products

Control: 0289; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should install, configure, operate and administer evaluated products in accordance with available documentation resulting from the product's evaluation.

Control: 0290; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that high assurance products and HGCE are installed, configured, operated and administered in accordance with all product specific ACSIs produced by DSD.

Use of evaluated products in unevaluated configurations

Control: 0291; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies wishing to use a product in an unevaluated configuration must undertake a security risk assessment including:

- the necessity of the unevaluated configuration
- testing of the unevaluated configuration
- the environment in which the unevaluated product is to be used.

Control: 0292; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
High assurance products and HGCE must not be used in unevaluated configurations.

Rationale

Installation and configuration of evaluated products

Evaluation of products provides assurance that the product will work as expected in a clearly defined set of constraints. These constraints, defined by the scope of the evaluation, generally specify what security functionality can be used, and how the products are configured and operated.

Using an evaluated product in a manner for which it was not intended could result in the introduction of new threats and vulnerabilities that were not considered by the initial evaluation.

For products evaluated under the Common Criteria, information is available from the developer in the product's installation, generation and startup documentation. Further information is also available in the security target and certification report.

Use of evaluated products in unevaluated configurations

To ensure that a product will still provide the assurance desired when used in a manner for which it was not intended, a security risk assessment must be conducted upon the altered configuration. The further a product deviates from its evaluated configuration, the less assurance can be gained from the evaluation.

Given the potential threat vectors and the value of the information being protected, high assurance products and HGCE must be configured in accordance with DSD's guidelines.

References

Nil.

Product Classifying and Labelling

Objective

ICT equipment is classified and appropriately labelled.

Context

Scope

This section describes classifying and labelling both evaluated and non-evaluated ICT equipment.

Non-essential labels

Non-essential labels are labels other than classification and asset labels.

Controls

Classifying ICT equipment

Control: 0293; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must classify ICT equipment based on the highest classification of information for which the equipment and any associated media in the equipment are approved for processing, storing or communicating.

Labelling ICT equipment

Control: 0294; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must clearly label all ICT equipment capable of storing information, with the exception of HGCE, with the appropriate protective marking.

Labelling high assurance products

Control: 0295; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not have any non-essential labels applied to external surfaces of high assurance products.

Labelling HGCE

Control: 0296; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: required

Agencies are required to seek DSD authorisation before applying labels to external surfaces of HGCE.

Rationale

Classifying ICT equipment

When media is used in ICT equipment there is no guarantee that the equipment has not automatically accessed information from the media and stored it locally, without the knowledge of the system user. The ICT equipment therefore needs to be afforded the same degree of protection as that of the associated media.

Labelling ICT equipment

The purpose of applying protective markings to all assets in an area is to reduce the likelihood that a system user will accidentally input classified information into another system residing in the same area that is of a lower classification than the information.

Applying protective markings to assets helps determine the appropriate sanitisation, disposal or destruction requirements of the asset based on its classification.

Labelling high assurance products

High assurance products often have tamper-evident seals placed on their external surfaces. To assist system users in noticing changes to the seals, and to prevent functionality being degraded, agencies must limit the use of non-essential labels.

Labelling HGCE

HGCE often have tamper-evident seals placed on their external surfaces. To assist system users in noticing changes to the seals, and to prevent functionality being degraded, agencies must only place seals on equipment when approved by DSD to do so.

References

Nil.

Product Patching and Updating

Objective

Products are updated with security patches.

Context

Scope

This section describes patching both evaluated and non-evaluated software and ICT equipment.

Controls

Vulnerabilities and patch availability awareness

Control: 0297; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should monitor relevant sources for information about new vulnerabilities and security patches for software and ICT equipment they use.

Patching vulnerabilities in products

Control: 1143; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must have a patch management strategy.

Control: 0940; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should apply all security patches as soon as possible.

Control: 1144; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must apply all critical security patches as soon as possible.

Control: 0298; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that security patches are applied through a vendor-recommended patch or upgrade process.

Control: 0300; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not patch high assurance products or HGCE without the patch being approved by DSD.

When security patches are not available

Control: 0941; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Where known vulnerabilities cannot be patched, or security patches are not available, agencies should implement one or more of:

- controls to resolve the vulnerability by either:
  - disabling the functionality associated with the vulnerability though product configuration
  - asking the vendor for an alternative method of managing the vulnerability
  - moving to a different product with a more responsive vendor
  - engaging a software developer to correct the software
- controls to prevent exploitation of the vulnerability by either:
  - applying external input sanitisation (if an input triggers the exploit)
  - applying filtering or verification on the software output (if the exploit relates to an information disclosure)
  - applying additional access controls that prevent access to the vulnerability
  - configuring firewall rules to limit access to the vulnerable software
- controls to contain the exploit by either:
  - applying firewall rules limiting outward traffic that is likely in the event of an exploitation
  - applying mandatory access control preventing the execution of exploitation code
  - setting file system permissions preventing exploitation code from being written to disk

Continued on next page

- controls to detect attacks by either:
  - deploying an IDS
  - monitoring logging alerts
  - using other mechanisms as appropriate for the detection of exploits using the known vulnerability.

Firmware updates

Control: 0303; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that any firmware updates are performed in a manner that verifies the integrity and authenticity of the updating process.

Unsupported products

Control: 0304; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should assess the risk of using software or ICT equipment when a cessation date for support is announced or when the product is no longer supported by the developer.

Rationale

Vulnerabilities and patch availability awareness

It is important agencies monitor relevant sources for information about new vulnerabilities and security patches. This way, they can take proactive steps to address vulnerabilities in their systems.

Patching vulnerabilities in products

The assurance provided by an evaluation is related to the date at which the results were issued. Over the course of a normal product lifecycle, patches could be released to address known vulnerabilities. Applying these patches should be considered as part of the security risk management program.

Given the value of the information being protected, high assurance products must not be patched without specific direction from DSD. If a patch is released for a high assurance product, DSD will conduct an assessment of the patch and might revise the product's usage guidance. Likewise, for patches released for HGCE, DSD will subsequently conduct an assessment of the cryptographic vulnerability and might revise usage guidance in the consumer guide for the product.

When security patches are not available

When a security patch is not available for a known vulnerability there are a number of approaches to reducing the risk to a system. This includes resolving the vulnerability through alternative means, preventing exploitation of the vulnerability, containing the exploit or implementing security measures to detect attacks attempting to exploit the vulnerability.

Firmware updates

As firmware provides the underlying functionality for hardware it is essential that the integrity of any firmware images or updates are maintained.

Unsupported products

Once a cessation date for support is announced for software or ICT equipment, agencies will find it increasingly difficult to protect against vulnerabilities found in the software or ICT equipment as no security patches will be made available by the manufacturer. Once a cessation date for support is announced agencies are recommended to investigate new solutions that will be appropriately supported.

References

Nil.

Product Maintenance and Repairs

Objective

Products are repaired by cleared or appropriately escorted personnel.

Context

Scope

This section describes maintaining and repairing both evaluated and non-evaluated ICT equipment.

Controls

Maintenance and repairs

Control: 1079; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: required

Agencies are required to seek DSD approval before undertaking any repairs to high assurance products and HGCE.

Control: 0305; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should

Where possible, maintenance and repairs for ICT equipment containing media should be carried out on-site by an appropriately cleared technician.

Maintenance and repairs by an uncleared technician

Control: 0307; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should

If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, agencies should sanitise and reclassify or declassify the equipment and associated media before maintenance or repair work is undertaken.

Control: 0306; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician must be escorted by someone who:

- is appropriately cleared and briefed
- takes due care to ensure that classified information is not disclosed
- takes all responsible measures to ensure the integrity of the equipment
- has the authority to direct the technician.

Control: 0308; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that the ratio of escorts to uncleared technicians allows for appropriate oversight of all activities.

Control: 0943; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended that if an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician is escorted by someone who is sufficiently familiar with the product to understand the work being performed.

Off-site maintenance and repairs

Control: 0310; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies having ICT equipment maintained or repaired off-site must ensure that the physical transfer, processing and storage requirements are appropriate for the classification of the product and that procedures are complied with at all times.

Maintenance and repair of ICT equipment from secured spaces

Control: 0944; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies having ICT equipment maintained or repaired off-site treat the equipment as per the requirements for the highest classification processed, stored or communicated in the area that the equipment will be returned to.

Rationale

Maintenance and repairs

Making unauthorised repairs to high assurance products or HGCE could impact the integrity of the product or equipment.

Using cleared technicians on-site is considered the most desired approach to maintaining and repairing ICT equipment. This ensures that if classified information is disclosed during the course of maintenance or repairs the technicians are aware of the protection requirements for the information.

Maintenance and repairs by an uncleared technician

Agencies choosing to use uncleared technicians to maintain or repair ICT equipment need to be aware of the requirement for cleared personnel to escort the uncleared technicians during maintenance or repair activities.

Off-site maintenance and repairs

Agencies choosing to have ICT equipment maintained or repaired off-site need to be aware of requirements for the company's off-site facilities to be approved to process and store the products at the appropriate classification as specified by the *Physical Security Protocol* of the PSPF.

Agencies choosing to have ICT equipment maintained or repaired off-site can sanitise, declassify or lower the classification of the product prior to transport and subsequent maintenance or repair activities, to lower the physical transfer, processing and storage requirements specified by the *Information Security Protocol* and *Physical Security Protocol* of the PSPF.

Maintenance and repairs of ICT equipment from secured spaces

When ICT equipment resides in an area that also contains ICT equipment of a higher classification, a technician could modify the lower classified ICT equipment in an attempt to compromise co-located ICT equipment of a higher classification.

References

Nil.

Product Sanitisation and Disposal

Objective

ICT equipment is sanitised and disposed of in an approved manner.

Context

Scope

This section describes sanitising and disposing of both evaluated and non-evaluated ICT equipment. Additional information on the sanitisation, destruction and disposal of media can be found in the *Media Security* chapter.

Media typically found in ICT equipment includes:

- electrostatic memory devices such as laser printer cartridges and photocopier drums
- non-volatile magnetic memory such as hard disks
- non-volatile semi-conductor memory such as flash cards
- volatile memory such as RAM cards.

Controls

Sanitisation or destruction of ICT equipment

Control: 0311; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must sanitise or destroy, then declassify, ICT equipment containing classified media before disposal.

Control: 0312; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should return ICT equipment and associated media that have processed or stored AUSTEO or AGAO information to Australia for sanitisation or destruction, declassification and disposal.

Disposal of ICT equipment

Control: 0313; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must have a documented process for the disposal of ICT equipment.

Control: 0314; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must contact DSD and comply with any requirements for the disposal of high assurance products.

Control: 0315; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: required
Agencies are required to contact DSD and comply with any requirements for the disposal of HGCE.

Control: 0321; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must contact DSD and comply with any requirements for disposing of TEMPEST rated ICT equipment.

Control: 0316; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must formally authorise the disposal of ICT equipment, or waste, into the public domain.

Sanitising printer cartridges and copier drums

Control: 0317; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must print at least three pages of random text with no blank areas on each colour printer cartridge or copier drum.

Destroying printer cartridges and copier drums

Control: 0318; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies unable to sanitise printer cartridges or copier drums must destroy the cartridge or drum in accordance with the requirements for electrostatic memory devices.

Disposal of televisions and monitors

Control: 0319; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must visually inspect video screens by turning up the brightness to the maximum level to determine if any information has been burnt into or persists on the screen.

Sanitising televisions and monitors

Control: 1076; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must attempt to sanitise video screens with minor burn-in or image persistence by displaying a solid white image on the screen for an extended period of time.

Rationale

Sanitisation or destruction of ICT equipment

In order to prevent the disclosure of classified information into the public domain agencies will need to ensure that ICT equipment is either sanitised or destroyed before being declassified and authorised for release into the public domain.

Disposal of ICT equipment

When disposing of ICT equipment, agencies need to sanitise or destroy and subsequently declassify any media in the product that is capable of storing classified information. Once the media has been removed from the product it can be considered sanitised. Following subsequent approval for declassification from the owner of the information previously processed by the product, it can be disposed of.

DSD provides specific advice on how to securely dispose of high assurance products, HGCE and TEMPEST equipment. There are a number of security risks that can occur due to improper disposal including providing an attacker with an opportunity to gain insight into government capabilities.

Sanitising printer cartridges and copier drums

Printing random text with no blank areas on each colour printer cartridge or drum ensures that no residual information will be kept on the printer or copier. DSD is able to provide a suitable sanitisation file to use upon request.

Destroying printer cartridges and copier drums

When printer cartridges and copier drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them.

Disposal of televisions and monitors

Turning up the brightness to the maximum level on video screens will allow agencies to easily determine if information has been burnt in or persists upon the screen.

Sanitising televisions and monitors

All types of video screens are capable of retaining information on the screen if appropriate mitigation measures are not taken during the lifetime of the screen. CRT monitors and plasma screens can be affected by burn-in while LCD screens can be affected by image persistence.

References

Nil.

Media Security

Media Handling

Objective

Media is classified, labelled and registered.

Context

Scope

This section describes classifying, labelling and registering media. Information relating to classifying and labelling ICT equipment can be found in the *Product Classifying and Labelling* section of the *Product Security* chapter.

Controls

Reclassification and declassification procedures

Control: 0322; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must document procedures for the reclassification and declassification of media.

Classifying media storing information

Control: 0323; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must classify media to the highest classification stored on the media since any previous reclassification.

Classifying media connected to systems

Control: 0325; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must classify any media connected to a system as the system classification unless either:

- the media is read-only
- the media is inserted into a read-only device
- the system has a mechanism through which read-only access can be assured.

Reclassifying media to a lower classification

Control: 0330; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies wishing to reclassify media to a lower classification must ensure that:

- the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed
- a formal administrative decision is made to reclassify the media.

Reclassifying media to a higher classification

Control: 0331; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must reclassify media if either:

- information copied onto the media is of a higher classification
- information contained on the media is subjected to a classification upgrade.

Labelling media

Control: 0332; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should label media with a marking that indicates the maximum classification and set of caveats applicable to the information it stores; unless it is internally mounted fixed media and the ICT equipment containing the media is labelled.

Control: 0333; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that the classification of all media is easily visually identifiable.

Control: 0334; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
When using non-textual protective markings due to operational security reasons, agencies must document the labelling scheme and train personnel appropriately.

Labelling sanitised media

Control: 0335; Revision: 2; Updated: Nov-10; Applicability: S/HP, TS; Compliance: must
Agencies must label non-volatile media that has been sanitised and reclassified with a notice similar to: 'Warning: media has been sanitised and reclassified from [classification] to [classification]. Further lowering of classification only via destruction.'

Registering media

Control: 0946; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: recommended
It is recommended agencies register all media with a unique identifier in an appropriate register; unless it is internally mounted fixed media and the ICT equipment containing the media is registered.

Control: 0336; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should
Agencies should register all media with a unique identifier in an appropriate register; unless it is internally mounted fixed media and the ICT equipment containing the media is registered.

Rationale

Reclassification and declassification procedures

When reclassifying or declassifying media, the process is based on an assessment of relevant issues, including:

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

Classifying media storing information

Media that is not correctly classified can be stored, identified and handled inappropriately or accessed by a person who does not have the appropriate security clearance.

Classifying media connected to systems

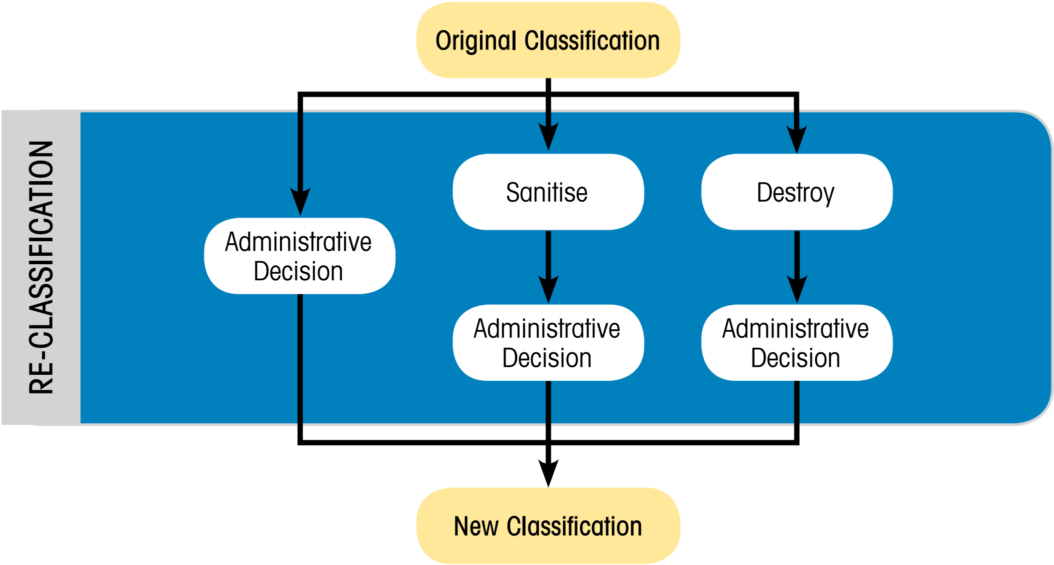
There is no guarantee that classified information is not be copied to media while connected to a system unless either read-only devices or media are used.

Classifying media below that of the system

When sufficient assurance exists that information cannot be written to media that is used with a system then the media can be treated in accordance with the classification of the information it stores rather than the classification of the system it is connect to or used with.

Reclassifying media to a lower classification

The following diagram shows an overview of the mandated reclassification process.



Reclassifying media to a higher classification

The media will always need to be protected according to the classification of the information it stores. If the classification of the information on the media changes, then so will the classification of the media.

Labelling media

Labelling helps personnel to identify the classification of media and ensure they afford the media the correct security measures.

Labelling sanitised media

It is not possible to sanitise and subsequently reclassify TOP SECRET non-volatile media.

Registering media

If agencies fail to register media with an appropriate identifier they will not be able to effectively keep track of their classified media and there will be a greater likelihood of unauthorised disclosure of classified information.

References

Nil.

Media Usage

Objective

Media is used with systems in a controlled and accountable manner.

Context

Scope

This section describes using media with systems. Further information on using media to transfer data between systems can be found in the *Data Transfer* section of the *Network Security* chapter.

Devices containing media

Where this section refers to storing media, connecting media to systems or transferring media, the controls are equally applicable to devices containing media such as cameras, mobile phones, digital audio players and portable media players.

Controls

Using media with systems

Control: 0337; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not use media with a system that has a lower classification than the media.

Storage of media

Control: 0338; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure that classified media meets the minimum physical security storage requirements as specified in the *Physical Security Protocol* of the PSPF.

Connecting media to systems

Control: 0341; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must disable any automatic execution features in operating systems for connectable devices and media.

Control: 0342; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must use one or more of the following to prevent unauthorised media from connecting to a system via the use of:

- device access control or data loss prevention software
- seals
- physical means
- other methods approved by the accreditation authority.

Control: 0343; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

When writable media is connected to a writable communications port or device, agencies should implement controls to prevent the unintended writing of data to the media.

IEEE 1394 interface connections

Control: 0344; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should

Agencies should disable IEEE 1394 interfaces (for example, FireWire ports).

Control: 0345; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies must disable IEEE 1394 interfaces (for example, FireWire ports).

Transferring media

Control: 0831; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that media containing classified information meets the minimum physical transfer requirements as specified in the *Information Security Protocol* of the PSPF.

Control: 0832; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should encrypt media with at least a DACA if it is to be transferred through an area not certified to process the classification of the information on the media.

Control: 1059; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies encrypt media with at least a DACA even if being transferred through an area certified to process the classification of the information on the media.

Using media for data transfers

Control: 0347; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies transferring data manually between two systems of different security domains or classifications should not use rewriteable media.

Media in secured areas

Control: 0346; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not
Agencies must not permit any media that uses external interface connections in a TOP SECRET area without prior written approval from the accreditation authority.

Rationale

Using media with systems

To prevent classified data spills agencies need to prevent classified media from being connected to, or used with, systems of a lesser classification than the media.

Storage of media

The security requirements for storage and physical transfer of classified information and ICT equipment are specified in the *Physical Security Protocol* and *Information Security Protocol* of the PSPF.

Connecting media to systems

Some operating systems provide the functionality to automatically execute certain types of programs that reside on optical media and flash memory media. While this functionality was designed with a legitimate purpose in mind—such as automatically loading a graphical user interface for the system user to browse the contents of the media, or to install software residing on the media—it can also be used for malicious purposes.

An attacker can create a file on optical media or a connectable device that the operating system believes it should automatically execute. However, when the operating system executes the file, it can have the same effect as when a system user explicitly executes malicious code. However, in this case the system user is taken out of the equation as the operating system executes the file without explicitly asking the system user for permission.

Some operating systems will cache information on media to improve performance. Inserting media of a higher classification into a system of a lower classification could therefore cause data to be read from the device without user intervention.

Using device access control software will prevent unauthorised media from being attached to a system. Using a whitelisting approach allows security personnel greater control over what can, and what cannot, be connected to the system.

IEEE 1394 interface connections

Known vulnerabilities have been demonstrated where attackers can connect a FireWire capable device to a locked workstation and modify information in RAM to gain access to encryption keys. Furthermore, as FireWire provides direct memory access to the system memory an attacker can read or write any content to memory that they desire. The best defence against this vulnerability is to disable access to FireWire ports using either software controls or physically damaging the FireWire ports so that devices cannot be connected.

Transferring media

As media is often transferred through areas not certified to process the classified information on the media, protection mechanisms need to be put in place to protect the information. When applying encryption to media it may reduce the requirements for storage and physical transfer as outlined in the *Physical Security Protocol* and *Information Security Protocol* of the PSPF. Any reduction in requirements is based on the original classification of information residing on the media and the level of assurance in the cryptographic product being used to encrypt the media.

Further information on reducing storage and physical transfer requirements can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Using media for data transfers

Agencies transferring data between systems of different security domains or classifications are strongly encouraged to use removal media such as write-once CDs and DVDs. This will ensure that classified information from the higher of the systems cannot be accidently transferred onto the media then onto the lower system when the media is reused for the next transfer.

Media in secured areas

Ensuring certain types of media—including USB, FireWire and eSATA capable devices—must be explicitly approved in a TOP SECRET environment provides an additional level of system user awareness and security. This practice should be used in addition to device access control software on workstations in case system users are unaware of, or choose to ignore, security requirements for media.

References

Nil.

Media Sanitisation

Objective

Media that is no longer required is sanitised.

Context

Scope

This section describes sanitising media. Information relating to sanitising ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Sanitising media

Sanitisation is the process of removing information from media. It does not automatically change the classification of the media, nor does it involve the destruction of media.

Product selection

Agencies are permitted to use non-evaluated products to sanitise media. However, the product still needs to conform to the requirements for sanitising media as outlined in this section.

Hybrid hard drives

When sanitising hybrid hard drives, the sanitisation and post sanitisation treatment requirements for flash memory devices apply.

Solid state drives

When sanitising solid state drives, the sanitisation and post sanitisation treatment requirements for flash memory devices apply.

Controls

Sanitisation procedures

Control: 0348; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must document procedures for the sanitisation of media.

Media that cannot be sanitised

Control: 0350; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must destroy the following media types prior to disposal, as they cannot be sanitised:

- microfiche
- microfilm
- optical discs
- printer ribbons and the impact surface facing the platen
- programmable read-only memory
- read-only memory
- faulty media that cannot be successfully sanitised.

Volatile media sanitisation

Control: 0351; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: must
Agencies must sanitise volatile media by either:

- removing power from the media for at least 10 minutes
- overwriting all locations of the media with an arbitrary pattern followed by a read back for verification.

Control: 0352; Revision: 1; Updated: Sep-09; Applicability: C, S/HP, TS; Compliance: must
Agencies must sanitise volatile media by overwriting the media at least once in its entirety with an arbitrary pattern, followed by a read back for verification, followed by removing power from the media for at least 10 minutes.

Treatment of volatile media following sanitisation

Control: 0353; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Following sanitisation, volatile media must be treated no less than as indicated in the table below.

PRE-SANITISATION CLASSIFICATION	POST-SANITISATION CLASSIFICATION
TOP SECRET	UNCLASSIFIED (under certain circumstances)
SECRET/HIGHLY PROTECTED	UNCLASSIFIED
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED/PROTECTED	UNCLASSIFIED
IN-CONFIDENCE	UNCLASSIFIED
UNCLASSIFIED	UNCLASSIFIED

Circumstances preventing reclassification of volatile media

Control: 0835; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not
Volatile media must not be reclassified below TOP SECRET if the volatile media either:

- stored sensitive, static, data for an extended period of time
- sensitive data was repeatedly stored or written to the same location on the volatile media for an extended period of time.

Non-volatile magnetic media sanitisation

Control: 0354; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must sanitise non-volatile magnetic media by:

- if pre-2001 or under 15GB: overwriting the media at least three times in its entirety with an arbitrary pattern followed by a read back for verification
- if post-2001 or over 15GB: overwriting the media at least once in its entirety with an arbitrary pattern followed by a read back for verification.

Control: 1065; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should reset the host protected area and drive configuration overlay table of non-volatile magnetic hard disks prior to overwriting the media.

Control: 1066; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies attempt to overwrite the growth defects table (g-list) on non-volatile magnetic hard disks.

Control: 1067; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use the ATA secure erase command, where available, for sanitising non-volatile magnetic hard disks instead of using block overwriting software.

Control: 1068; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must boot from separate media to the media being sanitised to undertake the sanitisation process.

Treatment of non-volatile magnetic media following sanitisation

Control: 0356; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Following sanitisation, non-volatile magnetic media must be treated no less than as indicated in the table below.

PRE-SANITISATION CLASSIFICATION	POST-SANITISATION CLASSIFICATION
TOP SECRET	TOP SECRET
SECRET/HIGHLY PROTECTED	CONFIDENTIAL
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED/PROTECTED	UNCLASSIFIED
IN-CONFIDENCE	UNCLASSIFIED
UNCLASSIFIED	UNCLASSIFIED

Non-volatile EPROM media sanitisation

Control: 0357; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must sanitise non-volatile EPROM media by erasing in accordance with the manufacturer's specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

Non-volatile EEPROM media sanitisation

Control: 0836; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must sanitise non-volatile EEPROM media by overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

Treatment of non-volatile EPROM and EEPROM media following sanitisation

Control: 0358; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Following sanitisation, non-volatile EPROM and EEPROM media must be treated no less than as indicated in the table below.

PRE-SANITISATION CLASSIFICATION	POST-SANITISATION CLASSIFICATION
TOP SECRET	TOP SECRET
SECRET/HIGHLY PROTECTED	CONFIDENTIAL
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED/PROTECTED	UNCLASSIFIED
IN-CONFIDENCE	UNCLASSIFIED
UNCLASSIFIED	UNCLASSIFIED

Non-volatile flash memory media sanitisation

Control: 0359; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must sanitise non-volatile flash memory media by overwriting the media at least twice in its entirety with a pseudo random pattern, followed by a read back for verification.

Treatment of non-volatile flash memory media following sanitisation

Control: 0360; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Following sanitisation, non-volatile flash memory media must be treated no less than as indicated in the table below.

PRE-SANITISATION CLASSIFICATION	POST-SANITISATION CLASSIFICATION
TOP SECRET	TOP SECRET
SECRET/HIGHLY PROTECTED	SECRET/HIGHLY PROTECTED
CONFIDENTIAL	CONFIDENTIAL
RESTRICTED/PROTECTED	UNCLASSIFIED
IN-CONFIDENCE	UNCLASSIFIED
UNCLASSIFIED	UNCLASSIFIED

Sanitising media prior to reuse

Control: 0947; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies sanitise all media prior to reuse at the same or higher classification.

Verifying sanitised media

Control: 0949; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies verify the sanitisation of media using a different product from the one used to perform the initial sanitisation.

Rationale

Sanitisation procedures

Sanitising media prior to reuse in a different environment ensures that information is not inadvertently accessed by an unauthorised individual or protected by insufficient security measures.

Using approved sanitisation methods provides a high level of assurance that no remnant data is on the media.

The procedures used in this manual are designed not only to prevent common attacks that are currently feasible but also to protect from threats that could emerge in the future.

When sanitising media, it is necessary to read back the contents of the media to verify the overwrite process completed successfully.

Media that cannot be sanitised

Some types of media cannot be sanitised and therefore must be destroyed. It is not possible to use these types of media while maintaining a high level of assurance that no previous data can be recovered.

Volatile media sanitisation

When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to times resulting from research on recovering the contents of volatile media.

Treatment of volatile media following sanitisation

There is published literature that supports short-term remanence effects (the residual information that remains on media after erasure) in volatile media. Data retention time is reported to be in the magnitude of minutes (at normal room temperatures) to hours (in extreme cold), depending on the temperature of the volatile media. Further, published literature has shown that some volatile media can suffer from long-term remanence effects resulting from physical changes to the media due to continuous storage of static data for an extended period of time. It is for these reasons that under certain circumstances TOP SECRET volatile media must always remain at this classification, even after sanitisation.

Circumstances preventing reclassification of volatile media

Typical circumstances preventing the reclassification of TOP SECRET volatile media include a static cryptographic key being stored in the same memory location in volatile media during every boot of a device and a static image being displayed on a device and stored in volatile media for a period of months.

Non-volatile magnetic media sanitisation

Both the host protected area and device configuration overlay table of non-volatile magnetic hard disks are normally not visible to the operating system or the computer's BIOS. Hence any sanitisation of the readable sectors on the media will not overwrite these hidden sectors leaving any information contained in these locations untouched. Some sanitisation programs include the ability to reset devices to their default state removing any host protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of the media during the subsequent sanitisation process.

Modern non-volatile magnetic hard disks automatically reallocate space for bad sectors at a hardware level. These bad sectors are maintained in what is known as the growth defects table or 'g-list'. If information was stored in a sector that is subsequently added to the g-list, sanitising the media will not overwrite these non-addressable bad sectors. While these sectors may be considered bad by the device, quite often this is due to the sectors no longer meeting expected performance norms for the device and not due to an inability to read/write to the sector. The ATA secure erase command was built into the firmware of post-2001 devices and is able to access sectors that have been added to the g-list. Modern non-volatile magnetic hard disks also contain a primary defects table or 'p-list'. The p-list contains a list of bad sectors found during post-production processes. No information is ever stored in sectors on the p-list for a device as they are inaccessible before the media is used for the first time.

Treatment of non-volatile magnetic media following sanitisation

Highly classified non-volatile magnetic media cannot be sanitised below its original classification due to concerns with the sanitisation of the host protected area, device configuration overlay table and growth defects table.

Non-volatile EPROM media sanitisation

When erasing non-volatile EPROM, the manufacturer's specification for ultraviolet erasure time is multiplied by a factor of three to provide an additional level of certainty in the process.

Non-volatile EEPROM media sanitisation

A single overwrite with a pseudo random pattern is considered best practice for sanitising non-volatile EEPROM media.

Treatment of non-volatile EPROM and EEPROM media following sanitisation

As little research has been conducted on the ability to recover data on non-volatile EPROM or EEPROM media after sanitisation, highly classified media retains its original classification.

Non-volatile flash memory media sanitisation

In flash memory media, a technique called wear levelling ensures that writes are distributed evenly across each memory block in flash memory. This feature necessitates flash memory being overwritten with a pseudo random pattern twice, rather than once, as this helps ensure that all memory blocks are overwritten during sanitisation.

Treatment of non-volatile flash memory media following sanitisation

Due to the use of wear levelling in flash memory, it is possible that not all physical memory locations are written to when attempting to overwrite the media. Classified information can therefore remain on the media. This is why TOP SECRET, SECRET/HIGHLY PROTECTED and CONFIDENTIAL flash memory media must always remain at their respective classification, even after sanitisation.

Sanitising media prior to reuse

Sanitising media prior to reuse at the same or higher classification assists with enforcing the need-to-know principle.

Verifying sanitised media

Verifying the sanitisation of media with a different product to the one conducting the sanitisation process provides an independent level of assurance that the sanitisation process was conducted correctly.

References

Further information on recoverability of information from volatile media can be found in the paper *Data Remanence in Semiconductor Devices* at www.cypherpunks.to/~peter/usenix01.pdf.

The RAM testing tool memtest86+ can be obtained from memtest.org.

The graphics card RAM testing tool MemtestG80 can be obtained from simtk.org/home/memtest.

HDDerase is a freeware tool developed by the Center for Magnetic Recording Research at the University of California San Diego. It is capable of calling the ATA secure erase command for non-volatile magnetic hard disks. It is also capable of resetting host protected area and device configuration overlay table information on the media. The tool is available for download from cmrr.ucsd.edu/people/Hughes/SecureErase.shtml.

Media Destruction

Objective

Media that cannot be sanitised is destroyed.

Context

Scope

This section describes the destruction of media. Information relating to the destruction of ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Controls

Destruction procedures

Control: 0363; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must document procedures for the destruction of media.

Media destruction

Control: 0364; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

To destroy media, agencies must either:

- break up the media
- heat the media until it has either burnt to ash or melted
- degauss the media.

Control: 0366; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must use one of the methods shown in the table below.

ITEM	DESTRUCTION METHODS					
	FURNACE/ INCINERATOR	HAMMER MILL	DISINTEGRATOR	GRINDER/ SANDER	CUTTING	DEGAUSSER
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No
Magnetic floppy disks	Yes	Yes	Yes	No	Yes	Yes
Magnetic hard disks	Yes	Yes	Yes	Yes	No	Yes
Magnetic tapes	Yes	Yes	Yes	No	Yes	Yes
Optical disks	Yes	Yes	Yes	Yes	Yes	No
Semi-conductor memory	Yes	Yes	Yes	No	No	No

Media destruction equipment

Control: 0365; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must employ security equipment approved by the SCEC, and published in the *Security Equipment Catalogue*, for the purpose of media destruction.

Control: 1160; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must employ degaussers certified by the National Security Agency/Central Security Service or the Government Communications Headquarters/Communications-Electronics Security Group for the purpose of degaussing media.

Storage and handling of media waste particles

Control: 0368; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must, at minimum, store and handle the resulting media waste for all methods, except for furnace/incinerator and degausser, as for the classification given in the table below.

INITIAL MEDIA CLASSIFICATION	SCREEN APERTURE SIZE PARTICLES CAN PASS THROUGH			
	LESS THAN OR EQUAL TO 3MM	LESS THAN OR EQUAL TO 6MM	LESS THAN OR EQUAL TO 9MM	LESS THAN OR EQUAL TO 12MM
TOP SECRET	UNCLASSIFIED	RESTRICTED/ PROTECTED	CONFIDENTIAL	SECRET/HIGHLY PROTECTED
SECRET/HIGHLY PROTECTED	UNCLASSIFIED	UNCLASSIFIED	RESTRICTED/ PROTECTED	CONFIDENTIAL
CONFIDENTIAL	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	RESTRICTED/ PROTECTED
RESTRICTED/ PROTECTED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED
IN-CONFIDENCE	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

Degaussers

Control: 0361; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must use a degausser of sufficient field strength for the coercivity of the media.

Control: 0838; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must use a degausser capable of the magnetic orientation (longitudinal or perpendicular) of the media.

Control: 0362; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must comply with any product specific directions provided by product manufacturers and certification authorities.

Supervision of destruction

Control: 0370; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must perform the destruction of media under the supervision of at least one person cleared to the highest classification of the media being destroyed.

Control: 0371; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Personnel supervising the destruction of media must:

- supervise the handling of the media to the point of destruction
- ensure that the destruction is completed successfully.

Supervision of accountable material destruction

Control: 0372; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must perform the destruction of accountable material under the supervision of at least two personnel cleared to the highest classification of the media being destroyed.

Control: 0373; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Personnel supervising the destruction of accountable media must:

- supervise the handling of the material to the point of destruction
- ensure that the destruction is completed successfully
- sign a destruction certificate.

Outsourcing media destruction

Control: 0839; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not outsource the destruction of TOP SECRET media or accountable material.

Control: 0840; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies outsourcing the destruction of media to a commercial facility must use a facility that has been approved by ASIO T4 Protective Security.

Transporting media for off-site destruction

Control: 1069; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies sanitise media, if possible, prior to transporting it to an off-site location for destruction.

Rationale

Destruction procedures

Documenting procedures for media destruction will ensure that agencies carry out media destruction in an appropriate and consistent manner.

Media destruction

The destruction methods given are designed to ensure that recovery of data is impossible or impractical.

Media destruction equipment

ASIO T4 Protective Security evaluates security equipment for the purpose of destroying media. Approved security equipment is listed in the *Security Equipment Catalogue* published by SCEC.

The National Security Agency/Central Security Service's EPLD contains a list of certified degaussers.

The Government Communications Headquarters/Communications-Electronics Security Group's certified data erasure products list contains a list of certified degaussers.

Storage and handling of media waste particles

Following destruction, normal accounting and auditing procedures do not apply for media items. It is therefore essential that when an item is recorded as being destroyed, destruction is assured.

Degaussers

Coercivity varies between media types and between brands and models of the same type. Care is needed when determining the desired coercivity since a degausser of insufficient strength will not be effective. The National Security Agency/Central Security Service's EPLD contains a list of common types of media and their associated coercivity ratings.

Since 2006 perpendicular magnetic media have become available. Some degaussers are only capable of sanitising longitudinal magnetic media. Care therefore needs to be taken to ensure that a suitable degausser is used when sanitising perpendicular magnetic media.

Agencies will need to comply with any product specific directions provided by product manufacturers and certification authorities to ensure that degaussers are being used in the correct manner to achieve an effective destruction outcome.

Supervision of destruction

To ensure that classified media is appropriately destroyed it needs to be supervised to the point of destruction and have its destruction overseen by at least one person cleared to the highest classification of the media being destroyed.

Supervision of accountable material destruction

Since accountable material is more sensitive than standard classified media, it needs to be supervised by at least two personnel and have a destruction certificate signed by the personnel supervising the process.

Outsourcing media destruction

ASIO T4 Protective Security maintains a list of businesses that are accredited to destroy media in an approved manner.

Transporting media for off-site destruction

Requirements for the physical transfer of media between agencies and commercial facilities can be found in the *Information Security Protocol* of the PSPF.

References

Further information on the *Security Equipment Catalogue* and the SCEC can be found at scec.gov.au.

The National Security Agency/Central Security Service's EPLD can be found at www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

The Government Communications Headquarters/Communications-Electronics Security Group's certified data erasure products list can be found at www.cesg.gov.uk/find_a/cert_products/index.cfm.

Media Disposal

Objective

Media is declassified and approved for release before disposal into the public domain.

Context

Scope

This section describes the disposal of media. Information relating to the disposal of ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Controls

Disposal procedures

Control: 0374; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must document procedures for the disposal of media.

Declassification prior to disposal

Control: 0375; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must declassify all media prior to disposing of it into the public domain.

Declassifying media

Control: 0329; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies declassifying media must ensure that:

- the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed
- a formal administrative decision is made to release the media into the public domain.

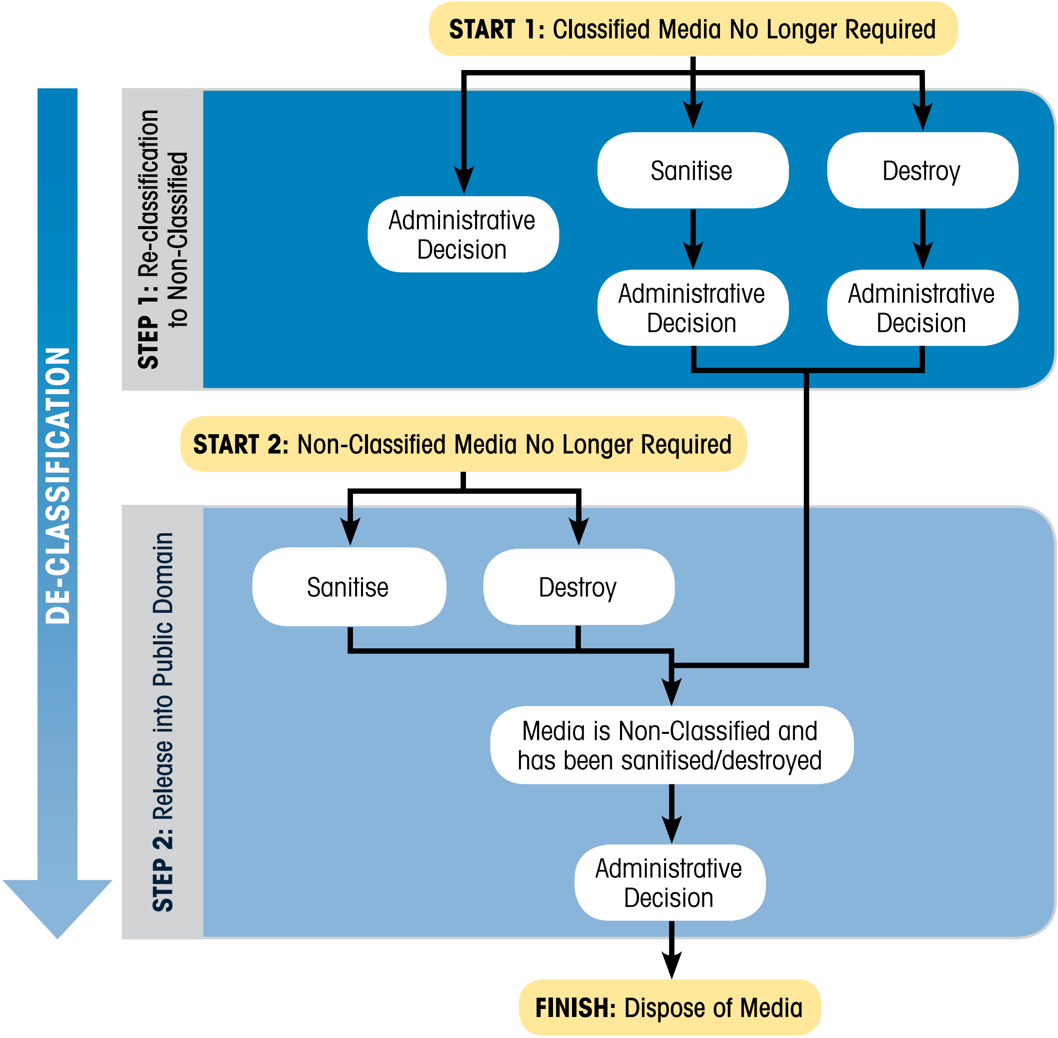
Disposal of media

Control: 0378; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must dispose of media in a manner that does not draw undue attention to its previous classification.

Rationale

Disposal procedures

The following diagram shows an overview of the mandated disposal process. In the diagram there are two starting points, one for classified media and one for unclassified media. Also note that declassification is the entire process, including any reclassifications and administrative decisions, that must be completed before media and media waste can be released into the public domain.


START 1: Classified Media No Longer Required
DE-CLASSIFICATION
STEP 1: Re-classification to Non-Classified
Administrative Decision
Sanitise
Destroy
Administrative Decision
Administrative Decision
START 2: Non-Classified Media No Longer Required
STEP 2: Release into Public Domain
Sanitise
Destroy
Media is Non-Classified and has been sanitised/destroyed
Administrative Decision
FINISH: Dispose of Media

Declassification prior to disposal

Prior to its disposal, media needs to be declassified to ensure that classified information is not accidentally released into the public domain.

Declassifying media

The process of reclassifying, sanitising or destroying media is not sufficient for media to be declassified and released into the public domain. In order to declassify media a formal administrative decision will need to be made to release the media or waste into the public domain.

Disposal of media

Disposing of media in a manner that does not draw undue attention ensures that media that was previously classified is not subjected to additional scrutiny over that of regular waste.

References

Nil.

Software Security

Standard Operating Environments

Objective

Standard Operating Environments are hardened.

Context

Scope

This section describes the hardening of SOEs used on workstations and servers.

Characterisation

Characterisation is a technique used to analyse and record a system's configuration. It is important since it can be used to verify the system's integrity at a later date.

Methods of characterising files and directories include:

- performing a cryptographic checksum on the files/directories when they are known to be virus/contaminant free
- documenting the name, type, size and attributes of legitimate files and directories, along with any changes to this information expected under normal operating conditions
- for a Windows system, taking a system difference snapshot.

Controls

Developing hardened SOEs

Control: 0380; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should develop a hardened SOE for workstations and servers, covering:

- removal of unneeded software and operating system components
- disabling of unused or undesired functionality in software and operating systems
- use of data execution prevention functionality, preferably hardware based, when available
- implementation of access controls on relevant objects to limit system users and programs to the minimum access required
- installation of antivirus software
- installation of software-based firewalls limiting inbound and outbound network connections
- configuration of either remote logging or the transfer of local event logs to a central server.

Maintaining hardened SOEs

Control: 1033; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that for all servers and workstations:

- virus detection heuristics are set to a high level
- virus pattern signatures are checked for updates on a daily basis
- virus pattern signatures are updated as soon as possible after vendors make them available
- all disks are regularly scanned for malicious code.

Control: 0382; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that for all servers and workstations:

- system users do not have the ability to install or disable software without approval
- installed software and operating system patching is current.

Default passwords and accounts

Control: 0383; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Agencies should reduce potential vulnerabilities in their SOEs by:

- removing unused accounts
- renaming or deleting default accounts
- replacing default passwords.

Control: 0384; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: must
Agencies must reduce potential vulnerabilities in their SOEs by:

- removing unused accounts
- renaming or deleting default accounts
- replacing default passwords.

Functional separation between servers

Control: 0385; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Where high value servers have connectivity to unsecured public networks, agencies should:

- maintain effective functional separation between servers allowing them to operate independently
- minimise communications between servers at both the network and file system level as appropriate
- limit system users and programs to the minimum access needed to perform their duties.

Control: 0953; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure that functional separation between servers is achieved either:

- physically, using single dedicated machines for each function
- using virtualisation technology to create separate virtual machines for each function in the same security domain.

Using virtualisation for functional separation between servers

Control: 0841; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Virtualisation technology should not be used for functional separation between servers in different security domains at the same classification.

Control: 0842; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Virtualisation technology must not be used for functional separation between servers of different classifications.

Characterisation

Control: 0386; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should:

- characterise all servers whose functions are critical, and those identified as being at a high risk of compromise
- store the characterisation information securely off the server in a manner that maintains integrity
- update the characterisation information after every legitimate change to a system
- as part of the 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
- perform the characterisation from a trusted environment rather than the standard operating system wherever possible
- resolve any detected changes in accordance with cyber security incident management procedures.

Control: 0954; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies meet the requirement for characterisation using a DACA to perform cryptographic checksums.

Automated outbound connections by software

Control: 0387; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should review all software applications to determine whether they attempt to establish any external connections.

Control: 0388; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
If automated outbound connection functionality is included, agencies should make a business decision to determine whether to permit or deny these connections, including an assessment of the security risks involved in doing so.

Knowledge of software used on systems

Control: 0381; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should limit the disclosure of software installed on their systems.

Rationale

Developing hardened SOEs

Antivirus software, while important, can be defeated by malicious code that has yet to be identified by antivirus vendors. This can include targeted attacks, where a new virus is engineered or an existing one modified to defeat the signature-based detection schemes used by most antivirus software.

The use of antivirus software adds value to the defence of workstations, but it cannot be relied upon by itself to protect the workstation. Hardened SOEs still need to be deployed to help protect workstations against a broader range of security risks.

Maintaining hardened SOEs

While a SOE can be sufficiently hardened when it is deployed, its security will progressively degrade over time.

Agencies can address the degradation of the security of a SOE by:

- ensuring that patches are continually applied
- system users cannot disable or bypass security functionality
- antivirus and other security software is appropriately maintained with the latest signatures.

Default passwords and accounts

Default passwords and accounts for operating systems are often exploited by attackers as they are well documented in product manuals and can be easily checked in an automated manner with little effort required.

Functional separation between servers

Servers with a high value include those in a gateway environment such as web, email, file and IP telephony servers.

Agencies may also implement separation through the use of techniques to restrict a process to a limited portion of the file system, but this is less effective.

Using virtualisation for functional separation between servers

Virtualisation is approved as a method of achieving functional separation between servers if the servers reside in the same security domain. Virtualisation is not approved as a domain separation method.

Characterisation

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 forensic investigations where an infected disk can be compared to stored characterisation data in order to determine what files have been changed or introduced.

Automated outbound connections by software

Examples of applications that include beaconing functionality (a continuous signalling of error or location information) are applications that initiate a connection to the vendor website over the Internet and applications for inbound remote management.

Knowledge of software used on systems

Information about installed software that could be disclosed includes:

- user agent on web requests disclosing the web browser type
- network and email client information in email headers
- email server software headers.

This information could provide a malicious entity with knowledge of how to tailor attacks to exploit vulnerabilities in the systems.

References

Independent testing of different antivirus software and their effectiveness can be found at www.av-comparatives.org.

Application Whitelisting

Objective

Only approved applications are used on operating systems.

Context

Scope

This section describes the use of technical controls to restrict the specific applications that can be accessed by a user or group of users.

Application whitelisting

Application whitelisting is an approach in which all executables and applications are prevented from executing by default. Those that are allowed to execute are explicitly specified.

Controls

Application whitelisting

Control: 0843; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should implement application whitelisting as part of the SOE for both workstations and servers.

System user permissions

Control: 0844; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should prevent a system user from running arbitrary executables.

Control: 0845; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should restrict a system user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties.

Control: 0846; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that a system user cannot disable the application whitelisting mechanism.

Control: 0847; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that application whitelisting does not replace the antivirus software already in place for a system.

System administrator permissions

Control: 0848; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that system administrators are not automatically exempt from application whitelisting policy.

Application whitelisting configuration

Control: 0849; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that the default policy is to deny the execution of software.

Control: 0850; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that application whitelisting is used in addition to a strong access control list model and the use of limited privilege accounts.

Control: 0851; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should plan and test application whitelisting thoroughly prior to implementation.

Control: 0955; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies restrict the decision whether to run an executable based on the following, in the order of preference shown:

- cryptographic hash
- executable absolute path
- digital signature
- parent folder.

Control: 0956; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies restrict write access to folders of any executables which are permitted to run by the application whitelisting controls.

Control: 0957; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that logs from the application whitelisting implementation include all relevant information.

Rationale

Application whitelisting

Application whitelisting can be an effective mechanism to prevent the compromise of a system resulting from the exploitation of vulnerabilities in an application or from the execution of malicious code.

Defining a list of trusted executables—a whitelist—is a more practical and secure method of securing a system than relying on a list of bad executables to be prevented from running.

Application whitelisting is just one part of a defence-in-depth strategy for preventing attacks and mitigating the consequences of attacks.

System user permissions

An average system user requires access to only a few applications, or groups of applications, in order to conduct their work. Restricting the system user's permissions to this limited set of applications reduces the opportunities for attacking the system.

System administrator permissions

Since the consequences of running malicious code as a privileged user are much more severe than as an unprivileged user, application whitelisting should also be enforced for system administrators.

Application whitelisting configuration

A decision to execute should be made based on cryptographic hash as it is more secure than a decision based on the executable's signature, path or parent folder.

In order for application whitelisting to be effective an agency must initially gather information on necessary executables and applications in order to ensure the implementation is fully effective.

Different application whitelisting controls, such as restricting execution based on cryptographic hash or folder, have various advantages and disadvantages. Agencies need to be aware of this when implementing application whitelisting.

Application whitelisting based on parent folder or executable path is futile if access control list permissions allow a system user to write to the folders or overwrite permitted executables.

Adequate logging information can allow system administrators to further refine the application whitelisting implementation and detect patterns of occurrences of system users being denied access.

References

Further information on application whitelisting as implemented by Microsoft can be found at technet.microsoft.com/en-us/library/bb457006.aspx.

Web Applications

Objective

Access to web content is implemented in a secure and accountable manner.

Context

Scope

This section describes web browsers, plug-ins and active content including developing and implementing appropriate use policies. The requirements in this section apply equally to websites accessed via the Internet as well as websites accessed on an intranet.

Controls

Web usage policy

Control: 0258; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must have a policy governing appropriate web usage.

Web proxy

Control: 0260; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should use a web proxy for all Web browsing activities.

Control: 0261; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

A web proxy should authenticate system users and provide logging that includes the following details about websites accessed:

- address (uniform resource locator)
- time/date
- system user
- internal IP address
- external IP address.

Control: 1149; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should block personnel without a demonstrated business requirement from downloading executable files from external websites.

Applications and plug-ins

Control: 0262; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

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

SSL/TLS filtering

Control: 0263; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies permitting SSL/TLS through their gateways should implement either:

- a solution that decrypts and inspects the SSL/TLS traffic as per content filtering requirements
- a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked.

Inspection of SSL/TLS traffic

Control: 0996; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies seek legal advice regarding the inspection of encrypted SSL/TLS traffic by their gateways.

Whitelisting websites

Control: 0958; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies implement whitelisting for all HTTP traffic being communicated through their gateways.

Control: 0995; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies using a whitelist on their gateways to specify the external addresses to which encrypted connections are permitted, specify whitelist addresses by domain name or IP address.

Blacklisting websites

Control: 0959; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that if agencies do not whitelist websites they blacklist websites to prevent access to known malicious websites.

Control: 0960; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies blacklisting websites update the blacklist on a frequent basis to ensure that it remains effective.

Client-side active content

Control: 0961; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies block client-side active content, such as Java and ActiveX, which might not have a large business impact.

Control: 0962; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies:

- use client-side controls that allow JavaScript on a per website basis
- add JavaScript functions used only for malicious purposes to the web content filter or IDS.

Web content filter

Control: 0963; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use the web proxy to filter content that is potentially harmful to system users and their workstations.

Rationale

Web usage policy

If agencies allow system users to access the Web they will need to define the extent of web access that is granted. This can be achieved through the web usage policy and education of system users.

Web proxy

Web proxies provide valuable information in determining if malicious code is performing regular interactions over web traffic. Web proxies also provide usable information if system users are violating web usage policies.

Applications and plug-ins

Web browsers can be configured to allow the automatic launching of downloaded files. This can occur with or without the system user’s knowledge thus making the workstation vulnerable to attack.

SSL/TLS filtering

Since SSL/TLS web traffic travelling over HTTPS connections can deliver content without any filtering, agencies can reduce this security risk by using SSL/TLS inspection so that web traffic can be filtered.

An alternative to using a whitelist for HTTPS websites is to allow websites that have a low risk of delivering malicious code and have a high privacy requirement, such as web banking, to continue to have end-to-end encryption.

Inspection of SSL/TLS traffic

As encrypted SSL/TLS traffic may contain personally identifiable information agencies are recommended to seek legal advice on whether inspecting such traffic could be in breach of the Privacy Act.

Whitelisting websites

Defining a whitelist of permitted websites and blocking all unlisted websites effectively removes one of the most common data delivery and exfiltration techniques used by malicious code. However, if personnel 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.

Client-side active content

Software that runs on systems should be controlled. Active content delivered though websites should be constrained so that it cannot arbitrarily access system users' files or deliver malicious code. Unfortunately the implementations of web browsers regularly contain flaws that permit such activity.

Web content filter

Using a web proxy provides an opportunity to filter out potentially harmful information to system users and their workstations.

References

A web whitelisting software application that allows for the management of whitelists can be obtained from whitetrash.sf.net.

Examples of client-side JavaScript controls are available at noscript.net.

A list of JavaScript functions that are typically used for malicious purposes is listed on the OnSecure website at members.onsecure.gov.au.

Email Applications

Objective

Email messages have appropriate protective markings.

Context

Scope

This section describes protective markings on email. Information on email infrastructure is located in the *Email Infrastructure* section of the *Network Security* chapter.

Automatically generated emails

The requirements for emails in this section apply equally to automatically generated emails.

Controls

Email usage policy

Control: 0264; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must have a policy governing the use of email.

Email distribution

Control: 0269; Revision: 1; Updated: Sep-09; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that emails containing AUSTEO, AGAO or other nationality releasability marked information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

Protective marking standard

Control: 0270; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should comply with the standard for the application of protective markings to emails as promulgated by AGIMO.

Marking tools

Control: 0271; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow a protective marking to be inserted into system user generated emails without their intervention.

Control: 0272; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies providing a marking tool should not allow system users to select protective markings that the system has not been accredited to process, store or communicate.

Control: 1089; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies providing a marking tool should not allow system users replying to or forwarding an email to select a protective marking that indicates that the classification of the email is lower than a previous classification used for the email.

Marking official emails

Control: 0273; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
All official emails must have a protective marking.

Control: 0275; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Email protective markings must accurately reflect each element of an email, including attachments.

Emails from outside the government

Control: 0278; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Where an unmarked email has originated outside the government, the agency must assess the information and determine how it is to be handled.

Marking personal emails

Control: 0852; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Where an email is of a personal nature and does not contain government information, protective markings for official information should not be used.

Control: 0966; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that where an email is of a personal nature and does not contain government information, the protective marking UNOFFICIAL be used.

Receiving unmarked emails

Control: 0967; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that where an unmarked email has originated from an Australian or overseas government agency, personnel contact the originator to determine how it is to be handled.

Receiving emails with unknown protective markings

Control: 0968; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that where an email is received with an unknown protective marking from an Australian or overseas government agency, personnel contact the originator to determine appropriate security measures.

Printing

Control: 0969; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies configure systems so that the protective markings appear at the top and bottom of every page when the email is printed.

Rationale

Email usage policy

There are many security risks associated with the non-secure nature of email that are often overlooked. Documenting them will inform information owners about these security risks and how they might affect business operations.

Email distribution

Often the membership and nationality of members of email distribution lists is unknown. Therefore personnel sending sensitive emails with AUSTEO, AGAO or other nationality releasability marked information to distribution lists could accidentally cause a cyber security incident.

Protective marking standard

Applying markings that reflect the protective requirements of an email informs the recipient on how to appropriately handle the email as a whole.

The application of protective markings as per the AGIMO standard facilitates interoperability across government.

Marking tools

Requiring system user intervention in the marking of system user-generated emails assures a conscious decision by the system user, lessening the chance of incorrectly marked emails.

Allowing system users to choose only protective markings for which the system is accredited lessens the chance of a system user inadvertently over-classifying an email. It also reminds them of the maximum classification of information permitted on the system.

Gateway filters can only check the most recent protective marking applied to an email. Therefore when system users are forwarding or responding to an email, forcing them to apply a protective marking that is at least as high as that of the email they received will help gateway filters prevent emails being sent to systems that are not accredited to handle the original classification of the email.

Marking official emails

As for paper-based information, all electronic-based information needs to be marked with an appropriate protective marking. This ensures that appropriate security measures are applied to the information and prevents unauthorised information being released into the public domain.

When a protective marking is applied to an email it is important that it reflects the highest classification of the information in the body of the email and in any attachments to the email.

Emails from outside the government

If an email is received from outside government the system user has an obligation to determine the appropriate security measures for the email if it is to be responded to, forwarded on or printed out.

Marking personal emails

Applying incorrect protective markings to emails that do not contain government information places an extra burden on protecting emails that do not need protection. The use of UNOFFICIAL as a protective marking has become the de facto standard in government for protectively marking emails that do not contain government information.

Receiving unmarked emails

If an email is received without a protective marking the agency has an obligation to contact the originator to seek clarification on the appropriate security measures for the email. Alternatively, where an agency receives unmarked non-government emails as part of its business practice the application of protective markings can be automated by a system.

Receiving emails with unknown protective markings

If an email is received with a protective marking that a system user is not familiar with, they have an obligation to contact the originator to clarify the protective marking and the appropriate security measures for the email.

Printing

The *Information Security Protocol* of the PSPF requires that paper-based information have the classification of the information placed at the top and bottom of each piece of paper.

References

The AGIMO email protective markings standard and its associated implementation guide is available from www.finance.gov.au/e-government/security-and-authentication/ict-security/index.html.

Software Application Development

Objective

Secure programming methods and testing are used for application development.

Context

Scope

This section describes developing, upgrading and maintaining application software used on systems.

Controls

Software development environments

Control: 0400; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that software development environments are configured such that:

- there are at least three environments covering:
  - development
  - testing
  - production
- information flow between the environments is strictly limited according to a defined and documented policy, with access granted only to system users with a clear business requirement
- new development and modifications only take place in the development environment
- write access to the authoritative source for the software is disabled.

Secure programming

Control: 0401; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that software developers use secure programming practices when writing code, including:

- designing software to use the lowest privilege level needed to achieve its task
- denying access by default
- checking return values of all system calls
- validating all inputs.

Software testing

Control: 0402; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Software should be reviewed or tested for vulnerabilities before it is used in a production environment.

Control: 0403; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Software should be reviewed or tested by an independent party as well as the developer.

Rationale

Software development environments

Segregating development, testing and production environments limits the spread of malicious code and minimises the likelihood of faulty code being put into production.

Limiting access to development and testing environments will reduce the information that can be gained by an internal attacker.

Secure programming

Designing software to use the lowest privilege level needed to achieve its task will limit the privileges an attacker could gain should they subvert the software security.

Validating all inputs will ensure that the input is within expected ranges, reducing the chance that malicious or erroneous input causes unexpected results.

Software testing

Software reviewing and testing will lessen the possibility of vulnerabilities being introduced into a production environment.

Using an independent party for software testing will remove any bias that can occur when a developer tests their own software.

References

Nil.

Web Application Development

Objective

Security measures are incorporated into all web applications.

Context

Scope

This section describes deploying web applications and websites.

Protecting web servers

Even though web servers may only contain information authorised for release into the public domain there still remains a need to protect the integrity and availability of the information. Web servers are therefore to be treated in accordance with the requirements of the classification of the system they are connected to.

Web application components

Web application components at a high level consist of a web server for presentation, a web application for processing and a database for content storage. There can be more or less components, however in general there is a presentation layer, application layer and database layer.

Controls

Website content

Control: 0389; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should review all active content on their web servers for information security issues.

Segregation of web application components

Control: 0390; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should minimise connectivity and access between each web application component.

Web applications

Control: 0971; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies follow the documentation provided in the Open Web Application Security Project guide to building secure web applications and web services.

Rationale

Website content

Reviewing active content on web servers will assist in identifying and mitigating information security issues.

Segregation of web application components

Web applications are typically very exposed services that provide complex interactions with system users. This greatly increases the risk of being compromised. By segregating components the impact of potential application flaws is limited.

Web applications

The Open Web Application Security Project guide provides a comprehensive resource to consult when developing web applications.

References

Further information on web application security is available from the Open Web Application Security Project at www.owasp.org.

Databases

Objective

Database content is protected from personnel without a need-to-know.

Context

Scope

This section describes databases and interfaces, such as search engines, to databases.

Controls

Data labelling

Control: 0391; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should

Agencies should ensure that all information stored in a database is associated with an appropriate protective marking if either the information:

- could be exported to a different system
- contains differing classifications or different handling requirements.

Control: 0392; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should

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

Control: 0393; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must ensure that all information stored in a database is associated with an appropriate protective marking if either the information:

- could be exported to a different system
- contains differing classifications or different handling requirements.

Control: 0394; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: must

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

Database files

Control: 0395; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should

Agencies should protect database files from access that bypasses the database's normal access controls.

Control: 0396; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: must

Agencies must protect database files from access that bypasses the database's normal access controls.

Accountability

Control: 0397; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that databases provide functionality to allow for auditing of system users' actions.

Search engines

Control: 0398; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that system users who do not have sufficient security clearances to view database contents cannot see associated metadata in a list of results from a search engine query.

Control: 0399; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

If results from database queries cannot be appropriately filtered, agencies must ensure that all query results are appropriately sanitised to meet the minimum security clearances of system users.

Rationale

Data labelling

Protective markings can be applied to records, tables or to the database as a whole, depending on structure and use.

Database files

Even though a database may provide access controls to the information it provides, the database files will still need to be protected.

Accountability

If system users' interactions with databases are not logged and audited, agencies will not be able to appropriately investigate any misuse or compromise of database content.

Search engines

Even if a search engine prevents system users viewing information that they do not have sufficient security clearances to access, the associated metadata could contain information above the security clearances of the system user. In such cases, restricting access to, or sanitising, this metadata prevents system users seeing information they are not cleared to view.

References

Nil.

Access Control

Identification and Authentication

Objective

Password selection policies and password management practices are implemented on systems.

Context

Scope

This section describes the identification and authentication of all system users.

Methods for user identification and authentication

User authentication can be achieved by various means, including biometrics, cryptographic tokens, passphrases, passwords and smartcards. Where this manual refers to passwords it equally applies to passphrases.

Controls

Policies and procedures

Control: 0413; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must:

- develop and maintain a set of policies and procedures covering system users':
  - identification
  - authentication
  - authorisation
- make their system users aware of the policies and procedures.

System user identification

Control: 0414; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure that all system users are:

- uniquely identifiable
- authenticated on each occasion that access is granted to a system.

Shared accounts

Control: 0973; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: recommended

It is recommended agencies do not use shared non user-specific accounts.

Control: 0415; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not

Agencies must not use shared non user-specific accounts.

System user identification for shared accounts

Control: 0416; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

If agencies choose to allow shared, non user-specific accounts they must ensure that another method of determining the identification of the system user is implemented.

Methods for system user identification and authentication

Control: 0417; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system.

Control: 0974; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure that they combine the use of multiple methods when identifying and authenticating system users.

Protecting stored authentication information

Control: 0418; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not allow storage of unprotected authentication information that grants system access or decrypts an encrypted device, to be located on, or with, the system or device to which the authentication information grants access.

Protecting authentication data in transit

Control: 0419; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that system authentication data is protected when in transit across networks.

Identification of foreign nationals

Control: 0420; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Where systems contain AUSTEO, AGAO or other nationality releasability marked information, agencies must provide a mechanism that allows system users and processes to identify system users who are foreign nationals, including seconded foreign nationals.

Control: 0975; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies using AUSTEO or AGAO systems that provide a mechanism allowing system users and processes to identify system users who are foreign nationals, including seconded foreign nationals, ensure that this identification includes their specific nationality.

Password selection policy

Control: 0421; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Agencies should implement a password policy enforcing either:

- a minimum password length of 12 characters with no complexity requirement; or
- a minimum password length of seven characters, consisting of at least three of the following character sets:
  - lowercase characters (a-z)
  - uppercase characters (A-Z)
  - digits (0-9)
  - punctuation and special characters.

Control: 0422; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: must
Agencies must implement a password policy enforcing either:

- a minimum password length of 15 characters with no complexity requirement; or
- a minimum password length of eight characters, consisting of at least three of the following character sets:
  - lowercase characters (a-z)
  - uppercase characters (A-Z)
  - digits (0-9)
  - punctuation and special characters.

Password management

Control: 0423; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should

Agencies should:

- ensure passwords are changed at least every 90 days
- prevent system users from changing their password more than once a day
- check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements
- force the system user to change an expired password on initial logon or if reset.

Control: 0424; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should not

Agencies should not:

- allow predictable reset passwords
- reuse passwords when resetting multiple accounts
- store passwords in the clear on the system
- allow passwords to be reused within eight password changes
- allow system users to use sequential passwords.

Control: 0425; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must

Agencies must:

- ensure passwords are changed at least every 90 days
- prevent system users from changing their password more than once a day
- check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements
- force the system user to change an expired password on initial logon or if reset.

Control: 0426; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not

Agencies must not:

- allow predictable reset passwords
- reuse passwords when resetting multiple accounts
- store passwords in the clear on the system
- allow passwords to be reused within eight password changes
- allow system users to use sequential passwords.

Resetting passwords

Control: 0976; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure system users provide sufficient evidence to verify their identity when requesting a password reset for their system account.

Password authentication

Control: 1055; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should disable LAN Manager for password authentication on workstations and servers.

Session termination

Control: 0853; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity.

Session and screen locking

Control: 0427; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Agencies should:

- configure systems with a session or screen lock
- configure the lock to activate either:
  - after a maximum of 15 minutes of system user inactivity
  - if manually activated by the system user
- configure the lock to completely conceal all information on the screen
- ensure the screen is not turned off or enters a power saving state before the screen or session lock is activated
- have the system user reauthenticate to unlock the system
- deny system users the ability to disable the locking mechanism.

Control: 0428; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must
Agencies must:

- configure systems with a session or screen lock
- configure the lock to activate either:
  - after a maximum of 10 minutes of system user inactivity
  - if manually activated by the system user
- configure the lock to completely conceal all information on the screen
- ensure the screen is not turned off or enters a power saving state before the screen or session lock is activated
- have the system user reauthenticate to unlock the system
- deny system users the ability to disable the locking mechanism.

Suspension of access

Control: 0429; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
Agencies should:

- lock system user accounts after five failed logon attempts
- have a system administrator reset locked accounts
- remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the agency
- remove or suspend inactive accounts after a specified number of days.

Control: 0430; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must:

- lock system user accounts after five failed logon attempts
- have a system administrator reset locked accounts
- remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the agency
- remove or suspend inactive accounts after a specified number of days.

Investigating repeated account lockouts

Control: 0431; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should
Agencies should ensure that repeated account lockouts are investigated before reauthorising access.

Logon banner

Control: 0408; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should have a logon banner that requires a system user to acknowledge and accept their security responsibilities before access to the system is granted.

Control: 0979; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies seek legal advice on the exact wording of logon banners.

Control: 0980; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended logon banners cover issues such as:

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

Displaying when a system user last logged in

Control: 0977; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies configure systems to display the date and time of the system user's previous login during the login process.

Rationale

Policies and procedures

Developing policies and procedures will ensure consistency in identification, authentication and authorisation.

System user identification

Having uniquely identifiable system users ensures accountability.

Shared accounts

Using shared non user-specific accounts can hamper efforts to attribute actions on a system to a specific person.

System user identification for shared accounts

As shared accounts are non user-specific, agencies allowing them need to determine an appropriate method of attributing actions undertaken by such accounts to specific personnel. For example, a logbook may be used to document the date and time that a person takes responsibility for using a shared account and the actions logged against the account by the system.

Methods for system user identification and authentication

A personal identification number is typically short in length and employs a small character set, making it susceptible to brute force attacks.

Protecting stored authentication information

Limiting the storage of unprotected authentication information reduces the risk of an attacker finding and using the information to access a system under the guise of a valid system user.

Protecting authentication data in transit

Secure transmission of authentication information reduces the risk of an attacker intercepting and using the authentication information to access a system under the guise of a valid system user.

Identification of foreign nationals

Where systems contain AUSTEO, AGAO or other nationality releasability marked information, and foreign nationals have access to such systems, it is important that agencies implement appropriate security measures to help systems users identify other system users that are foreign nationals. Such security measures should help prevent the release of particularly sensitive information to those not authorised to access it.

Password selection policy

A simple six-letter password can be brute-forced in minutes by software available on the Web. Passwords with at least seven characters utilising upper and lower case, numbers and special characters have a much greater resistance to brute force attacks.

Password management

Requiring a password to be changed at least every 90 days limits the time period in which a disclosed password could be used by an unauthorised system user.

Preventing a system user from changing their password more than once a day stops the system user from immediately changing their password back to their old password.

Checking passwords for compliance with the password selection policy allows system administrators to detect unsafe password selection and ensure that the system user changes it.

Forcing a system user to change a password on account reset ensures that the system user changes the password and has a password that only they know and remember.

Disallowing predictable reset passwords reduces the risk of brute force attacks and password guessing attacks.

Using different passwords when resetting multiple accounts prevents a system user whose account has been recently reset from logging into another such account.

Disallowing passwords from being reused within eight changes prevents a system user from cycling between a small subset of passwords.

Disallowing sequential passwords reduces the risk of an attacker easily guessing a system user's next password based on their knowledge of the system user's previous password.

Resetting passwords

To reduce the likelihood of social engineering attacks aimed at service desks, agencies need to ensure that system users provide sufficient evidence to verify their identity when requesting a password reset for their system account. This evidence could be in the form of the system user either:

- physically presenting themselves and their security pass to service desk personnel who then reset their password
- physically presenting themselves to a known colleague who uses an approved online tool to reset their password
- establishing their identity by responding correctly to a number of questions before resetting their own password.

Password authentication

LAN Manager's authentication mechanism uses a very weak hashing algorithm known as the LAN Manager hash algorithm. Passwords hashed using the LAN Manager hash algorithm can easily be compromised using rainbow tables or brute force attacks.

Session termination

Developing a policy to automatically logout and shutdown workstations after an appropriate time of inactivity helps prevent the compromise of a workstation that has been authenticated to and contains classified or sensitive information in memory. Such a policy also reduces the power consumption of systems during non-operational hours.

Session and screen locking

Screen and session locking prevents unauthorised access to a system to which an authorised system user has already been authenticated to.

Ensuring that the screen does not appear to be turned off while in the locked state prevents system users forgetting they are still logged in and will prevent other system users mistakenly thinking there is a problem with a workstation and resetting it.

Suspension of access

Locking a system user account after a specified number of failed logon attempts reduces the risk of brute force attacks.

Removing a system user account when it is no longer required prevents personnel accessing their old account and reduces the number of accounts that an attacker can target.

Suspending inactive accounts after a specified number of days reduces the number of accounts that an attacker can target.

Investigating repeated account lockouts reduces the risk of any ongoing brute force logon attempts and allows security management to act accordingly.

Investigating repeated account lockouts

Repeated account lockouts may be an indication of malicious activity being directed towards compromising a particular account.

Logon banner

A logon banner for a system reminds system users of their responsibilities when using the system.

Displaying when a system user last logged in

Displaying when a system user has last logged onto a system helps system users identify any unauthorised use of their account. Accordingly, when any case of unauthorised use of an account is identified, it should be reported to an ITSM immediately so that it can be investigated.

References

Nil.

System Access

Objective

Access to information on systems is controlled through appropriate access controls.

Context

Scope

This section describes how system users access systems. Additional information on privileged users can be found in the *Privileged Access* section of this chapter, while additional information on security clearance, briefing and authorisation requirements can be found in the *Authorisations, Security Clearances and Briefings* section of the *Personnel Security for Systems* chapter.

Controls

Access from foreign controlled systems and facilities

Control: 0854; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not allow access to AUSTEO or AGAO information from systems and facilities not under the sole control of the government of Australia.

Control: 0855; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should not
Unless a security of information arrangement is in place with a foreign government, agencies should not allow access to classified information from systems and facilities not under the sole control of the government of Australia.

Enforcing authorisations on systems

Control: 0856; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must have system users' authorisations enforced by access controls.

Protecting compartmented information on systems

Control: 0857; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must have access to compartmented information enforced by the system access controls.

Developing an access control list

Control: 0981; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies follow the process in the table below for developing an access control list.

STAGE	DESCRIPTION
1	Establish groups of all system resources based on similar security objectives.
2	Determine the information 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 system users.
5	Determine the degree of access to the resource for each system user group.
6	Decide on the degree of delegation for security administration, based on the internal security policy.

Rationale

Access from foreign controlled systems and facilities

If an Australian system is to be accessed from overseas, it needs to be from at least a facility owned by a foreign government with which Australia has a security of information arrangement. Furthermore, due to the sensitivities involved with AUSTEO and AGAO systems, they can only be accessed from facilities under the sole control of the government of Australia.

Enforcing authorisations on systems

Enforcing authorisations of system users through the use of access controls on a system helps enforce the need-to-know principle.

Protecting compartmented information on systems

Compartmented information is particularly sensitive. Therefore, extra security measures need to be put in place on systems to restrict access to those with sufficient authorisations, briefings and a demonstrated need-to-know.

Developing an access control list

A process is required to assist in the development of access control lists for systems.

References

Nil.

Remote Access

Objective

Remote access to systems is minimised and strongly controlled.

Context

Scope

This section describes the method used by personnel to access a system from an off-site location to process or store information.

Controls

Authentication

Control: 0858; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must authenticate each remote connection before permitting access to a system.

Control: 0706; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should authenticate both the remote system user and device during the authentication process.

Remote privileged access

Control: 0985; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: recommended
It is recommended that agencies do not allow the use of privileged access remotely, including logging in as an unprivileged system user and then escalating privileges.

Control: 0709; Revision: 1; Updated: Sep-09; Applicability: C, S/HP, TS; Compliance: must not
Agencies must not allow the use of privileged access remotely, including logging in as an unprivileged system user and then escalating privileges.

Rationale

Authentication

Authenticating remote system users and devices ensures that only authorised system users and devices are allowed to connect to systems.

Remote privileged access

The extent of a compromise of remote access to a system can be limited by preventing the use of remote privileged access.

References

Nil.

Event Logging and Auditing

Objective

Security related events are logged and audited.

Context

Scope

This section describes automatic logging of information relating to network activities. Information on manual logging of system management activities can be found in the *Privileged Access* section of the *Personnel Security for Systems* chapter.

Controls

Logging requirements

Control: 0580; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must develop and document logging requirements covering:

- the logging facility, including:
  - log server availability requirements
  - the reliable delivery of log information to the log server
- the list of events associated with a system or software component to be logged
- event log protection and archival requirements.

Events to be logged

Control: 0986; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: recommended

It is recommended agencies log, at minimum, the following events for all software components:

- all privileged operations
- failed attempts to elevate privileges
- security related system alerts and failures
- system user and group additions, deletions and modification to permissions
- unauthorised access attempts to critical systems and files.

Control: 0582; Revision: 1; Updated: Nov-10; Applicability: C, S/HP; Compliance: should

Agencies should log, at minimum, the following events for all software components:

- all privileged operations
- failed attempts to elevate privileges
- security related system alerts and failures
- system user and group additions, deletions and modification to permissions
- unauthorised access attempts to critical systems and files.

Control: 0583; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must
Agencies must log, at minimum, the following events for all software components:

- all privileged operations
- failed attempts to elevate privileges
- security related system alerts and failures
- system user and group additions, deletions and modification to permissions
- unauthorised access attempts to critical systems and files.

Control: 0584; Revision: 0; Updated: Sep-08; Applicability: C, S/HP, TS; Compliance: must
Agencies must log the following events for all software components:

- logons
- failed logon attempts
- logoffs.

Additional events to be logged

Control: 0987; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies log the events listed in the table below for specific software components.

SOFTWARE COMPONENT	EVENTS TO LOG
Database	System user access to the database
	Attempted access that is denied
	Changes to system user roles or database rights
	Addition of new system users, especially privileged users
	Modifications to the data
	Modifications to the format of the database
Network/operating system	Successful and failed attempts to logon and logoff
	Changes to system administrator and system user accounts
	Failed attempts to access data and system resources
	Attempts to use special privileges
	Use of special privileges
	System user or group management
	Changes to the security policy
	Service failures and restarts
	System startup and shutdown
	Changes to system configuration data
	Access to sensitive data and processes
	Data export operations
Web application	System user access to the web application
	Attempted access that is denied
	System user access to the web documents
	Search engine queries initiated by system users

Event log facility

Control: 0585; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
For each event identified as needing to be logged, agencies must ensure that the log facility records at least the following details, where applicable:

- date and time of the event
- relevant system users or process
- event description
- success or failure of the event
- event source (for example, application name)
- ICT equipment location/identification.

Control: 0988; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies establish an accurate time source, and use it consistently throughout their systems, to assist with the correlation of logged events across multiple systems.

Event log protection

Control: 0586; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Event logs must be protected from:

- modification and unauthorised access
- whole or partial loss within the defined retention period.

Control: 0989; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure that:

- systems are configured to save event logs to a separate secure log server
- event log data is archived in a manner that maintains its integrity.

Control: 0587; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should
Agencies should configure systems to save event logs to separate secure servers as soon as possible after each event occurs.

Event log archival

Control: 0859; Revision: 0; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Event logs must be archived and retained for an appropriate period as determined by the agency.

Control: 0990; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies seek advice to determine if their access and event logs are subject to the Archives Act.

Control: 0991; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies retain DNS and proxy logs for at least 18 months.

Event log auditing

Control: 0109; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must develop and document event log audit requirements covering:

- the scope of audits
- the audit schedule
- action to be taken when violations are detected
- reporting requirements
- specific responsibilities.

Rationale

Logging requirements

Event logging helps raise the security posture of a system by increasing the accountability for all system user actions.

Event logging increases the chances that malicious behaviour will be detected by logging the actions of a malicious party.

Well configured event logging allows for easier and more effective auditing if a cyber security incident occurs.

Events to be logged

The events to be logged are listed in their importance to monitoring the security posture of systems and contributing to reviews, audits and investigations.

Additional events to be logged

The additional events to be logged can be useful for reviewing, auditing or investigating software components of systems.

Event log facility

The act of logging events is not enough in itself. For each event logged, sufficient detail needs to be recorded in order for the logs to be useful when reviewed.

Event log protection

Effective log protection and storage (possibly involving the use of a dedicated event logging server) will help ensure the integrity and availability of the collected logs when they are audited.

Event log archival

It is important agencies determine an appropriate length of time to retain event logs for systems. Since event logs can assist in reviews, audits and investigations, logs should ideally be retained for the life of the system and potentially longer. The Archives Act may also influence the length of time that event logs need to be retained.

Event log auditing

Conducting audits of event logs should be seen as an integral part of the maintenance of systems, since they will help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions.

References

Nil.

Cryptography

Cryptographic Fundamentals

Objective

Cryptographic products, algorithms and protocols are evaluated by DSD before being used.

Context

Scope

This section describes the fundamentals of cryptography including the use of encryption to protect data at rest and in transit. Detailed information on algorithms and protocols approved to protect classified information can be found in the *DSD Approved Cryptographic Algorithms* and *DSD Approved Cryptographic Protocols* sections of this chapter.

Purpose of cryptography

Encryption is primarily used to provide confidentiality, thus protecting against the risk of information being intercepted by an attacker. More broadly, cryptography can also provide authentication, non-repudiation and integrity.

Using approved encryption generally reduces the likelihood of an unauthorised party gaining access to the encrypted information. However, it does not reduce the consequences of a successful attack.

Care needs to 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.

Using encryption

Encryption of data at rest can be used to reduce the physical storage and handling requirements of the media or systems containing classified information to a lesser classification or an unclassified level.

Encryption of data in transit can be used to provide protection for classified information being communicated over unclassified or public networks.

When agencies use encryption for data at rest or in transit, they are not reducing the classification of the information. However, because the information is encrypted, the consequences of it being accessed by unauthorised people are considered to be less. Therefore the security requirements applied to such information can be reduced. However, as the classification of the information does not change, the lowered security requirements cannot be used as a baseline to further lower requirements with an additional cryptographic product.

Product specific cryptographic requirements

This section describes the use of cryptography to protect classified information. Additional requirements can exist in consumer guides for products once they have completed a DCE. Such requirements supplement this manual and where conflict occurs the product specific requirements take precedence.

Using products with DACPs and DACAs

Where this manual states a requirement for a product that implements a DACP or DACA to be used to provide protection for information at rest or in transit, the product does not need to have undergone a DCE.

Federal Information Processing Standard 140

The FIPS 140 is a United States standard for the validation of both hardware and software cryptographic modules.

FIPS 140 is in its second iteration and is formally referred to as FIPS 140-2. This section refers to the standard as FIPS 140 but applies to both FIPS 140-1 and FIPS 140-2. The third iteration, FIPS 140-3, has been released in draft and this section also applies to that iteration.

FIPS 140 is not a substitute for a DCE of a product with cryptographic functionality. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality.

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

DSD will review the FIPS 140 validation report to confirm compliance with Australia's national cryptographic policy.

Controls

Using cryptographic products

Control: 1150; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using cryptographic functionality in a product must use cryptographic algorithms and protocols approved by DSD.

Control: 0453; Revision: 2; Updated: Nov-10; Applicability: R/P, C, S/HP, TS; Compliance: must

Agencies using cryptographic functionality in a product for the protection of classified information must ensure that the product has completed a DCE or other cryptographic evaluation recognised by DSD.

Reducing storage and physical transfer requirements

Control: 1161; Revision: 0; Updated: Apr-11; Applicability: IC; Compliance: must

Agencies must use an encryption product that implements a DACA if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to an unclassified level.

Control: 0457; Revision: 2; Updated: Nov-10; Applicability: R/P; Compliance: must

Agencies must use an EAL2 encryption product from DSD's EPL that has completed a DCE if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to an unclassified level.

Control: 0460; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: required

Agencies are required to use HGCE if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to an unclassified level.

Encrypting information at rest

Control: 0459; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should

Agencies using encryption to secure data at rest should use either:

- full disk encryption
- partial encryption where the access control will only allow writing to the encrypted partition.

Control: 0461; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: required

Agencies using encryption to secure data at rest are required to use either:

- full disk encryption
- partial encryption where the access control will only allow writing to the encrypted partition.

Encrypting AUSTEO and AGAO information at rest

Control: 1080; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

In addition to any encryption already in place agencies must, at minimum, use a DACA to protect AUSTEO and AGAO information when at rest on a system.

Data recovery

Control: 0455; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: must

Where practical, cryptographic products must provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

Control: 0456; Revision: 0; Updated: Sep-08; Applicability: C, S/HP, TS; Compliance: required

Where practical, cryptographic products are required to provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

Handling encrypted ICT equipment

Control: 0462; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

When ICT equipment storing encrypted information is turned on and authenticated to, it must be treated in accordance with the original classification of the equipment.

Reducing network infrastructure requirements

Control: 1162; Revision: 0; Updated: Apr-11; Applicability: IC; Compliance: must

Agencies must use an encryption product that implements a DACP if they wish to communicate classified information over unclassified or public networks.

Control: 0465; Revision: 2; Updated: Nov-10; Applicability: R/P; Compliance: must

Agencies must use an EAL2 encryption product from DSD's EPL that has completed a DCE if they wish to communicate classified information over unclassified or public networks.

Control: 0467; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: required

Agencies are required to use HGCE if they wish to communicate classified information over unclassified or public networks.

Encrypting AUSTEO and AGAO information in transit

Control: 0469; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

In addition to any encryption already in place for communication mediums, agencies must, at minimum, use a DACP to protect AUSTEO and AGAO information when in transit.

Rationale

Using cryptographic products

No real-world product can ever be guaranteed to be free of vulnerabilities. The best that can be done is to increase the amount of assurance in a product to a point that represents satisfactory security risk management. A product having undergone a DCE provides a greater amount of assurance than selecting an unevaluated cryptographic product.

Reducing storage and physical transfer requirements

When encryption is applied to media or media residing in ICT equipment it provides an additional layer of defence. While such security measures do not downgrade the classification of the information, they can be used to store and physically transfer the media or ICT equipment at an unclassified level.

Encrypting information at rest

Full disk encryption providers at greater level of protection than file based encryption. While file based encryption may encrypt individual files there is the possibility that unencrypted copies of the file may be left in temporary locations used by the operating system.

Encrypting AUSTEO and AGAO information at rest

As AUSTEO and AGAO information is particularly sensitive it needs to be encrypted when at rest.

Data recovery

The requirement for an encryption product to provide a key escrow function, where practical, was issued under a Cabinet directive in July 1998.

Handling encrypted ICT equipment

When ICT equipment employing encryption functionality is turned on and authenticated to, all information becomes accessible to the system user. At such a time the ICT equipment will need to be handled as per the classification of information.

Reducing network infrastructure requirements

When encryption is applied to classified information being communicated over networks, less assurance needs to be placed in the physical protection of the communications infrastructure. In some cases, where no physical security can be applied to the communications infrastructure—for example where information is in the public domain—encryption of classified information is the only mechanism to prevent the information being compromised.

Encrypting AUSTEO and AGAO information in transit

As AUSTEO and AGAO information is particularly sensitive it needs to be encrypted when being communicated across communications infrastructure.

References

Further information on the FIPS 140 standards can be found at:

- www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- www.csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf.

The storage and physical transfer requirements for classified information can be found in *Physical Security Protocol* and *Information Security Protocol* of the PSPF.

DSD Approved Cryptographic Algorithms

Objective

Information at rest is protected by a DSD approved cryptographic algorithm.

Context

Scope

This section describes cryptographic algorithms that DSD has approved for use in government. Implementations of the algorithms in this section need to undergo a DCE before they can be approved to protect classified information.

High grade cryptographic algorithms, which are not covered in this section, can be used for the protection of classified information if they are found suitably implemented in a product that has undergone a high grade cryptographic evaluation by DSD. Further information on high grade cryptographic algorithms can be obtained by contacting DSD.

DSD approved cryptographic algorithms

There is no guarantee or proof of security of an algorithm against presently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attacks. There have been some cases where theoretically impressive vulnerabilities have been found, however these results are not of practical application.

Where there is a range of possible key sizes for an algorithm, some of the smaller key sizes do not provide an adequate safety margin against attacks that might be found in the future. For example, future advances in number factorisation could render the use of smaller RSA moduli a vulnerability.

DSD approved cryptographic algorithms fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

The approved asymmetric/public key algorithms are:

- DH for agreeing on encryption session keys
- DSA for digital signatures
- ECDH for agreeing on encryption session keys
- ECDSA for digital signatures
- RSA for digital signatures and passing encryption session keys or similar keys.

The approved hashing algorithms are:

- Secure Hashing Algorithm 1 (SHA-1)
- Secure Hashing Algorithm 2 (SHA-224, SHA-256, SHA-384 and SHA-512).

The approved symmetric encryption algorithms are:

- AES using key lengths of 128, 192 and 256 bits
- 3DES.

Controls

Using DACAs

Control: 0471; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using an unevaluated product that implements a DACA must ensure that only DACAs can be used.

Approved asymmetric/public key algorithms

Control: 0994; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies use ECDH and ECDSA before using DH and DSA.

Using DH

Control: 0472; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using DH, for the approved use of agreeing on encryption session keys, must use a modulus of at least 1024 bits.

Using DSA

Control: 0473; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using DSA, for the approved use of digital signatures, must use a modulus of at least 1024 bits.

Using ECDH

Control: 0474; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using ECDH, for the approved use of agreeing on encryption session keys, must use a field/key size of at least 160 bits.

Using ECDSA

Control: 0475; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using ECDSA, for the approved use of digital signatures, must use a field/key size of at least 160 bits.

Using RSA

Control: 0476; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, must use a modulus of at least 1024 bits.

Control: 0477; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, must ensure that the public keys used for passing encrypted session keys are different to the keys used for digital signatures.

Approved hashing algorithms

Control: 1054; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies use SHA-2 in preference to SHA-1.

Approved symmetric encryption algorithms

Control: 0479; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not

Agencies using AES or 3DES should not use electronic codebook mode.

Using 3DES

Control: 0480; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

3DES must use either two distinct keys in the order key 1, key 2, key 1 or three distinct keys.

Rationale

Using DACAs

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

When configuring unevaluated products that implement a DACA, agencies can ensure that only the DACA can be used by disabling the unapproved algorithms in the products (preferred) or advising system users not to use them via a policy.

Approved asymmetric/public key algorithms

Over the last decade DSA and DH cryptosystems have been subject to increasingly successful sub-exponential factorisation and index-calculus based attacks. ECDH and ECDSA offer more security per bit increase in key size than either DH or DSA and are considered more secure alternatives.

Using DH

A modulus of at least 1024 bits for DH is considered best practice by the cryptographic community.

Using DSA

A modulus of at least 1024 bits for DSA is considered best practice by the cryptographic community.

Using ECDH

A field/key size of at least 160 bits for ECDH is considered best practice by the cryptographic community.

Using ECDSA

A field/key size of at least 160 bits for ECDSA is considered best practice by the cryptographic community.

Using RSA

A modulus of at least 1024 bits for RSA is considered best practice by the cryptographic community.

Approved hashing algorithms

Recent research conducted by the cryptographic community suggests that SHA-1 may be susceptible to collision attacks. While no practical collision attacks have been published for SHA-1, they may become feasible in the near future.

Approved symmetric encryption algorithms

The use of Electronic Code Book mode in block ciphers allows repeated patterns in plaintext to appear as repeated patterns in the ciphertext. Most cleartext, including written language and formatted files, contains significant repeated patterns. An attacker can use this to deduce possible meanings of ciphertext by comparison with previously intercepted data. In other cases they might be able to determine information about the key by inferring certain contents of the cleartext. The use of other modes such as Cipher Block Chaining, Cipher Feedback, Output Feedback or Counter prevents such attacks.

Using 3DES

Using three distinct keys is the most secure option, while using two distinct keys in the order key 1, key 2, key 1 is also deemed secure for practical purposes. All other keying options are equivalent to single DES, which is not deemed secure for practical purposes.

References

The following references are provided for the approved asymmetric/public key algorithms, hashing algorithms and encryption algorithms.

Further information on DH can be found in Diffie, W and Hellman, ME ‘New Directions in Cryptography’, IEEE Transactions on Information Theory, vol. 22, is. 6, pp. 644-654, November 1976.

Further information on DSA can be found in FIPS 186.

Further information on ECDH can be found in ANSI X9.63 and ANSI X9.42.

Further information on ECDSA can be found in FIPS 186-2 + Change Notice, ANSI X9.63 and ANSI X9.62.

Further information on RSA can be found in Public Key Cryptography Standards #1, RSA Laboratories.

Further information on SHA can be found in AS 2805.13.3 and FIPS 180-2.

Further information on AES can be found in FIPS 197.

Further information on 3DES can be found in AS 2805.5.4 and ANSI X9.52.

DSD Approved Cryptographic Protocols

Objective

Information in transit is protected by a DSD approved cryptographic protocol implementing a DSD approved cryptographic algorithm.

Context

Scope

This section describes cryptographic protocols that DSD has approved for use in government. Implementations of the protocols in this section need to undergo a DCE before they can be approved to protect classified information.

High grade cryptographic protocols, which are not covered in this section, can be used for the protection of classified information if they are found suitably implemented in a product that has undergone a high grade cryptographic evaluation by DSD. Further information on high grade cryptographic protocols can be obtained by contacting DSD.

DSD approved cryptographic protocols

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 in specific products have not been formally evaluated by DSD. This approval is limited to cases where they are used in accordance with the requirements in this manual.

The DSD approved cryptographic protocols are:

- SSL/TLS
- SSH
- S/MIME
- OpenPGP Message Format
- IPSec.

Controls

Using DACPs

Control: 0481; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies using a product that implements a DACP must ensure that only DACAs can be used.

Rationale

Using DACPs

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

When configuring unevaluated products that implement a DACP, agencies can ensure that only the DACA can be used by disabling the unapproved algorithms in the products (which is preferred) or advising system users not to use them via a policy.

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
- ensuring the correct management of certificate authentication processes including certificate revocation checking
- using a legitimate identity registration scheme.

References

Nil.

Secure Sockets Layer and Transport Layer Security

Objective

Secure Sockets Layer and Transport Layer Security is implemented correctly as a DSD approved cryptographic protocol.

Context

Scope

This section describes the conditions under which SSL and TLS can be used as DACPs. Additionally, as File Transfer Protocol over SSL is built on SSL/TLS it is also considered in scope.

When using a product that implements SSL/TLS, requirements for using DACPs also need to be consulted in the *DSD Approved Cryptographic Protocols* section of this chapter.

Further information on handling SSL/TLS traffic through gateways can be found in the *Web Applications* section of the *Software Security* chapter.

Controls

Using SSL and TLS

Control: 0482; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not use versions of SSL prior to version 3.0.

Control: 1139; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use the current version of TLS instead of SSL.

Rationale

Using SSL and TLS

Version 1.0 of SSL was never released and version 2.0 had significant security flaws leading to the development of SSL 3.0. SSL has since been superseded by TLS with the latest version being TLS 1.2 which was released in August 2008.

References

Further information on SSL and TLS can be found in:

- the SSL 3.0 specification at wp.netscape.com/eng/ssl3
- the TLS 1.2 definition at tools.ietf.org/html/rfc5246.

Secure Shell

Objective

Secure Shell is implemented correctly as a DSD approved cryptographic protocol.

Context

Scope

This section describes the conditions under which commercial and open-source implementations of SSH can be used as a DACP. Additionally, secure copy and Secure File Transfer Protocol use SSH and are therefore also covered by this section.

When using a product that implements SSH, requirements for using DACPs also need to be consulted in the *DSD Approved Cryptographic Protocols* section of this chapter.

Controls

Using SSH

Control: 0484; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

The table below outlines the settings that should be implemented when using SSH.

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
Do not allow empty passwords	PermitEmptyPasswords no
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

Authentication mechanisms

Control: 0485; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should use public key-based authentication in preference to using password-based authentication.

Control: 0486; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies that allow password authentication should use techniques to block brute force attempts against the password.

Automated remote access

Control: 0487; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies that use logins without a password for automated purposes should disable:

- access from IP addresses that do not need access
- port forwarding
- agent credential forwarding
- X11 display remoting
- console access.

Control: 0488; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies that use remote access without the use of a password should use the 'forced command' option to specify what command is executed.

Control: 0997; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use parameter checking when using the 'forced command' option.

SSH-agent

Control: 0489; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies that use SSH-agent or other similar key caching programs should:

- only use the software on workstation and servers with screen locks
- ensure the key cache expires within four hours of inactivity
- ensure agent credential forwarding is used when multiple SSH transversal is needed.

Rationale

Using SSH

The configuration directives provided are based on the OpenSSH implementation of SSH. Agencies implementing SSH will need to adapt these settings to suit other SSH implementations.

SSH version 1 is known to have vulnerabilities. In particular, it is susceptible to a man-in-the-middle attack, where an attacker who can intercept the protocol in each direction can make each node believe they are talking to the other. SSH version 2 does not have this vulnerability.

SSH has the ability to forward connections and access privileges in a variety of ways. This means that an attacker who can exploit any of these features can gain unauthorised access to a potentially large amount of information.

Host-based authentication requires no credentials (for example, password, public key) to authenticate (though in some cases it might make use of a host key). This renders SSH vulnerable to an IP spoofing attack.

An attacker who gains access to a system with system administrator privileges will have the ability to not only access information but to control that system completely. Given the clearly more serious consequences of this, system administrator login should not be permitted.

Authentication mechanisms

Public key–based systems have greater potential for strong authentication—put simply, people cannot remember particularly strong passwords. Password-based authentication schemes are also more susceptible to interception than public key-based authentication schemes.

Passwords are more susceptible to guessing attacks, so if passwords are used in a system then counter-measures should be put into place to reduce the chance of a successful brute force.

Automated remote access

If password-less authentication is enabled, allowing access from unknown IP addresses would allow untrusted parties to automatically authenticate to systems without needing to know the password.

If port forwarding is not disabled or it is not configured securely, an attacker may be able to gain access to forwarded ports and thereby create a communication channel between the attacker and the host.

If agent credential forwarding is enabled, an intruder could connect to the stored authentication credentials and then use them to connect to other trusted hosts or even intranet hosts, if port forwarding has been allowed as well.

X11 is a computer software system and network protocol that provides a graphical user interface for networked computers. Failing to disable X11 display remoting could result in an attacker being able to gain control of the computer displays as well as keyboard and mouse control functions.

Allowing console access allows every user who logs into the console to run programs that are normally restricted to the root user.

SSH-agent

SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH-agent launches, it will request the user's password. This password is used to unlock the user's private key. Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their password. Screen locks and expiring key caches ensure that the user's private key is not left unlocked for long periods of time.

Agent credential forwarding is required when multiple SSH connections are chained to allow each system in the chain to authenticate the user.

References

Further information on SSH can be found in the SSH specification at tools.ietf.org/html/rfc4252.

Secure Multipurpose Internet Mail Extension

Objective

Secure Multipurpose Internal Mail Extension is implemented correctly as a DSD approved cryptographic protocol.

Context

Scope

This section describes the conditions under which S/MIME can be used as a DACP.

When using a product that implements S/MIME, requirements for using DACPs also need to be consulted in the *DSD Approved Cryptographic Protocols* section of this chapter.

Information relating to the development of password selection policies and password requirements can be found in the *Identification and Authentication* section of the *Access Control* chapter.

Controls

Using S/MIME

Control: 0490; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not

Agencies should not allow versions of S/MIME earlier than 3.0 to be used.

Rationale

Using S/MIME

S/MIME 2.0 required the use of weaker cryptography (40-bit keys) than is approved for use by the government. Version 3.0 was the first version to become an Internet Engineering Task Force standard.

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 antivirus software to scan for viruses and other malicious code.

References

Further information on S/MIME can be found in the S/MIME charter at www.ietf.org/html.charters/smime-charter.html.

OpenPGP Message Format

Objective

OpenPGP Message Format is implemented correctly as a DSD approved cryptographic protocol.

Context

Scope

This section describes the conditions under which the OpenPGP Message Format can be used as a DACP. It applies to the protocol as specified in IETF's RFC 4880, which obsoletes RFC 2440.

When using a product that implements the OpenPGP Message Format, requirements for using DACPs also need to be consulted in the *DSD Approved Cryptographic Protocols* section of this chapter.

Information relating to the development of password selection policies and password requirements can be found in the *Identification and Authentication* section of the *Access Control* chapter.

Controls

Using OpenPGP Message Format

Control: 1091; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must immediately revoke key pairs when a private certificate is suspected of being compromised.

Rationale

Using OpenPGP Message Format

If the private certificate and associated key used for encrypting messages is suspected of being compromised (that is, stolen, lost or transmitted over the Internet), then no assurance can be placed in the integrity of subsequent messages that are signed by that private key. Likewise no assurance can be placed in the confidentiality of a message encrypted using the public key since third parties could intercept the message and decrypt it using the private key.

References

Further information on the OpenPGP Message Format can be found in the OpenPGP Message Format specification at tools.ietf.org/html/rfc4880.

Internet Protocol Security

Objective

Internet Protocol Security is implemented correctly as a DSD approved cryptographic protocol.

Context

Scope

This section describes conditions under which IPSec can be used as a DACP.

When using a product that implements IPSec, requirements for using DACPs also need to be consulted in the *DSD Approved Cryptographic Protocols* section of this chapter.

Modes of operation

IPSec can be operated in two modes: transport mode or tunnel mode.

Cryptographic protocols

IPSec contains two major protocols: Authentication Header and Encapsulating Security Payload.

Cryptographic algorithms

Most IPSec implementations can handle a number of cryptographic algorithms for encrypting data when the ESP protocol is used. These include 3DES and AES.

Key exchange

Most IPSec implementations handle a number of methods for sharing keying material used in hashing and encryption processes. Two common methods are manual keying and IKE using the ISAKMP. Both methods are considered suitable for use.

ISAKMP authentication

Most IPSec implementations handle a number of methods for authentication as part of ISAKMP. These can include digital certificates, encrypted nonces or pre-shared keys. These methods are considered suitable for use.

ISAKMP modes

ISAKMP uses two modes to exchange information as part of IKE. These are main mode and aggressive mode.

Controls

Mode of operation

Control: 0494; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use tunnel mode for IPSec connections.

Control: 0495; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies choosing to use transport mode should additionally use an IP tunnel for IPSec connections.

Protocols

Control: 0496; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use the ESP protocol for IPSec connections.

ISAKMP modes

Control: 0497; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies using ISAKMP should disable aggressive mode for IKE.

Security association lifetimes

Control: 0498; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should use a security association lifetime of less than four hours or 14400 seconds.

HMAC algorithms

Control: 0998; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies use HMAC-SHA-1-96 as the HMAC algorithm.

DH groups

Control: 0999; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies use the largest modulus size available for the DH exchange.

Perfect Forward Secrecy

Control: 1000; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies use Perfect Forward Secrecy for IPSec connections.

IKE Extended Authentication

Control: 1001; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies disable the use of XAUTH for IPSec connections.

Rationale

Mode of operation

The tunnel mode of operation provides full encapsulation of IP packets while the transport mode of operation only encapsulates the payload of the IP packet.

Protocols

In order to provide a secure VPN style connection both authentication and encryption are needed. ESP is the only way of providing encryption yet AH and ESP can provide authentication for the entire IP packet and the payload respectively. However ESP is generally preferred for authentication since AH by its nature has network address translation limitations.

If, however, maximum security is desired at the expense of network address translation functionality, then ESP can be wrapped inside of AH which will then authenticate the entire IP packet and not just the encrypted payload.

ISAKMP modes

Using main mode instead of aggressive mode provides greater security since all exchanges are protected.

Security association lifetimes

Using a secure association lifetime of four hours or 14400 seconds provides a balance between security and usability.

HMAC algorithms

As MD5 is no longer a DACP the only approved algorithm that can be used with HMAC is SHA-1.

DH groups

Using a larger DH group provides more entropy for the key exchange.

Perfect Forward Secrecy

Using Perfect Forward Secrecy reduces the impact of the compromise of a security association.

IKE Extended Authentication

XAUTH has documented vulnerabilities associated with its use.

References

Further information on IPSec can be found in the security architecture for the IP overview at tools.ietf.org/html/rfc2401.

Key Management

Objective

Cryptographic keying material is protected by key management procedures.

Context

Scope

This section describes the general management of cryptographic system material. Due to the wide variety of cryptographic systems and technologies available, and the varied security risks for each, detailed key management guidance is not provided in this manual.

If HGCE is being used agencies are advised to consult the respective ACSI for the equipment.

Cryptographic systems

In general, the requirements specified for systems apply equally to cryptographic systems. Where the requirements for cryptographic systems are different, the variations are contained in this section, and overrule all requirements specified elsewhere in this manual.

Controls

High grade cryptographic equipment

Control: 0499; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: required

Agencies are required to comply with *ACSI 53* and *ACSI 105* when using HGCE.

Transporting commercial grade cryptographic equipment

Control: 1002; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: recommended

It is recommended agencies do not transport commercial grade cryptographic equipment in a keyed state.

Control: 0500; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: must

Unkeyed commercial grade cryptographic equipment must be distributed and managed by a means approved for the transportation and management of government property.

Control: 0501; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: must

Keyed commercial grade cryptographic equipment must be distributed, managed and stored by a means approved for the transportation and management of government property based on the classification of the key in the equipment.

Cryptographic system administrator access

Control: 0502; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Before personnel are granted cryptographic system administrator access, agencies must ensure that they have:

- a demonstrated need for access
- read and agreed to comply with the relevant KMP for the cryptographic system they are using
- a security clearance at least equal to the highest classification of information processed by the cryptographic system
- agreed to protect the authentication information for the cryptographic system at the highest classification of information it secures
- agreed not to share authentication information for the cryptographic system without approval
- agreed to be responsible for all actions under their accounts
- agreed to report all potentially security related problems to an ITSM.

Accounting

Control: 0503; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should be able to readily account for all transactions relating to cryptographic system material including identifying hardware and software that was issued with the cryptographic equipment and materials, when they were issued and where they were issued.

Audits

Control: 0504; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should conduct audits of cryptographic system material:

- on handover/takeover of administrative responsibility for the cryptographic system
- on change of personnel with access to the cryptographic system
- at least annually.

Control: 1003; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies perform audits to:

- check all cryptographic system material as per the accounting documentation
- confirm that agreed security measures documented in the KMP are being followed.

Control: 1004; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies conduct audits using two personnel with cryptographic system administrator access.

Area security and access control

Control: 0505; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Cryptographic equipment should be stored in a room that meets the requirements for a server room of an appropriate level based on the classification of information the cryptographic system processes.

Control: 0506; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Areas in which cryptographic system material is used should be separated from other areas and designated as a cryptography controlled area.

Developing KMPs for cryptographic systems

Control: 0507; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
Agencies should develop a KMP when they have implemented a cryptographic system using commercial grade cryptographic equipment.

Control: 0509; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: required
Agencies are required to develop a KMP when they have implemented a cryptographic system using HGCE.

Contents of KMPs

Control: 0510; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
The table below describes the minimum contents which should be documented in the KMP.

TOPIC	CONTENT
Accounting	How accounting will be undertaken for the cryptographic system
	What records will be maintained
	How records will be audited
Classification	Classification of the cryptographic system hardware
	Classification of the cryptographic system software
	Classification of the cryptographic system documentation

Continued on next page

TOPIC	CONTENT
Cyber 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 cyber security incidents
Key management	Who generates keys
	How keys are delivered
	How keys are received
	Key distribution, including local, remote and 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
Maintenance	Maintaining the cryptographic system software and hardware
	Destroying cryptographic equipment and media
Objectives	Objectives of the cryptographic system and KMP, including organisational aims
References	Relevant ACSIs
	Vendor documentation
	Related policies
System description	Maximum classification of information protected
	The use of keys
	The environment
	Administrative responsibilities
	Key algorithm
	Key length
	Key lifetime
Topology	Diagrams and description of the cryptographic system topology including data flows

Control: 0511; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
The level of detail included in a KMP must be consistent with the criticality and classification of the information to be protected.

Access register

Control: 1005; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies hold and maintain an access register that records cryptographic system information such as:

- details of personnel with system administrator access
- details of those whose system administrator access was withdrawn
- details of system documents
- accounting activities
- audit activities.

Rationale

High grade cryptographic equipment

ACSI 53 and *ACSI 105* provide product specific policy for HGCE.

Transporting commercial grade cryptographic equipment

Transporting commercial grade cryptographic equipment in a keyed state exposes the equipment to the potential for interception and compromise of the key stored in the equipment. Therefore when commercial grade cryptographic equipment is transported in a keyed state it needs to be done according to the requirements for the classification of the key stored in the equipment.

Cryptographic system administrator access

Since cryptographic system administrator access involves granting privileged access to a cryptographic system, extra precautions need to be put in place surrounding the personnel chosen to be cryptographic system administrators.

Accounting

As cryptographic equipment, and the keys they store, provides a significant security function for systems it is important that agencies are able to account for all cryptographic equipment.

Audits

Cryptographic system audits are used as a process to account for cryptographic equipment.

Area security and access control

As cryptographic equipment contains particularly sensitive information additional physical security measures need to be applied to the equipment.

Developing KMPs for cryptographic systems

Most modern cryptographic systems are designed to be highly resistant to cryptographic analysis but it must be assumed that a determined attacker could obtain details of the cryptographic logic either by stealing or copying relevant material directly or by suborning an Australian national or allied national. The safeguarding of cryptographic system material by using adequate personnel, physical, documentation and procedural security measures is therefore crucial.

Contents of KMPs

When agencies implement the recommended contents for KMPs they will have a good starting point for the protection of cryptographic systems and their material.

Access register

Access registers can assist in documenting personnel who have privileged access to cryptographic systems along with previous accounting and audit activities for the system.

References

Further information key management practices can be found in AS 11770.1:2003, *Information Technology – Security Techniques – Key Management.*

ACSI 53 and *ACSI 105* can also be consulted for additional information on high grade cryptography.

Network Security

Network Management

Objective

The configuration of networks is controlled through appropriate change management processes.

Context

Scope

This section describes the management of network infrastructure.

Network diagrams

A network diagram illustrates all network devices including firewalls, IDSs, routers, switches and hubs. It does not need to illustrate all ICT equipment on the network, such as workstations or printers, although the inclusion of significant devices such as servers could aid in its interpretation.

Controls

Configuration management

Control: 0513; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should keep the network configuration under the control of a central network management authority.

Control: 0514; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
All changes to the configuration should be documented and approved through a formal change control process.

Control: 0515; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should regularly review their network configuration to ensure that it conforms to the documented network configuration.

Control: 1007; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies deploy an automated tool that compares the running configuration of network devices against the documented configuration.

Network diagrams

Control: 0516; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
For each network an agency must have:

- a high-level diagram showing all connections into the network
- a logical network diagram showing all network devices.

Updating network diagrams

Control: 0517; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
Network diagrams should:

- be updated as network changes are made
- include a ‘Current as at [date]’ statement on each page.

Control: 0518; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Network diagrams must:

- be updated as network changes are made
- include a ‘Current as at [date]’ statement on each page.

Limiting network access

Control: 1008; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: recommended
It is recommended agencies implement network access controls on all networks.

Control: 0520; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should
Agencies should implement network access controls on all networks.

Management traffic

Control: 1006; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies implement security measures to minimise the risk of unauthorised access to network management traffic travelling across a network.

Rationale

Configuration management

If the network is not centrally managed there could be sections of the network that do not comply with information security policies.

Changes should be approved by a change management process, involving representatives from all parties involved in the management of the network. This process ensures that changes are understood by all parties and reduces the likelihood of an unexpected impact on the network.

Network diagrams

As most decisions are made on the documentation that illustrates the network, it is important:

- a network diagram exists
- the network diagram is an accurate depiction of the network
- the network diagram indicates when it was last updated.

Updating network diagrams

Due to the importance of the network diagram and decisions made based upon its contents, the network diagram should be updated as changes are made. This will assist system administrators to completely understand and adequately protect the network.

Limiting network access

If an attacker has limited opportunities to connect to a given network, they have limited opportunities to attack that network. Network access controls not only prevent attackers gaining access to a network but also prevent system users carelessly connecting a network to another network of a different classification. It is also useful in segregating sensitive or compartmented information for specific system users with a need-to-know.

Circumventing some network access controls can be trivial. However their use is primarily aimed at the protection they provide against accidental connection to another network.

Management traffic

Implementing security measures specifically for management traffic provides another layer of defence on the network, should an attacker find an opportunity to connect to a given network. This also makes it more difficult for an attacker to enumerate their target network.

References

Nil.

Virtual Local Area Networks

Objective

Virtual local area networks are deployed in a secure manner that does not compromise the security of information and systems.

Context

Scope

This section describes the use of VLANs in networks.

Multi Protocol Label Switching

For the purposes of this section Multi Protocol Label Switching is considered to be equivalent to VLANs and is subject to the same controls.

Separation of networks in the same security domain

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

VLANs can also be used to separate IP telephony traffic from data traffic at the same classification.

Controls

Using VLANs

Control: 0529; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must not
Agencies must not use VLANs between classified networks and any other network of a lower classification.

Control: 1138; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not use VLANs between a classified network and an unclassified or public network.

Control: 0535; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not
VLAN trunking must not be used on switches managing VLANs of differing security domains.

Configuration and administration

Control: 0530; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Administrative access must only be permitted from the most trusted network.

Disabling unused ports

Control: 0533; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP; Compliance: should
Unused ports on the switches should be disabled.

Control: 0534; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: must
Unused ports on the switches must be disabled.

Rationale

Using VLANs

Limiting the sharing of a common switch between VLANs of differing classifications reduces the chance of data leaks that could occur due to VLAN vulnerabilities. Furthermore, disabling trunking on switches that carry VLANs of differing security domains will also reduce the risk of data leakage across the VLANs.

Configuration and administration

When administrative access is limited to originating from the highest classified network on a switch, the risk of a data spill is reduced.

Disabling unused ports

Disabling unused ports on a switch will reduce the attack landscape from which attacks could be launched.

References

Nil.

Wireless Local Area Networks

Objective

Wireless local area networks are deployed in a secure manner that does not compromise the security of information and systems.

Context

Scope

This section describes 802.11 WLANs. It does not cover other wireless communications—these communication methods are covered in the *Communications Systems and Devices* chapter.

Controls

Providing wireless communications for public access

Control: 0536; Revision: 2; Updated: Apr-11; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies deploying a wireless network for public access must physically segregate it from all other agency networks.

Using wireless communications

Control: 0538; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not

Agencies must not use wireless networks unless the security of the wireless deployment has been approved by DSD.

Wired Equivalent Privacy

Control: 0539; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must not

Agencies must not use WEP for wireless deployments.

Wi-Fi Protected Access

Control: 0540; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not

Agencies should not use Wi-Fi Protected Access for wireless deployments.

Authentication

Control: 0541; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should use WPA2 with EAP-TLS for wireless deployments.

Control: 0542; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies not using WPA2 with EAP-TLS should use an authentication protocol that authenticates each end of the link.

Encryption

Control: 0543; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies using wireless networks to communicate classified information must use encryption to reduce the protection requirements to that for unclassified and public networks.

Pre-shared keys

Control: 1010; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies do not use pre-shared keys for wireless authentication.

Control: 1011; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended that if pre-shared keys are used, random keys of the maximum allowable length are implemented.

Management frames

Control: 1012; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies take steps to ensure the confidentiality, integrity and authenticity of 802.11 management frames.

Documentation

Control: 0544; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Key generation, distribution and rekeying procedures should be documented in a SSP for the wireless network.

Control: 0860; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Wireless device drivers and their versions should be documented in the SSP for the wireless network.

Agency devices connecting to non-agency controlled wireless networks

Control: 1081; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow agency devices to connect to non-agency controlled wireless networks.

RF controls

Control: 1013; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies limit the effective range of communications outside their area of control by:

- minimising the output power level of wireless devices
- RF shielding.

Rationale

Providing wireless communications for public access

To ensure a wireless network provided for public access cannot be used as a launching platform for further attacks, it must be segregated from all other systems.

Using wireless communications

As the accreditation authority for TOP SECRET systems, DSD has mandated that all agencies considering deploying a wireless TOP SECRET network seek approval from DSD before initiating any networking projects.

Wired Equivalent Privacy

WEP has serious flaws which allow it to be easily compromised. A WEP network should be considered equivalent to an unprotected network.

Wi-Fi Protected Access

WPA has been superseded by WPA2. Agencies are strongly encouraged to deploy WPA2 wireless networks instead of unsecured, WEP or WPA based wireless networks.

Authentication

Authenticating each end of a wireless link will prevent a range of man-in-the-middle and rogue WAP attacks.

The use of WPA2 with EAP-TLS or an evaluated VPN solution will satisfy the requirement for mutual authentication and reduce the risk of off-line brute-forcing of passwords when using pre-shared keys.

Encryption

As wireless transmissions are capable of radiating outside of secured areas into unsecured areas, they need to be encrypted to the same level as classified information communicated over cabled infrastructure in unsecured areas.

Pre-shared keys

While the use of pre-shared keys is not recommended for wireless authentication, the longer pre-shared keys are the greater the security they provide.

Management frames

Effective denial-of-service attacks can be performed on the 802.11 protocol by exploiting unprotected management frames using inexpensive commercial hardware. WPA2 provides no protection for management frames and therefore does not prevent spoofing or denial-of-service attacks.

Documentation

Wireless device driver and WAP vulnerabilities are very exposed to the threat environment and require specific attention as exploits can provide immediate unauthorised access to the network.

Agency devices connecting to non-agency controlled wireless networks

When agency devices connect to non-agency controlled wireless networks, particularly public wireless networks, the devices may be exposed to viruses, malware or other malicious code circulating on the network. If any agency device becomes infected and is later connected to an agency controlled wireless network then a crossover of viruses, malware or malicious code could occur.

RF controls

Minimising the output power of wireless devices and using RF shielding on facilities will assist in limiting the wireless communications to areas under the control of the agency.

References

Information on wireless vulnerabilities can be found at www.wve.org. This website is run by the SANS Institute, Aruba Networks, WNP and the Center for Advanced Defense Studies.

Internet Protocol Telephony

Objective

IP telephony is deployed in a secure manner that does not compromise the security of information and systems.

Context

Scope

This section describes IP telephony. Although IP telephony refers to the transport of telephone calls over IP networks, the scope of this section includes connectivity to the PSTN as well as remote sites.

Additional information on topics covered in this section can be found in the *Product Security* chapter, the *Telephone and Telephone Systems* section of the *Communications Systems and Devices* chapter, the *Gateway Security* chapter and any section relating to the protection of data networks in this manual.

IP telephony gateways

Where a gateway connects between an analogue telephone network such as the PSTN and a computer network, the *Gateways* section of the *Gateway Security* chapter does not apply.

Where a gateway connects between an IP telephony network and an IP telephony network the *Gateways* section of the *Gateway Security* chapter still applies.

Hardening Internet Protocol telephony

Voice data in an IP telephony network consists of IP packets and should not be treated any differently to other data. As such, hardening can be applied to handsets, software, servers and gateways. For example a Session Initiation Protocol server could:

- have a fully patched operating system
- have fully patched software
- run only required services
- use encrypted non-replayable authentication
- apply network restrictions that only allow secure Session Initiation Protocol and secure RTP traffic from phones on a VLAN to reach the server.

Controls

IP telephony gateways

Control: 0546; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies using IP telephony that have a requirement to implement a firewall in a gateway environment should use a voice-aware firewall that meets the same minimum level of assurance as specified for normal firewalls.

Protecting IP telephony signalling and data

Control: 0547; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should protect IP telephony signalling and data to ensure confidentiality, integrity, availability, authenticity and non-replayability.

Establishment of secure IP telephony signalling and data

Control: 0548; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should ensure that IP telephony functions can only be established using the secure signalling and data protocols.

Local area network traffic separation

Control: 0549; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P; Compliance: should
Agencies should either physically or logically separate the IP telephony traffic from other data traffic.

Control: 0550; Revision: 0; Updated: Sep-08; Applicability: C, S/HP, TS; Compliance: must
Agencies must either physically or logically separate the IP telephony traffic from other data traffic.

VoIP phone setup

Control: 0551; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
Agencies should:

- configure VoIP phones to authenticate themselves to the call controller upon registration
- disable phone auto-registration and only allow a whitelist of authorised devices to access the network
- block unauthorised devices by default
- disable all unused and prohibited functionality.

Control: 0552; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must:

- configure VoIP phones to authenticate themselves to the call controller upon registration
- disable phone auto-registration and only allow a whitelist of authorised devices to access the network
- block unauthorised devices by default
- disable all unused and prohibited functionality.

Control: 1014; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: recommended
It is recommended agencies use individual logins for VoIP phones.

Call authentication and authorisation

Control: 0553; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Authentication and authorisation should be used for all actions on the IP telephony network, including:

- call setup
- changing settings
- checking voice mail.

Control: 0554; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
An encrypted and non-replayable two-way authentication scheme should be used for call authentication and authorisation.

Control: 0555; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Authentication should be enforced for:

- registering a new phone
- changing phone users
- changing settings
- accessing voice mail.

Phone to workstation connections

Control: 0556; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should not
Agencies should not connect workstations to VoIP phones unless the workstation or the phone, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between IP telephony and other data traffic.

Control: 0557; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must not
Agencies must not connect workstations to VoIP phones unless the workstation or the phone, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between IP telephony and other data traffic.

Lobby and shared area phones

Control: 0558; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Where an agency uses a VoIP phone in a lobby or shared area they should limit the phone's:

- ability to access data networks
- functionality for voice mail and directory services.

Control: 1015; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use traditional analog phones in lobby and shared areas.

Softphone usage

Control: 0559; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not use softphones.

Control: 1016; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that agencies using softphones have separate dedicated network interface cards on the host for IP telephony network access.

Control: 1017; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that agencies using softphones install a host-based firewall on workstations using softphones that only allows traffic to and from the minimum number of RTP ports required.

Workstations using softphones

Control: 1018; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use access control software to control USB ports on workstations using softphones by using the specific vendor and product identifier of the authorised phone.

Developing a denial of service response plan

Control: 1019; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies develop a denial of service response plan including:

- how to diagnose the source of the denial of service
- what actions can be taken to clear the denial of service
- how voice capability could be maintained during a denial of service.

Content of a denial of service response plan

Control: 1020; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended a denial of service response plan include monitoring and use of:

- router and switch logging and flow data
- packet captures
- proxy and call manager logs and access control lists
- IP telephony-aware firewalls and voice gateways
- network redundancy
- load balancing
- PSTN failover.

Rationale

IP telephony gateways

The use of a voice-aware firewall ensures that only voice traffic (for example, signalling and data) is allowed for a given call and that session state is maintained throughout the transaction.

Protecting IP telephony signalling and data

IP telephony voice and signalling data is more vulnerable to eavesdropping but can be easily protected with encryption. This control helps protect against denial-of-service, man-in-the-middle and call spoofing attacks made possible by inherent weaknesses in the IP telephony protocols.

When protecting IP telephony signalling and data, voice control signalling can be protected using TLS and the 'sips://' identifier to force the encryption of all legs of the connection. Similar protections are available for RTP and the Real-time Control Protocol.

Establishment of secure IP telephony signalling and data

Use of secure signalling and data protects against eavesdropping, some types of denial-of-service, man-in-the-middle and call spoofing attacks.

Local area network traffic separation

Availability and quality of service are the main drivers for logical and physical separation.

VoIP phone setup

VoIP phones need to be hardened and logically or physically separated from the data network to ensure they do not provide an easy entry point to the network for an attacker. USB ports on phones may be used to circumvent USB workstation policy while unprotected management interfaces may be used to upload malicious firmware for call recording/spoofing and entry into the data network. Unauthorised telephony devices and unauthenticated devices should be blocked by default to reduce the risk of a denial of service.

Call authentication and authorisation

This control ensures server-client mutual authentication.

Softphone usage

Softphones can introduce additional vulnerabilities into the network as they are exposed to threats from the data network via the workstation and can subsequently be used to gain access to the voice network.

Softphones typically require workstation to workstation communication on (potentially) a number of randomly assigned ports to facilitate RTP data exchange. This presents a security risk as workstations generally should be separated, using host-based firewalls that deny all connections between workstations, to make malicious code propagation inside the network difficult.

Phone to workstation connections

Availability and quality of service are the main drivers for logical and physical separation.

Lobby and shared area phones

Lobby VoIP phones are in public areas and may give an attacker an opportunity to access the internal data network (depending on separation arrangements) by replacing the phone with another device, or installing a device in-line. There is also a risk to the voice network of social engineering (since the call may appear to be internal) and data leakage from poorly protected voice mail-boxes.

Softphone usage

Separate network cards facilitate simple VLAN separation. Host-based firewalls ensure a minimal set of ports are exposed to a minimal set of workstations.

Workstations using softphones

Adding softphones to a whitelist of allowed USB devices on a workstation will assist with restricting access to only authorised devices, and allowing the SOE to maintain defences against removable media storage and other unauthorised USB devices.

Developing a denial of service response plan

Telephony is considered critical for any business and is therefore especially vulnerable to a denial of service. The guidance provided will assist in protecting against IP telephony denial-of-service attacks, signalling floods, established call teardown and RTP data floods.

Content of a denial of service response plan

An IP telephony denial of service response plan will need to address the following:

- how to identify the source of the denial of service, either internal or external (location and content of logs)
- how to minimise the effect on telephony of a denial of service of the data network (for example, Internet or internal denial of service), including separate links to other office locations for IP telephony and quality of service prioritisation
- strategies that can mitigate the denial of service (banning certain devices/IPs at the call controller and firewalls, implementing quality of service, changing VoIP authentication, changing dial-in authentication
- alternative communication options (such as personal mobile phones) that have been identified for use in case of an emergency.

References

Nil.

Email Infrastructure

Objective

Email servers are hardened and protective marking of email messages is enforced.

Context

Scope

This section describes email infrastructure security. Information on using email applications can be found in the *Email Applications* section of the *Software Security* chapter.

Controls

Blocking emails

Control: 0561; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should block:

- inbound and outbound email, including any attachments, that contain either:
  - malicious code
  - content in conflict with the email policy
  - content that cannot be identified
  - encrypted content, when that content cannot be inspected for malicious code or authenticated as originating from a trusted source
- emails addressed to internal email aliases with source addresses located from outside the domain
- all emails arriving via an external connection where the source address uses an internal domain name.

Preventing unmarked or inappropriately marked emails

Control: 1022; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended

It is recommended agencies prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the workstation.

Control: 0562; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should

Agencies should prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server.

Control: 0875; Revision: 0; Updated: Sep-09; Applicability: C, S/HP, TS; Compliance: must

Agencies must prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server.

Blocking of outbound emails

Control: 0563; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must configure systems to block any outbound emails with a protective marking indicating that the content of the email exceeds the classification of the path over which the email would be communicated.

Control: 0564; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should configure systems to log every occurrence of a blocked email.

Blocking of inbound emails

Control: 0565; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must configure email systems to reject, log and report inbound emails with protective markings indicating that the content of the email exceeds the accreditation of the receiving system.

Control: 1023; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies notify the intended recipient of any blocked emails.

Undeliverable messages

Control: 1024; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies send notification of undeliverable, bounced or blocked emails to senders that can be verified via SPF or other trusted means.

Automatic forwarding of emails

Control: 0566; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that the requirements for blocking unmarked and outbound emails are also applied to automatically forwarded emails.

Open relay email servers

Control: 0567; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should disable open email relaying so that email servers will only relay messages destined for their domains and those originating from inside the domain.

Email server maintenance activities

Control: 0568; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should perform regular email server auditing, security reviews and vulnerability analysis activities.

Centralised email gateways

Control: 0569; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should route email through a centralised email gateway.

Control: 0570; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Where backup or alternative email gateways are in place, additional email gateways should be maintained at the same standard as the primary email gateway.

Control: 0571; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Where system users send email from outside their network, an authenticated and encrypted channel must be configured to allow email to be sent via the centralised email gateway.

Email server transport encryption

Control: 0572; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must enable opportunistic TLS encryption as defined in IETF's RFC 3207 on email servers that make incoming or outgoing email connections over public infrastructure.

Sender Policy Framework

Control: 0574; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must specify their mail severs using SPF.

Control: 1151; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use SPF to verify the authenticity of incoming emails.

Control: 1152; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should block, or mark as spam, incoming emails that fail SPF checks.

DomainKeys Identified Mail

Control: 0861; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should enable DKIM signing on all email originating from their domain.

Control: 1025; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use DKIM in conjunction with SPF.

Control: 1026; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures.

Control: 1027; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies operating email distribution list software used by external senders, configure the software so that it does not break the validity of the sender's DKIM signature.

Active web addresses in emails

Control: 1057; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that email servers strip active web addresses from emails and replace them with non-active versions.

Rationale

Blocking emails

The intent of blocking specific types of emails is to reduce the likelihood of phishing emails and emails containing malicious code.

Preventing unmarked or inappropriately marked emails

Unmarked or inappropriately marked emails can be blocked at two points, the workstation or the email server. The email server is the preferred location to block emails as it is a single location, under the control of system administrators, where the requirements for the entire network can be enforced. In addition email servers can apply controls for emails generated by applications.

While blocking at the email server is considered the most appropriate control there is still an advantage in blocking at the workstation as this adds an extra layer of security and will also reduce the likelihood of a data spill occurring on the email server.

For classified systems it is important to note that all classified emails must have an appropriate classification. This requirement is described in the *Email Applications* section of the *Software Security* chapter and mirrors the requirements in the *Information Security Protocol* of the PSPF for paper-based material.

Blocking of outbound emails

Blocking an outbound email with a protective marking higher than the classification of the path over which it would be communicated stops data spills that could occur due to interception or storage of the email at any point along the path.

Agencies may remove protective markings from emails destined for private citizens and businesses once they have been approved for release from their gateways.

Blocking of inbound emails

Blocking an inbound email with a protective marking higher than the classification that the receiving system is accredited to process prevents a data spill from occurring on the receiving system.

Undeliverable messages

Undeliverable or bounce emails are commonly sent by email servers to the original sender when the email cannot be delivered, usually because the destination address is invalid. Due to the common spamming practice of spoofing sender addresses, this often results in a large amount of bounce emails being sent to an innocent third party. Sending bounces only to senders that can be verified via SPF, or other trusted means, avoids contributing to this problem and allows trusted parties to receive legitimate bounce messages.

Automatic forwarding of emails

Automatic forwarding of emails, if left unsecured, can pose a risk to the unauthorised disclosure of classified information. For example, a system user could setup a server-side rule to automatically forward all emails received on a classified Internet-connected system to their personal email account outside work. Unfortunately this would also result in all classified emails being forwarded to their personal email account.

Open relay email servers

An open relay email server (or open mail relay) is a server that is configured to allow anyone on the Internet to send emails through the server. Such configurations are highly undesirable as they allow spammers and worms to exploit this functionality.

Email server maintenance activities

Email servers perform a critical business function; as such it is important that agencies perform regular email server auditing, security reviews and vulnerability analysis activities.

Centralised email gateways

Without a centralised email gateway it is exceptionally difficult to deploy SPF, DKIM and outbound email protective markings verification.

Attackers will almost invariably avoid using the primary email server when sending malicious emails. This is because the backup or alternative gateways are often poorly maintained in terms of out-of-date blacklists and content filtering.

Email server transport encryption

Email can be intercepted anywhere between the originating email server and the destination email server. Enabling TLS on the originating and accepting email server will defeat passive attacks on the network, with the exception of cryptanalysis against email traffic. TLS encryption between email servers will not interfere with email content filtering schemes. Email servers will remain compatible with other email servers as IETF's RFC 3207 specifies the encryption as opportunistic.

Sender Policy Framework

SPF aids in the detection of spoofed email server address domains. The SPF record specifies a list of IP addresses or domains that are allowed to send email from a specific domain. If the email server that sent the email is not in the list, the verification fails. There are a number of different fail types available.

DomainKeys Identified Mail

DKIM enables a method of determining spoofed email content. The DKIM record specifies a public key that will sign the content of the message. If the signed digest in the email header does not match the signed content of the email, the verification fails.

Active web addresses in emails

Spoofed emails often contain an active web address directing personnel to a malicious website to either illicit information or infect their workstation with malicious code. To reduce the success rate of such attacks agencies can strip active web addresses from emails and replace them with non-active versions that personnel can type or copy and paste into their web browser.

References

Further information on email security is available from the following IETF documents:

- RFC 3207, SMTP Service Extension for Secure SMTP over Transport Layer Security
- RFC 4408, Sender Policy Framework
- RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail
- RFC 4871, DomainKeys Identified Mail Signatures
- RFC 5617, DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP).

Further information on email server security can be obtained from NIST publication SP 800-45 v2, *Guidelines on Electronic Mail Security.*

Intrusion Detection and Prevention

Objective

An intrusion detection strategy is implemented for Internet-connected systems.

Context

Scope

This section describes detecting and preventing malicious code propagating through networks as well as detecting and preventing unusual or malicious activities.

Methods of infections or delivery

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
- security weaknesses in an application
- contact with an infected system or media.

Controls

Intrusion detection strategy

Control: 0575; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should

Agencies should develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDSs and host-based IDSs as necessary
- the audit analysis of event logs, including IDS logs
- a periodic audit of intrusion detection procedures
- information security awareness and training programs
- a documented IRP.

Control: 0576; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies must develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDSs and host-based IDSs as necessary
- the audit analysis of event logs, including IDS logs
- a periodic audit of intrusion detection procedures
- information security awareness and training programs
- a documented IRP
- the capability to detect cyber security incidents and attempted network intrusions on gateways and provide real-time alerts.

IDSs on gateways

Control: 0577; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies should deploy IDSs in all gateways between their networks and unsecured public networks.

Control: 1029; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies deploy IDSs at all gateways between their networks and any network they do not manage.

Control: 1028; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies locate IDSs in the gateway environment, immediately inside the outermost firewall.

Signature-based intrusion detection

Control: 0578; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
When signature-based intrusion detection is used, agencies should keep the signatures current.

Malicious code counter-measures

Control: 0579; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must:

- develop and maintain a set of policies and procedures covering how to:
  - minimise the likelihood of malicious code being introduced into a system
  - prevent all unauthorised code from executing on their networks
  - detect any malicious code installed on a system
- make their system users aware of the policies and procedures
- ensure that all instances of detected malicious code outbreaks are handled according to the procedures.

Configuring the IDS

Control: 1030; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended that in addition to defined configuration requirements, IDSs located inside a firewall be configured to generate a log entry, and an alert, for any information flows that contravene any rule in the firewall rule set.

Control: 1031; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies test IDSs rule sets prior to implementation to ensure that they perform as expected.

Event management and correlation

Control: 1032; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies deploy tools for:

- the management and archival of security event information
- the correlation of events of interest across all networks.

Host-based IDSs

Control: 1034; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies install host-based IDSs on DNS, email, web and other high value servers.

Active content blocking

Control: 1035; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use:

- filters to block unwanted content and exploits against applications that cannot be patched
- settings in the applications to disable unwanted functionality
- digital signatures to restrict active content to trusted sources only.

Rationale

Intrusion detection strategy

An IDS when configured correctly, kept current and supported by appropriate processes can be an effective way of identifying and responding to known attack profiles.

IDSs on gateways

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 generate an alert if they are detected.

Signature-based intrusion detection

When signature-based intrusion detection is used the effectiveness of the IDS will degrade over time as new intrusion methods are developed. It is for this reason that signatures for the IDS need to be kept current to identify the latest intrusion methods.

Malicious code counter-measures

Implementing policies and procedures for preventing and dealing with malicious code outbreaks enables agencies to provide consistent incident response, as well as giving clear directions to system users about what to do in the case of a cyber security incident.

Configuring the IDS

Generating alerts for information flows that contravene any rule in the firewall rule set helps security personnel respond to possible breaches of systems.

Event management and correlation

Deploying tools to manage the archival and correlation of events of interest across all networks helps identify suspicious patterns in information flows.

Host-based IDSs

Host-based IDSs use behaviour-based detection schemes and can therefore detect malicious code that has yet to be identified by antivirus vendors.

Active content blocking

Filtering unnecessary content and disabling unwanted functionality reduces the number of possible entry points that an attacker can exploit.

References

Additional information relating to intrusion detection and audit analysis is contained in HB 171:2003, *Guidelines for the Management of Information Technology Evidence.*

Internet Protocol Version 6

Objective

IPv6 is disabled until it is ready to be deployed.

Context

Scope

This section describes IPv6 and its deployment in networks. Where this manual specifies requirements for network devices, the requirements apply equally whether deploying IPv6 or IPv4.

Controls

Use of dual-stack functionality

Control: 0521; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies not using IPv6, but which have deployed dual-stack network devices, ICT equipment or operating systems that support IPv6, must disable the functionality.

Using IPv6

Control: 0523; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies using IPv6 must conduct a security risk assessment on any security risks that could be introduced as a result of running a dual stack environment or transitioning completely to IPv6.

Introducing IPv6 in gateways

Control: 0524; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should

Agencies deploying IPv6 in their gateways should undergo reaccreditation.

Enabling IPv6 in gateways

Control: 0525; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies enabling IPv6 in their gateways must undergo reaccreditation.

Rationale

Use of dual-stack functionality

In order to reduce the risk of attack to their systems, agencies need to disable unused services and functions in network devices, ICT equipment and operating systems. This includes dual-stack functionality if it is not being used.

Using IPv6

The security implications around the use of IPv6 are still largely unknown and un-tested. As many of the current network protection technologies such as firewalls and IDSs do not currently support IPv6, agencies choosing to implement IPv6 face a significant risk of being compromised.

Introducing IPv6 in gateways

Introducing IPv6 in gateways introduces a significant number of new security risks. Undergoing reaccreditation when IPv6 is introduced will ensure that any IPv6 functionality that is not intended to be used cannot be exploited by an attacker before appropriate security measures have been put in place.

Enabling IPv6 in gateways

Once agencies have completed the transition to a dual-stack environment or completely to an IPv6 environment, reaccreditation will assist in ensuring that the associated security measures for IPv6 are working effectively.

References

A Strategy for the Transition to IPv6 for Australian Government agencies can be found on the AGIMO website at www.finance.gov.au/e-government/infrastructure/internet-protocol-version-6.html.

Additional IPv6 information can be found at:

- www.nsa.gov/ia/guidance/security_configuration_guides/IPv6.shtml
- www.cpni.gov.uk/Products/technicalnotes/3008.aspx.

Data Transfers

Objective

Data is transferred between systems in a controlled and accountable manner.

Context

Scope

This section describes data transfers between systems. It applies equally to data transfers using removable media and to data transfers via gateways. Additional requirements for data transfers using removable media can be found in the *Media Usage* section of the *Media Security* chapter while additional requirements for data transfers via gateways can be found in the *Data Import and Export* section of the *Gateway Security* chapter.

Controls

System user responsibilities

Control: 0661; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure that system users transferring data to and from a system are held accountable for the data they transfer.

Data transfer processes and procedures

Control: 0662; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should

Agencies should ensure that data transfers are performed in accordance with processes and procedures approved by the accreditation authority.

Control: 0663; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies must ensure that data transfers are performed in accordance with processes and procedures approved by the accreditation authority.

Data transfer authorisation

Control: 0664; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies must ensure that all data transferred to a system of a lesser classification is approved by a trusted source.

Trusted sources

Control: 0665; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Trusted sources must be:

- a strictly limited list derived from business requirements and the result of a security risk assessment
- approved by the accreditation authority.

Import of data

Control: 0657; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: must

Agencies importing data to a system must ensure that the data is scanned for malicious and active content.

Control: 0658; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies importing data to a system must implement the following controls:

- scanning for malicious and active content
- data format checks
- log of each event
- monitoring to detect overuse/unusual usage patterns.

Export of highly formatted textual data

Control: 0669; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

When exporting formatted textual data with no free-text fields and all fields have a predefined set of permitted values, agencies must implement the following controls:

- protective marking checks
- log of each event
- monitoring to detect overuse/unusual usage patterns.

Export of other data

Control: 0670; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

When exporting data, other than highly formatted textual data, agencies must implement the following controls:

- protective marking checks
- log of each event
- monitoring to detect overuse/unusual usage patterns
- data format checks
- limitations on data types
- keyword searches
- size limits.

Preventing export of AUSTEO and AGAO data to foreign systems

Control: 0678; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must:

- ensure keyword searches are performed on all textual data
- ensure any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator
- develop procedures to prevent AUSTEO and AGAO information in both textual and non-textual formats from being exported.

Rationale

System user responsibilities

When system users transfer data to or from a system they need to be aware of the potential consequences of their actions. This could include data spills of classified information onto systems not accredited to handle the classification of the data, or the unintended introduction of malicious code to a system. Accordingly personnel need to be held accountable for all data transfers that they make.

Data transfer processes and procedures

Personnel can help prevent cyber security incidents by:

- checking protective markings to ensure that the destination system is appropriate for the classification of the data being transferred
- performing antivirus checks on data to be transferred to and from a system
- following all processes and procedures for the transfer of data.

Data transfer authorisation

Having a trusted source approve transfers from a classified system to another system of a lesser classification ensures appropriate oversight of the activity.

Trusted sources

Trusted sources include security personnel such as the CISO, the ITSA, ITSMs and ITSOs.

Import of data

Scanning imported data for malicious content reduces the risk of a system or network being infected, thus allowing the continued confidentiality, integrity and availability of the system or network.

Format checks provide a method to prevent known malicious formats from entering the system or network. Keeping and regularly auditing these logs allow for the system or network to be checked for any unusual usage.

Export of highly formatted textual data

When highly formatted textual data with no free-text fields is transferred between systems the checking requirements are lessened due to the strongly defined format of the information.

Export of other data

As data that it is not highly formatted textual data cannot be checked in an automated manner, a number of checking measures are needed to ensure that classified information is not accidentally transferred to a system not authorised to handle it or into the public domain.

Preventing export of AUSTEO and AGAO data to foreign systems

In order to reduce the risk of spilling data with a caveat onto foreign systems, it is important that procedures are developed to detect AUSTEO and AGAO data and to prevent it from crossing into foreign systems.

References

Nil.

Peripheral Switches

Objective

An evaluated peripheral switch is used when sharing keyboards, monitors and mice between different systems.

Context

Scope

This section describes the use of keyboard/video/mouse switches.

Peripheral switches with more than two connections

If the peripheral switch has more than two systems connected to it then the level of assurance needed is determined by the highest and lowest of the classifications involved.

Controls

Peripheral switches

Control: 0591; Revision: 2; Updated: Nov-10; Applicability: IC, R/P; Compliance: must
Agencies accessing a classified system and an unclassified or public system via a peripheral switch must use an EAL2 product from DSD’s EPL.

Control: 0593; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies accessing a classified system and a less classified system or an unclassified or public system via a peripheral switch must use a high assurance product from DSD’s EPL.

Peripheral switches for AUSTEO and AGAO systems

Control: 0594; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies accessing a system containing AUSTEO or AGAO information and a system of the same classification that is not accredited to process the same caveat should use an EAL2 product from DSD’s EPL.

Rationale

Peripheral switches

When accessing multiple systems through a peripheral switch it is important that sufficient assurance is available in the operation of the switch to ensure that information does not accidently pass between the connected systems.

Peripheral switches for AUSTEO and AGAO systems

As AUSTEO and AGAO systems are particularly sensitive additional security measures need to be put in place when connecting them to other systems.

References

Nil.

Gateway Security

Gateways

Objective

Gateways facilitate secure information transfers between systems from different security domains.

Context

Scope

This section describes the use of gateways and cross domain solutions.

Gateways act as information flow control mechanisms at the network layer. Gateways may also control information at the transport, session, presentation and application layers of the OSI model. Cross domain solutions provide information flow control mechanisms at each layer of the OSI model with a higher level of assurance than typical gateways. This section is equally applicable to both typical gateways and cross domain solutions.

Additional information relating to topics covered in this section can be found in the following chapters:

- *System Accreditation*
- *Physical Security for Systems*
- *Access Control*
- *Network Security*
- *Gateway Security.*

Deploying gateways

This section describes a baseline for deploying gateways. Agencies need to consult additional sections of this manual depending on the specific type of gateways deployed.

For devices used to control data flow in bi-directional gateways the *Firewalls* section of this chapter needs to be consulted.

For devices used to control data flow in uni-directional gateways the *Diodes* section of this chapter needs to be consulted.

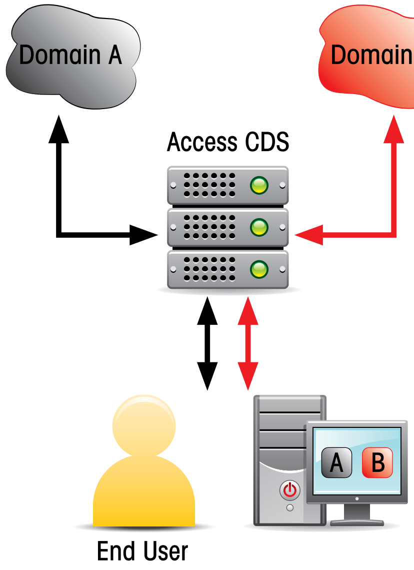
For both bi-directional and uni-directional gateways the *Data Transfers* section of the *Network Security* chapter and the *Data Import and Export* section of this chapter need to be consulted for requirements on appropriately controlling data flows.

The requirements in this manual for content filtering, data import and data export apply to all types of gateways.

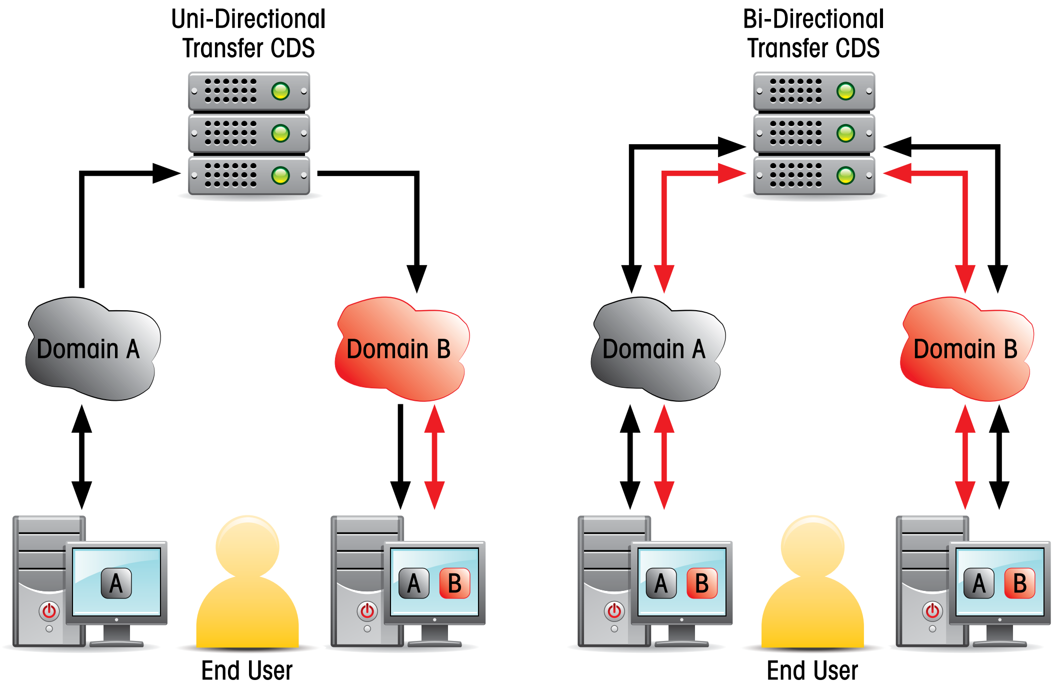
Types of gateways

This manual defines three types of gateways: access gateways, multilevel gateways and transfer gateways.

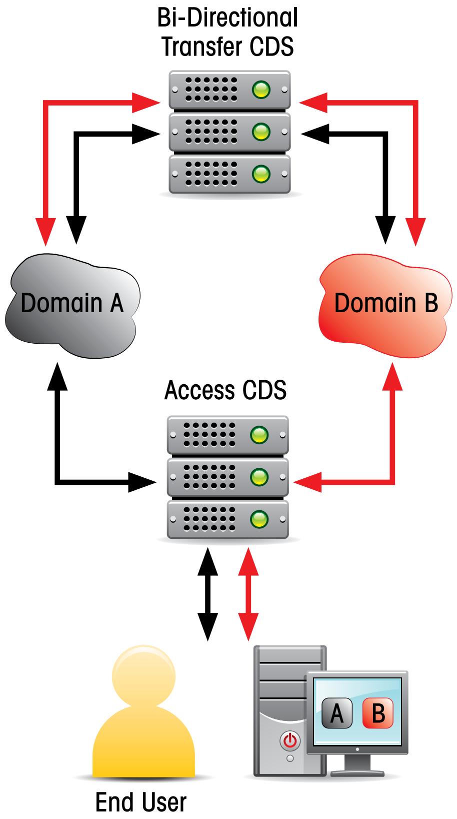
An access gateway provides the system user with access to multiple security domains from a single device.



A transfer gateway facilitates the transfer of information, in one (uni-directional) or multiple (bi-directional) directions between different security domains. A typical gateway to the Internet is considered a form of transfer gateway.



A multilevel gateway enables access, based on authorisations, to data at multiple classifications and releasability levels.



Applying the controls

For the purposes of this section, the gateway assumes the highest classification of the connected security domains.

Controls

Allowable gateways

Control: 0626; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies connecting a TOP SECRET, SECRET/HIGHLY PROTECTED or CONFIDENTIAL network to any other network from a different security domain must implement a cross domain solution.

Implementing gateways

Control: 0597; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

When deploying a cross domain solution agencies must consult with DSD and comply with all directions provided.

Control: 0627; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

Agencies connecting a typical gateway and a cross domain solution to a common network must consult with DSD on the impact to the security of the cross domain solution and comply with all directions provided.

Using gateways

Control: 0628; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that:

- all systems are protected from systems in other security domains by one or more gateways
- all gateways contain mechanisms to limit data flow at network and content levels to only the information necessary for business purposes
- all gateway components are physically located in an appropriately secured server room.

Control: 0629; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
For gateways between networks in different security domains, any shared components must be managed by the system owners of the highest security domain or by a mutually agreed party.

Configuration of gateways

Control: 0631; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that gateways:

- are the only communications paths into and out of internal networks
- by default, deny all connections into and out of the network
- allow only explicitly authorised connections
- are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network)
- provide sufficient logging and audit capabilities to detect cyber security incidents and attempted intrusions
- provide real-time alerts.

Operation of gateways

Control: 0634; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that all gateways connecting networks in different security domains:

- include a firewall on all gateways to filter and log network traffic attempting to enter the gateway
- are configured to save event logs to a separate secure log server
- are protected by authentication, logging and audit of all physical access to gateway components
- have all controls tested to verify their effectiveness after any changes to their configuration.

Separation of data flows

Control: 0635; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must ensure that all bi-directional gateways between TOP SECRET, SECRET/HIGHLY PROTECTED or CONFIDENTIAL networks and any other network have separate upward and downward network paths using a diode, content filtering and physically separate infrastructure for each path.

Demilitarised zones

Control: 0637; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use demilitarised zones to house systems accessed externally and mediate external access to information held on internal systems.

Security risk assessment

Control: 0598; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must perform a security risk assessment on gateways and their configuration before their implementation.

Security risk transfer

Control: 0605; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
All owners of systems connected via a gateway must understand and accept the residual security risk of the gateway and from any connected security domains including those connected via a cascaded connection.

Control: 1041; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies annually review the security architecture of the gateway and security risks of all connected security domains including those connected via a cascaded connection.

Information stakeholders

Control: 0607; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
Once connectivity is established, system owners should become information stakeholders for all connected security domains.

Control: 0608; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Once connectivity is established, system owners must become information stakeholders for all connected security domains.

System user training

Control: 0609; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
All system users should be trained on the secure use and security risks of the gateways before being granted access.

Control: 0610; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
All system users must be trained on the secure use and security risks of the gateways before being granted access.

Administration of gateways

Control: 0611; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must limit access to gateway administration functions.

Control: 0612; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that system administrators are fully trained to manage gateways by qualified trainers.

Control: 0613; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that all system administrators of gateways that process AUSTEO or AGAO information meet the nationality requirements for these caveats.

Control: 0616; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
Agencies should separate roles for the administration of gateways (for example, separate network and security policy configuration roles).

Control: 0617; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must separate roles for the administration of gateways (for example, separate network and security policy configuration roles).

System user authentication

Control: 0619; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must authenticate system users to all classified networks accessed through gateways.

Control: 0620; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure that only system users authenticated and authorised to a gateway can use the gateway.

Control: 1039; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use multi-factor authentication for access to networks and gateways.

ICT equipment authentication

Control: 0622; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should authenticate ICT equipment (for example, by media access control address) to networks accessed through gateways.

Configuration control

Control: 0624; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should
Agencies should limit changes to gateways after installation.

Control: 0625; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must limit changes to gateways after installation.

Testing of gateways

Control: 1037; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: recommended
It is recommended agencies ensure that testing of security measures is performed at random intervals no more than six months apart.

Rationale

Allowable gateways

Due to the security risks associated with connecting systems to the Internet, highly classified systems are prohibited from being allowed to directly connect to the Internet unless via a cross domain solution. Additionally, if an agency wishes to connect a highly classified system to a lesser classified system the connection needs to be via a cross domain solution.

Implementing gateways

It is recommended that cross domain solutions implement products that have completed a high assurance evaluation. DSD's EPL includes products that have been evaluated in the high assurance scheme. The EPL is not an exhaustive list of products which are suitable for use in cross domain solutions. Cross domain solutions are not listed on the EPL. DSD can provide guidance on the implementation of a cross domain solution in response to a formal request for advice and assistance.

Connecting multiple sets of gateways and cross domain solutions increases the threat surface and, consequently, the likelihood and consequence of a network compromise. When a gateway and a cross domain solution share a common network, it opens the higher classified networks to exploitation from the lower classified networks, which may include the Internet. DSD will be able to provide the necessary adjustments to the security controls of one or more of these connections to maintain adequate protection of networks connected through the cross domain solution.

Using gateways

Physically locating all gateway components inside a server room reduces the risk of unauthorised access to the device.

The system owner of the higher security domain of connected security domains would be most familiar with the controls required to protect the more sensitive information and as such is best placed to manage any shared components of gateways. However, in some cases where multiple security domains from different agencies are connected to a gateway it may be more appropriate to have a qualified third party manage the gateway on behalf of all connected agencies.

Configuration of gateways

Given the criticality of gateways in controlling the flow of information between security domains, any failure, particularly at the higher classifications may have serious consequences. Hence mechanisms for alerting personnel to situations that may cause cyber security incidents are especially important for gateways.

Operation of gateways

Providing a sufficient logging and audit capability helps detect cyber security incidents and attempted network intrusions, allowing the agency to implement counter-measures to reduce the risk of future attempts.

Storing event logs on a separate secure log server increases the difficulty for attackers to delete logging information in an attempt to destroy evidence of their attack.

Separation of data flows

Gateways connecting highly classified systems to other potentially Internet-connected systems need to implement diodes, content filtering and physically separate paths to provide stronger control of information flows. Such gateways are generally restricted to highly-structured formal messaging traffic.

Demilitarised zones

Demilitarised zones are used to prevent direct access to information and systems on internal networks. Agencies that require certain information and systems to be accessed from the Internet can place them in the less trusted demilitarised zone instead of on internal networks.

Security risk assessment

Performing a security risk assessment on the gateway and its configuration before its implementation assists in the early identification and mitigation of security risks.

Security risk transfer

Gateways can connect networks in different security domains including across agency boundaries. As a result, all system owners must understand and accept the security risks from all other networks before gateways are implemented.

Information stakeholders

As changes to a security domain connected to a gateway potentially affects the security posture of other connected security domains, system owners need to become stakeholders in other security domains to which they are connected via a gateway.

System user training

It is important that system users know how to use gateways securely. This can be achieved through appropriate training before being granted access.

Administration of gateways

Application of role separation in administration protects against security risks posed by a malicious system user with extensive access to gateways.

System user authentication

Authentication to networks as well as gateways can reduce the risk of unauthorised access and provide audit capability to support the investigation of cyber security incidents.

ICT equipment authentication

Authenticating ICT equipment to networks accessed through gateways assists in preventing unauthorised ICT equipment connecting to a network.

Configuration control

To avoid unnecessary changes that could introduce vulnerabilities into a gateway, agencies are strongly recommended to avoid changes to a gateway once it has been installed.

Testing of gateways

Testing security measures on gateways assists in ensuring that the integrity of the gateway is being maintained. Testing at irregular intervals is recommended since if an attacker is aware of any regular testing activities they may cease any malicious activities during the known testing period to avoid detection.

References

Additional information on implementing a cross domain solution can be accessed from the OnSecure website at members.onsecure.gov.au in the *Guide to Secure Configuration of Cross Domain Solutions* publication.

Data Import and Export

Objective

Data is transferred through gateways in a controlled and accountable manner.

Context

Scope

This section describes the requirements for the movement of data between systems via gateways. Fundamental requirements of data transfers between systems can be found in the *Data Transfers* section of the *Network Security* chapter.

Controls

Import of data through gateways

Control: 1156; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: must

Agencies importing data to a system must ensure that the data is scanned for malicious and active content.

Control: 1042; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: recommended

It is recommended agencies convert data being imported at gateways into another format before entering the network.

Control: 0659; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

When importing data to a system through gateways, the data must be filtered by a product specifically designed for that purpose.

Control: 0660; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

When importing data to a system through gateways, full or partial audits of the event logs must be performed at least monthly.

Export of data through gateways

Control: 0667; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: should

Agencies should restrict the export of data to a system of a lesser classification by filtering data using at least protective marking checks.

Export of highly formatted textual data through gateways

Control: 0671; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

When the export of highly formatted textual data occurs through gateways, agencies must implement:

- data filtering performed by a product specifically designed for that purpose
- data range checks
- full or partial audits of the event logs performed at least monthly.

Export of other data through gateways

Control: 0672; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must

When exporting data, other than highly formatted textual data, through gateways, agencies must implement data filtering performed by a product specifically designed for that purpose.

Control: 0673; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should

When the export of other data occurs through gateways agencies should perform audits of the complete data transfer logs at least monthly.

Control: 0674; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
When agencies do not perform audits of the complete data transfer logs at least monthly they must perform randomly timed audits of random subsets of the data transfer logs on a weekly basis.

Preventing export of AUSTEO and AGAO data to foreign systems

Control: 1077; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
To prevent the export of AUSTEO and AGAO data to foreign systems, agencies must implement data filtering performed by a product specifically designed for that purpose.

Requirement to sign exported data

Control: 0675; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
If, to reach the transfer point, the data is communicated over a network to which personnel or systems that are not trusted sources have access, then a trusted source must sign the data to be exported.

Control: 0676; Revision: 1; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should
Agencies should use an EAL4 product from DSD's EPL that has completed a DCE to perform data signing and signature confirmation.

Control: 0677; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must ensure that the gateway confirms the signature before the release of the data to be exported.

Rationale

Import of data through gateways

To ensure the continued functioning of systems it is important to constantly analyse data being imported over a network.

Translating data from one format into another effectively destroys most malicious active content.

Export of data through gateways

To ensure the continued integrity and confidentiality of data on a network, data must pass through a series of checks before it is exported onto systems of a lesser classification.

Export of highly formatted textual data through gateways

The security risks of releasing higher classified data are partially reduced when the data is restricted to highly formatted textual data. In such cases the data is less likely to contain hidden data and have classified content. Such data can be automatically scanned through a series of checks to detect classified content. In addition, security risk is further reduced when there is a gateway filter that refuses to export data classified above the classification of the network outside the gateway, and when logs are regularly reviewed to detect unusual usage or overuse.

Export of other data through gateways

Textual data which is not highly formatted can contain hidden data as well as having a higher classification due to the aggregated content. Security risk is somewhat reduced by running additional automated checks on non-formatted data being exported in addition to those for highly formatted textual data. A human trusted source also should assess the classification of the content of the data, which cannot be interpreted by automated means.

Preventing export of AUSTEO and AGAO data to foreign systems

As AUSTEO and AGAO networks are particularly sensitive additional security measures need to be put in place when connecting them to other networks.

Requirement to sign exported data

Digitally signing data being exported to systems where there is access by non-trusted sources reduces the risk of compromising data integrity.

References

Nil.

Content Filtering

Objective

The flow of data in gateways is controlled by a content filter.

Context

Scope

This section describes the use of content filters in uni-directional or bi-directional gateways.

Controls

Limiting transfers by file type

Control: 0649; Revision: 1; Updated: Sep-09; Applicability: U, IC, R/P; Compliance: should

Agencies should strictly define and limit the types of files that can be transferred, based on business requirements and the results of a security risk assessment.

Control: 0650; Revision: 1; Updated: Sep-09; Applicability: C, S/HP, TS; Compliance: must

Agencies must strictly define and limit the types of files that can be transferred, based on business requirements and the results of a security risk assessment.

Blocking active content

Control: 0651; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: should

Agencies should block all executables and active content from being communicated though gateways.

Blocking suspicious data

Control: 0652; Revision: 0; Updated: Sep-08; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

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

Rationale

Limiting transfers by file types

The level of security risk will be determined 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 and releasability of the content
- handle compressed files appropriately.

Reducing allowed file types reduces the number of potential vulnerabilities available for an attacker to exploit.

Blocking active content

Many files are executable and are potentially harmful if activated by a system user.

Many static file type specifications allow active content to be embedded in the file, which increases the attack surface.

Blocking suspicious data

The definition of suspicious content will depend on the system's security risk profile and what is considered normal traffic. The table below identifies some filtering techniques that can be used to identify suspicious data.

TECHNIQUE	PURPOSE
Antivirus scan	Scans the data for viruses and other malicious code.
Data format check	Inspects data to ensure that it conforms to expected/permitted formats.
Data range check	Checks the data in each field to ensure that it falls within the expected/ permitted range.
Data type check	Inspects each file header to determine the actual file type.
File extension check	Inspects the file name extension to determine the purported file type.
Keyword search	Searches data for keywords or 'dirty words' that could indicate the presence of classified or inappropriate material.
Metadata check	Inspects files for metadata that should be removed prior to release.
Protective marking check	Validates the protective marking of the data to ensure that it complies with the permitted classifications and caveats.
Visual inspection	The manual inspection of data for suspicious content that an automated system could miss, which is particularly important for the transfer of image files.

References

Nil.

Firewalls

Objective

Networks connected to bi-directional gateways implement firewalls and traffic flow filters.

Context

Scope

This section describes filtering requirements for bi-directional gateways between networks of different security domains.

When a control specifies a requirement for a diode or filter the appropriate information can be found in the *Diodes* and *Content Filtering* sections of this chapter. Additional information that also applies to topics covered in the section can be found in the *Data Transfers* section of the *Network Security* chapter and the *Data Import and Export* section of this chapter.

Controls

Firewalls

Control: 0639; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must use a firewall from DSD's EPL, as shown in the table below, in their gateway when connecting a network to another network in a different security domain.

YOUR NETWORK	THEIR NETWORK	YOU REQUIRE	THEY REQUIRE
UNCLASSIFIED	Public	Traffic flow filter	Not applicable
	UNCLASSIFIED	Traffic flow filter	Traffic flow filter
	IN-CONFIDENCE	Traffic flow filter	EAL2 firewall
	RESTRICTED/PROTECTED	Traffic flow filter	EAL4 firewall
	CONFIDENTIAL	Traffic flow filter	Consultation with DSD
	SECRET/HIGHLY PROTECTED	Traffic flow filter	Consultation with DSD
	TOP SECRET	Traffic flow filter	Consultation with DSD
IN-CONFIDENCE	Public	EAL2 firewall	Not applicable
	UNCLASSIFIED	EAL2 firewall	Traffic flow filter
	IN-CONFIDENCE	Traffic flow filter	Traffic flow filter
	RESTRICTED/PROTECTED	Traffic flow filter	EAL4 firewall
	CONFIDENTIAL	Traffic flow filter	Consultation with DSD
	SECRET/HIGHLY PROTECTED	Traffic flow filter	Consultation with DSD
	TOP SECRET	Traffic flow filter	Consultation with DSD

Continued on next page

YOUR NETWORK	THEIR NETWORK	YOU REQUIRE	THEY REQUIRE
RESTRICTED/ PROTECTED	Public	EAL4 firewall	Not applicable
	UNCLASSIFIED	EAL4 firewall	Traffic flow filter
	IN-CONFIDENCE	EAL4 firewall	Traffic flow filter
	RESTRICTED/PROTECTED	EAL2 firewall	EAL2 firewall
	CONFIDENTIAL	EAL2 firewall	Consultation with DSD
	SECRET/HIGHLY PROTECTED	EAL2 firewall	Consultation with DSD
	TOP SECRET	EAL2 firewall	Consultation with DSD
CONFIDENTIAL	Public	Consultation with DSD	Not applicable
	UNCLASSIFIED	Consultation with DSD	Traffic flow filter
	IN-CONFIDENCE	Consultation with DSD	Traffic flow filter
	RESTRICTED/PROTECTED	Consultation with DSD	EAL2 firewall
	CONFIDENTIAL	Consultation with DSD	Consultation with DSD
	SECRET/HIGHLY PROTECTED	Consultation with DSD	Consultation with DSD
	TOP SECRET	Consultation with DSD	Consultation with DSD
SECRET/HIGHLY PROTECTED	Public	Consultation with DSD	Not applicable
	UNCLASSIFIED	Consultation with DSD	Traffic flow filter
	IN-CONFIDENCE	Consultation with DSD	Traffic flow filter
	RESTRICTED/PROTECTED	Consultation with DSD	EAL2 firewall
	CONFIDENTIAL	Consultation with DSD	Consultation with DSD
	SECRET/HIGHLY PROTECTED	Consultation with DSD	Consultation with DSD
	TOP SECRET	Consultation with DSD	Consultation with DSD
TOP SECRET	Public	Consultation with DSD	Not applicable
	UNCLASSIFIED	Consultation with DSD	Traffic flow filter
	IN-CONFIDENCE	Consultation with DSD	Traffic flow filter
	RESTRICTED/PROTECTED	Consultation with DSD	EAL2 firewall
	CONFIDENTIAL	Consultation with DSD	Consultation with DSD
	SECRET/HIGHLY PROTECTED	Consultation with DSD	Consultation with DSD
	TOP SECRET	Consultation with DSD	Consultation with DSD

Traffic flow filters

Control: 0638; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

When selecting a traffic flow filter, agencies must use at least one of the following in the order of preference as shown:

- a firewall
- a proxy
- a router with appropriate access control lists configured.

Firewalls for AUSTEO and AGAO networks

Control: 0641; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must use an EAL4 firewall from DSD's EPL between an AUSTEO or AGAO network and a foreign network in addition to the firewall between networks of different classifications or security domains.

Control: 0642; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use an EAL2 firewall from DSD's EPL between an AUSTEO or AGAO network and another Australian controlled network in addition to the firewall between networks of different classifications or security domains.

Rationale

Firewalls

Where an agency connects to another agency over the Internet both agencies need a gateway with a firewall between their network and the Internet to protect themselves from attacks that originate from the Internet.

Where an agency connects from one site to another site over public infrastructure, and no traffic is expected to originate from the public infrastructure, a gateway and firewall is not required as the infrastructure can be considered an extension of the network; however, in such cases encryption will still need to be applied to the public infrastructure between the sites.

Traffic flow filters

A firewall provides a greater degree of control over filtering requirements than a proxy, which providers a greater degree of control than a router.

Firewalls for AUSTEO and AGAO networks

As AUSTEO and AGAO networks are particularly sensitive additional security measures need to be put in place when connecting them to other networks.

References

Nil.

Diodes

Objective

Networks connected to uni-directional gateways implement diodes.

Context

Scope

This section describes filtering requirements for uni-directional gateways used to facilitate data transfers. Additional information that also applies to topics covered in the section can be found in the *Data Transfers* section of the *Network Security* chapter and the *Data Import and Export* section of this chapter.

Controls

Diodes

Control: 0643; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P; Compliance: must
Agencies must use an EAL2 diode from DSD's EPL for controlling the data flow of uni-directional gateways between classified networks and unclassified or public networks.

Control: 0645; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must use a high assurance diode from DSD's EPL for controlling the data flow of uni-directional gateways between classified networks and unclassified or public networks.

Control: 1157; Revision: 0; Updated: Nov-10; Applicability: IC, R/P; Compliance: must
Agencies must use an EAL2 diode from DSD's EPL for controlling the data flow of uni-directional gateways between classified networks of different classifications where the highest system classification is RESTRICTED/PROTECTED.

Control: 1158; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must use a high assurance diode from DSD's EPL for controlling the data flow of uni-directional gateways between classified networks of different classifications where the highest system classification is CONFIDENTIAL or above.

Diodes for AUSTEO and AGAO networks

Control: 0646; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must use an EAL4 diode from DSD's EPL between an AUSTEO or AGAO network and a foreign network at the same classification.

Control: 0647; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should use an EAL2 diode from DSD's EPL between an AUSTEO or AGAO network and another Australian controlled network at the same classification.

Volume checking

Control: 0648; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies deploying a diode to control data flow in uni-directional gateways should monitor the volume of the data being transferred.

Rationale

Diodes

A diode enforces one-way flow of network traffic thus requiring separate paths for incoming and outgoing data. This makes it much more difficult for an attacker to use the same path to both launch an attack and release the information.

Diodes for AUSTEO and AGAO networks

While diodes between networks at the same classification generally are not needed, AUSTEO and AGAO networks are particularly sensitive and additional security measures need to be put in place when connecting them to other networks.

Volume checking

Monitoring the volume of data being transferred across a diode ensures that it conforms to expectations. It can also alert the agency to potential malicious activity if the volume of data suddenly changes from the norm.

References

Nil.

Working Off-Site

Mobile Devices

Objective

Information on mobile devices is protected from unauthorised disclosure.

Context

Scope

This section describes constraints on the use of mobiles devices including: mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers, and other portable Internet-connected devices.

Treating workstations as mobile devices

When a workstation is issued for home-based work instead of a mobile device, the requirements in this section equally apply to the workstation.

Devices with multiple operating states

Some mobile devices have functionality to allow them to operate in either an unprotected state or a protected state. In such cases the mobile devices need to be handled according to the state that it is being operated in at the time.

Controls

Mobile devices usage policy

Control: 1082; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must develop a policy governing the use of mobile devices.

Control: 0687; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not

Agencies must not allow mobile devices to process or store TOP SECRET information unless explicitly approved by DSD to do so.

Personnel awareness

Control: 1083; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must advise personnel of the maximum permitted classifications for data and voice communications when using mobile devices.

Non-agency owned mobile devices

Control: 1047; Revision: 2; Updated: Nov-10; Applicability: U; Compliance: should

Non-agency owned mobile devices accessing unclassified systems should use a trusted operating environment.

Control: 0693; Revision: 2; Updated: Nov-10; Applicability: IC, R/P; Compliance: must

Non-agency owned mobile devices accessing classified systems must use a trusted operating environment that also prevents classified information being stored on the device.

Control: 0694; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must not

Agencies must not allow non-agency owned mobile devices to access classified systems.

Mobile device storage encryption

Control: 0869; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should
Agencies should encrypt information on all mobile devices using at least a DACA.

Control: 1084; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption must physically transfer the device as a classified asset in an approved secure briefcase.

Mobile device communications encryption

Control: 1085; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must
Agencies must use encryption on mobile devices communicating classified information over public network infrastructure to lower requirements to that for unclassified and public networks.

Mobile device privacy filters

Control: 1145; Revision: 0; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies apply privacy filters to the screens of mobile devices.

Disabling Bluetooth functionality

Control: 0682; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not enable Bluetooth functionality on mobile devices.

Configuration control

Control: 0862; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should control the configuration of mobile devices in the same manner as devices in the office environment.

Control: 0863; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should prevent personnel from installing or uninstalling applications on a mobile device once provisioned.

Control: 0864; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must prevent personnel from disabling security functions on a mobile device once provisioned.

Maintaining mobile device security

Control: 1049; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should
Agencies should ensure that mobile devices have security updates applied on a regular basis and are regularly tested to ensure that they are still secure.

Connecting mobile devices to the Internet

Control: 0874; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Agencies should not allow mobile devices to connect to the Internet except when temporarily connecting to facilitate the establishment of a VPN connection to a system.

Control: 0705; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must disable split tunnelling when using a VPN connection from a mobile device to connect to a system.

Paging and message services

Control: 0240; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not use paging, MMS or SMS to communicate classified information.

Emergency destruction

Control: 1050; Revision: 2; Updated: Nov-10; Applicability: IC, R/P; Compliance: recommended
It is recommended agencies develop an emergency destruction plan for mobile devices.

Control: 0700; Revision: 2; Updated: Nov-10; Applicability: IC, R/P; Compliance: should
Agencies should develop an emergency destruction plan for any mobile devices used in situations where there is a higher probability of loss or compromise.

Control: 0701; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
Agencies must develop an emergency destruction plan for mobile devices.

Control: 0702; Revision: 2; Updated: Nov-10; Applicability: C, S/HP, TS; Compliance: must
If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a mobile device, the function must be used as part of the emergency destruction procedures.

Labelling

Control: 1051; Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: recommended
It is recommended agencies use soft labelling for mobile devices when appropriate to reduce their attractiveness value.

Unauthorised use of mobile devices

Control: 1086; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: should not
Mobile devices should not be used for personal non-business use or by people other than those specifically authorised.

Rationale

Mobile devices usage policy

Since mobile devices routinely leave the office environment and the protection it affords, it is important that policies are developed to ensure that mobile devices are protected in an appropriate manner when used outside controlled facilities.

Personnel awareness

Mobile devices can have both a data and voice component capable of processing or communicating classified information. In such cases, personnel need to know the classification of information which the device has been approved to process or communicate.

Non-agency owned mobile devices

If agencies choose to allow personnel to use their personal mobile devices to access their systems they will need to ensure that the device does not present a threat to the systems and for classified systems it does not retain any classified information once a session has been completed. DSD recommends that agencies achieve this outcome through the use of a bootable DVD or USB stick running an endorsed SOE.

Mobile device storage encryption

If a mobile device does not have encryption suitable for lowering the storage and physical transfer requirements of the device to an unclassified level, agencies should attempt to use a DACA to encrypt the device.

Mobile device communications encryption

The above approach cannot be used for communicating classified information over unsecured public infrastructure. If appropriate encryption is not available the mobile device will not be approved for communicating classified information.

Mobile device privacy filters

Privacy filters can be applied to the screens of mobile devices to prevent onlookers from reading the contents off the screen of the device. This assists in mitigating security risks from shoulder surfing.

Disabling Bluetooth functionality

As Bluetooth provides little security for the information that is passed between devices it must not be used on mobile devices.

Configuration control

Poorly controlled devices are more vulnerable to compromise and provide an attacker with a potential access point into systems. Although agencies may initially provide a secure device, the state of security may degrade over time. The security of devices needs to be audited regularly to ensure their integrity.

Maintaining mobile device security

It is important that mobile devices are routinely returned so that patches can be applied and they can be tested to ensure that they are still secure.

Connecting mobile devices to the Internet

During the time a device is connected to the Internet for Web browsing, instead of establishing a VPN connection to a system, it is directly exposed to attacks originating from the Internet. Should Web browsing be needed, system users should establish a VPN connection and browse the Web though their Internet gateway.

A split tunnel VPN can allow access to systems from another network, including unsecured networks such as the Internet. If split tunnelling is not disabled there is an increased risk that the VPN connection is susceptible to attack from such networks.

Paging and message services

As paging and message services do not appropriately encrypt information they cannot be relied upon for the communication of classified information.

Emergency destruction

Where a mobile device carries highly classified information, or where there is an increased risk of loss or compromise of the device, agencies need to develop emergency destruction procedures. Such procedures should focus on destroying information on the mobile device and not necessarily the device itself if it can be avoided. Many mobile devices used for highly classified information achieve this through the use of a cryptographic key zeroise or sanitisation function.

Labelling

Agencies may wish to affix an additional label to mobile devices asking finders of lost devices to hand it in to any Australian police station, or if overseas, an Australian embassy, consulate or high commission.

Unauthorised use of mobile devices

If mobile devices are issued to personnel for business purposes they should not be used for private purposes.

References

Nil.

Working Outside the Office

Objective

Information on mobile devices is accessed with due care in public locations.

Context

Scope

This section describes restrictions on accessing classified information using mobile devices from unsecured locations outside the office and home environments. This section does not apply to working from home; requirements relating to home-based work are outlined in the *Working From Home* section in this chapter. Further information on the use of mobile devices can be found in the *Mobile Devices* section of this chapter.

Controls

Working outside the office

Control: 0867; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must not
Agencies must not allow personnel to access or communicate classified information on mobile devices outside of secured areas unless there is a reduced chance of being overheard or having the screen of the device observed.

Control: 0866; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: should not
Agencies allowing personnel to access or communication classified information outside of the office should not allow personnel to do so in public locations (for example, public transport, transit lounges and coffee shops).

Carrying mobile devices

Control: 0870; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
Agencies must ensure mobile devices are carried in a secured state when not being actively used.

Using mobile devices

Control: 0871; Revision: 1; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
When in use mobile devices must be kept under continual direct supervision.

Travelling with mobile devices

Control: 1087; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
When travelling with mobile devices and media, personnel must retain control over them at all times, this includes not placing them in checked-in luggage or leaving them unattended for any period of time.

Control: 1088; Revision: 0; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must
If personnel are requested to decrypt mobile devices for inspection by customs personnel, or their mobile device is taken out of sight by customs personnel, then the member must report the potential compromise of information or the device to an ITSM as soon as possible.

Rationale

Working outside the office

As the security risk relating to specific targeting of mobile devices capable of processing highly classified information is high, these mobile devices cannot be used outside of facilities certified to an appropriate level to allow for their use. In addition, as agencies have no control over public locations including, but not limited to, such locations as public transport, transit lounges and coffee shops, mobile devices are not approved to process classified information as the risk of classified information being overheard or observed is considered to be too high in such locations.

Carrying mobile devices

As mobile devices used outside the office will be carried through areas not certified to process the classified information on the device, mechanisms need to be put in place to protect the information stored on them.

When agencies apply encryption to mobile devices to reduce their physical transfer requirements, the encryption protection will only be effective when the decryption function of the device has been deactivated. In most cases this will mean the mobile device will be in an unpowered state (i.e. not turned on), however, some devices are capable of deauthenticating the cryptography when it enters a locked state after a predefined timeout period. Such mobile devices can be carried in a locked state in accordance with reduced physical transfer requirements based on the assurance given in the cryptographic functions.

Using mobile devices

As mobile devices are often portable in nature and can be easily stolen it is strongly advised that personnel do not leave mobile device unattended at any time.

Travelling with mobile devices

If personnel place mobile devices or media in checked-in luggage when travelling they lose control over the devices. Such situations provide an opportunity for mobile devices to be stolen or tampered with by an attacker.

References

Nil.

Working From Home

Objective

Personnel working from home protect information in the same manner as in the office environment.

Context

Scope

This section describes information on accessing classified information from a home environment in order to conduct home-based work. When a workstation is issued for home-based work, instead of a mobile device, the requirements from the *Mobile Devices* section in this chapter equally apply to the workstation.

Controls

Physical security for the home environment

Control: 0865; Revision: 1; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure that the area in which devices are used meets the minimum physical security requirements in the *Physical Security Protocol* of the PSPF.

Securing devices in the home environment

Control: 0685; Revision: 2; Updated: Nov-10; Applicability: IC, R/P, C, S/HP, TS; Compliance: must

Agencies must ensure that when devices are not being actively used they are secured in accordance with the minimum physical security requirements in the *Physical Security Protocol* of the PSPF.

Rationale

Physical security for the home environment

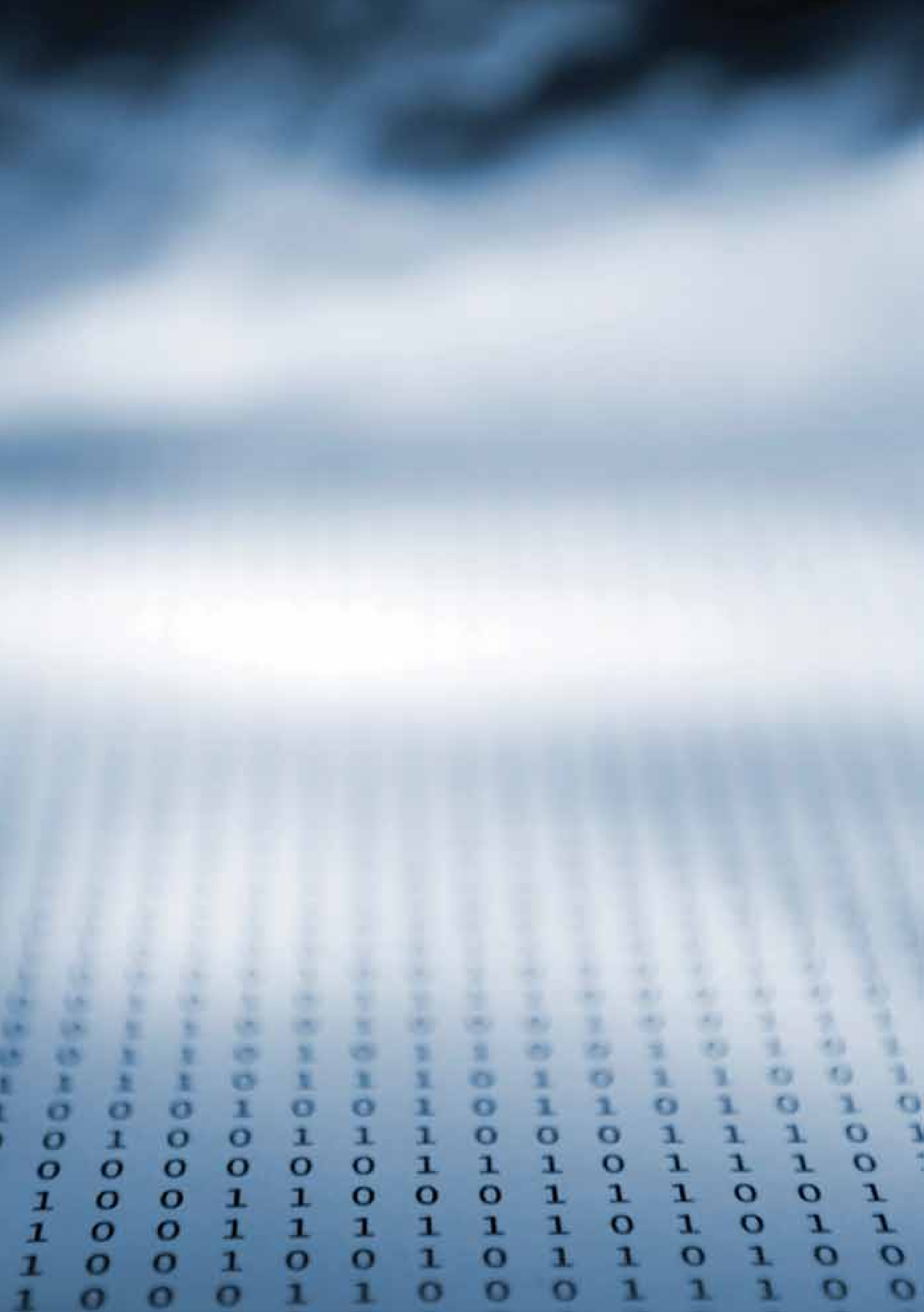
When agencies consider allowing personnel to work from a home environment they need to be aware that implementing physical security measures may require modifications to the person’s home at the expense of the agency.

Securing devices in the home environment

All devices have the potential to store classified information and therefore need protection against loss and compromise.

References

Nil.



Supporting Information

Glossaries and Index

Glossary of Abbreviations

ABBREVIATION	MEANING
3DES	Triple Data Encryption Standard
ACSI	Australian Communications Security Instruction
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AGD	Attorney-General's Department
AGIMO	Australian Government Information Management Office
AH	Authentication Header
AISEP	Australasian Information Security Evaluation Program
ANAO	Australian National Audit Office
AS	Australian Standard
ASA	agency security advisor
ASIO	Australian Security Intelligence Organisation
AUSTEO	Australian Eyes Only
CEO	chief executive officer
CIO	chief information officer
CISO	chief information security officer
COMSEC	communications security
CSER	Cyber Security Event Reporting
CSO	chief security officer
CSOC	Cyber Security Operations Centre
DACA	DSD approved cryptographic algorithm
DACP	DSD approved cryptographic protocol
DCE	DSD cryptographic evaluation
DFAT	Department of Foreign Affairs and Trade
DH	Diffie-Hellman
DIO	Defence Intelligence Organisation
DIS	Draft International Standard
DKIM	DomainKeys Identified Mail
DSA	Digital Signature Algorithm
DSD	Defence Signals Directorate
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm

EEPROM	electrically erasable programmable read-only memory
EPL	Evaluated Products List
EPLD	Evaluated Products List – Degausser
EPROM	erasable programmable read-only memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HB	handbook
HGCE	high grade cryptographic equipment
HMAC	hashed message authentication code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	information and communications technology
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM	instant messaging
IP	Internet Protocol
IPSec	Internet Protocol Security
IRC	Internet Relay Chat
IRP	incident response plan
ISAKMP	Internet Security Association Key Management Protocol
ISM	Australian Government Information Security Manual
ISO	International Organization for Standardization
ISP	information security policy
ITSA	information technology security advisor
ITSM	information technology security manager
ITSO	information technology security officer
KMP	key management plan
MFD	multifunction device
MMS	multimedia message service
NAA	National Archives of Australia
NIST	National Institute of Standards and Technology
NZS	New Zealand Standard
OECD	Organisation for Economic Co-operation and Development
OSI	Open System Interconnect
PMC	Department of Prime Minister and Cabinet
PSPF	Protective Security Policy Framework
PSTN	public switched telephone network

RAM	random access memory
RF	radio frequency
RFC	request for comments
RSA	Rivest-Shamir-Adleman
RTP	Real-time Transport Protocol
SCEC	Security Construction and Equipment Committee
SCIF	secure compartmented intelligence facility
SHA	Secure Hashing Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SMS	short message service
SOE	Standard Operating Environment
SOP	standard operating procedure
SP	Special Publication
SPF	Sender Policy Framework
SRMP	security risk management plan
SSH	Secure Shell
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSP	system security plan
VLAN	virtual local area network
VoIP	Voice over Internet Protocol
VPN	virtual private network
WAP	wireless access point
WEP	Wired Equivalent Privacy
WLAN	wireless local area network
WPA2	Wi-Fi Protected Access 2
XAUTH	IKE Extended Authentication

Glossary of Terms

TERM	MEANING
802.11	The Institute of Electrical and Electronics Engineers standard defining WLAN communications.
access gateway	A gateway that provides the system user access to multiple security domains from a single device, typically a workstation.
accreditation	A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the operation of a system.
accreditation authority	The authoritative body associated with accreditation activities.
agency	Australian Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the *Public Service Act 1999.*
agency head	The government employee with ultimate responsibly for the secure operation of agency functions, whether performed in-house or outsourced.
application whitelisting	An approach in which all executables and applications are prevented from executing by default, with an explicitly defined set of executables allowed to execute.
asset	Anything of value, such as ICT equipment and software, information, personnel, documentation, reputation and public confidence.
attack surface	The amount of ICT equipment and software used in a system. The greater the attack surface the greater the chances are of an attacker finding an exploitable vulnerability.
audit	An independent review of event logs and related activities performed to determine the adequacy of current security measures, to identify the degree of conformance with established policy or to develop recommendations for improvements to the security measures currently applied.
Australasian Information Security Evaluation Program	A program under which evaluations are performed by impartial companies against the Common Criteria. The results of these evaluations are then certified by DSD, which is responsible for the overall operation of the program.
Australian Eyes Only	A caveat indicating that the information is not to be passed to or accessed by foreign nationals.
Australian Government Access Only	A caveat used by the Department of Defence and ASIO indicating the information is not to be passed to or accessed by foreign nationals, with the exception of seconded foreign nationals. Such material received in other agencies must be handled as if it were marked as AUSTEO.
Australian Government Information Security Manual	National information security policy produced by the Defence Signals Directorate that aims to provide a common approach to the implementation of security measures for information and systems across government.
Authentication Header	A protocol used for authentication in IPSec.
baseline	A release of this manual including errata and interim policy releases.

blacklist	A set of inclusive non-accepted items that confirm the item being analysed is not acceptable. It is the opposite of a whitelist which confirms that items are acceptable.
cascaded connections	Cascaded connections occur when one network is connected to another, which has a connection to a third network, and so on.
caveat	A marking that indicates that the information has special requirements in addition to those indicated by the classification. The term covers codewords, source codewords, releasability indicators and special-handling caveats.
certification	A procedure by which a formal assurance statement is given that a deliverable conforms to a specified standard.
certification authority	An official with the authority to assert that a system complies with prescribed controls in a standard.
certification report	A report generated by a certification body of a Common Criteria scheme that provides a summary of the findings of an evaluation.
chief information security officer	A senior executive who is responsible for coordinating communication between security and business functions as well as overseeing the application of controls and security risk management processes.
classification	The business impact level associated with information or a system.
classified information	Government information that requires protection from unauthorised disclosure.
classified systems	Systems that process, store or communicate classified information.
coercivity	A property of magnetic material, used as a measure of the amount of coercive force required to reduce the magnetic induction to zero from its remnant state.
Common Criteria	An International Organization for Standardization standard (15408) for information security evaluations.
Common Criteria Recognition Arrangement	An international agreement which facilitates the mutual recognition of Common Criteria evaluations by certificate producing schemes, including the Australian and New Zealand certification scheme.
communications security	The security measures taken to deny unauthorised personnel information derived from telecommunications and to ensure the authenticity of such telecommunications.
conduit	A tube, duct or pipe used to protect cables.
connection forwarding	The use of network address translation to allow a port on a network node inside a local area network to be accessed from outside the network. Alternatively, using a Secure Shell server to forward a Transmission Control Protocol connection to an arbitrary port on the local host.
consumer guide	Product specific advice concerning evaluated products can consist of findings from mutually recognised information security evaluations (such as the Common Criteria), findings from DSD internal evaluations, any recommendations for use and references to relevant policy and standards.
content filtering	The most commonly used method to filter spam. Most antivirus methods are classified as content filters too, since they scan files, binary attachments of email and Hypertext Markup Language payload.

cross domain solution	A highly trusted implementation of a gateway for high assurance applications.
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 protocol	An agreed standard for secure communication between two or more entities.
cryptographic system	A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.
cryptographic system material	Material that includes, but is not limited to, cryptographic: key, equipment, devices, documents and firmware or software that embodies or describes cryptographic logic.
cyber security	Security measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.
Cyber Security Event Reporting scheme	A scheme established by DSD to collect information on cyber security incidents that affect government systems.
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
data at rest	Information residing on media or a system that is not powered or is unauthenticated to.
data in transit	Information that is being communicated across a communication medium.
data in use	Information that has been decrypted for processing by a system.
data spill	A cyber security incident that occurs when information is transferred between two security domains by an unauthorised means. This can include from a classified network to a less classified network or between two areas with different need-to-know requirements.
declassification	A process whereby information is reduced to an unclassified state and an administrative decision is made to formally authorise its release into the public domain.
degausser	An electrical device or permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage devices.
degaussing	A process for reducing the magnetisation of a magnetic storage device to zero by applying a reverse (coercive) magnetic force, rendering any previously stored information unreadable.
delegate	A person or group of personnel to whom the authority to authorise non-compliance with requirements in this manual has been delegated by the agency head.

demilitarised zone	A small network with one or more servers that is kept separate from the core network, either on the outside of the firewall, or as a separate network protected by the firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet.
device access control software	Software that can be installed on a system to restrict access to communications ports on workstations. Device access control software can either block all access to a communications port or allow access using a whitelisting approach based on device types, manufacturer's identification, or even unique device identifiers.
Diffie-Hellman groups	A method used for specifying the modulus size used in the hashed message authentication code algorithms. Each DH group represents a specific modulus size. For example, group 2 represents a modulus size of 1024 bits.
diode	A device that allows data to flow in only one direction.
dual-stack device	A product that implements both IP version 4 and 6 protocol stacks.
emanation security	The counter-measure employed to reduce classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of RF energy, sound waves or optical signals.
emergency access	The process of a system user accessing a system that they do not hold appropriate security clearances for due to an immediate and critical emergency requirement.
emergency situation	A situation requiring the evacuation of a site. Examples include fires and bomb threats.
Encapsulating Security Payload	A protocol used for encryption and authentication in IPSec.
escort	A person who ensures that when maintenance or repairs are undertaken to ICT equipment that uncleared personnel are not exposed to information.
facility	An area that facilitates government business. For example, a facility can be a building, a floor of a building or a designated space on the floor of a building.
fax machine	A device that allows copies of documents to be sent over a telephone network.
filter	A hardware or software device that controls the flow of data in accordance with a security policy.
firewall	A network protection device that filters incoming and outgoing network data, based on a series of rules.
firmware	Software embedded in a hardware device.
flash memory media	A specific type of EEPROM.
fly lead	A lead that connects ICT equipment to the fixed infrastructure of the facility. For example, the lead that connects a workstation to a network wall socket.
foreign national	A person who is not an Australian citizen.
foreign system	A system that is not solely owned and managed by the Australian Government.

gateway	Gateways connect two or more networks from different security domains to allow access to or transfer of information according to defined security polices. Some gateways can be automated through a combination of physical or software mechanisms. Gateways are grouped into three categories: access gateways, multilevel gateways and transfer gateways. Typical gateways process information at the network layer while gateways that process information at all layers of the OSI model are often known as cross domain solutions.
general user	A system user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security.
hardware	A generic term for any physical component of information and communication technology.
hashed message authentication code algorithms	The SHA-1 hashing algorithm, combined with additional cryptographic functions, forms the HMAC algorithms of HMAC-SHA-1-96.
high grade cryptographic equipment	The equivalent to United States Type 1 cryptographic equipment.
host-based intrusion prevention system	A security device, resident on a specific host, which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities.
hybrid hard drives	Non-volatile magnetic media that use a cache to increase read and write speeds and reduce boot time. The cache is normally flash memory media or battery backed RAM.
incident response plan	A plan for responding to cyber security incidents.
information security	Security measures relating to the confidentiality, availability and integrity of information.
information security policy	A high-level document that describes how an agency protects its systems. The ISP is normally developed to cover all systems and can exist as a single document or as a set of related documents.
Information Security-Registered Assessor Program	A DSD initiative designed to register suitably qualified information security assessors to carry out specific types of security assessments.
information technology security advisor	The ITSA has responsibility for information technology security management across the agency.
information technology security manager	ITSMs are executives that act as a conduit between the strategic directions provided by the CISO and the technical efforts of ITSOs. The main responsibility of ITSMs is the administrative controls relating to information security.
information technology security officer	ITSOs are experts in administering and configuring a broad range of systems as well as analysing and reporting on information security issues. The main responsibility of ITSOs is the technical controls relating to information security.
infrared device	Devices such as mice, keyboards, pointing devices and mobile devices that have an infrared communications capability.

Internet Key Exchange Extended Authentication	Internet Key Exchange Extended Authentication is used for providing an additional level of authentication by allowing IPSec gateways to request additional authentication information from remote users. As a result, users are forced to respond with credentials before being allowed access to the connection.
IP Security	A suite of protocols for secure IP communications through authentication or encryption of IP packets as well as including protocols for cryptographic key establishment.
IP telephony	The transport of telephone calls over IP networks.
IP version 6	A protocol used for communicating over a packet switched network. Version 6 is the successor to version 4 which is widely used on the Internet. The main change introduced in version 6 is a greater address space available for identifying network devices, workstations and servers.
intrusion detection system	An automated system used to identify an infringement of security policy.
ISAKMP aggressive mode	An IPSec protocol that uses half the exchanges of main mode to establish an IPSec connection.
ISAKMP main mode	An IPSec protocol that offers optimal security using 6 packets to establish an IPSec connection.
ISAKMP quick mode	An IPSec protocol that is used for refreshing security association information.
ICT equipment	ICT equipment includes, but is not limited to, workstations, printers, photocopiers, scanners and multifunction devices.
key management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.
key management plan	A plan that describes how cryptographic services are securely deployed. 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.
limited higher access	The process of a system user accessing a system that they do not hold appropriate security clearances for, for a limited non-ongoing period of time.
lockable commercial cabinet	A cabinet that is commercially available, of robust construction and is fitted with a commercial lock.
logging facility	A facility that includes the software component which generates the event and associated details, the transmission (if necessary) of these logs and how they are stored.
malicious code	Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms.
malicious code infection	A cyber security incident that occurs when malicious code is used to infect a system. Example methods of malicious code infection include viruses, worms and Trojans.

management traffic	Traffic generated by system administrators over a network in order to control a device. This traffic includes standard management protocols, but also includes traffic that contains information relating to the management of the network.
mandatory controls	Controls in this manual with either a 'required', 'must', 'must not', 'should' or 'should not' compliance requirement.
media	A generic term for hardware that is used to store information.
media destruction	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 in which the data is stored needs to be destroyed.
media disposal	The process of relinquishing control of media when no longer required, in a manner that ensures that no data can be recovered from the media.
media sanitisation	The process of erasing or overwriting data stored on media.
multifunction devices	The class of devices that combines printing, scanning, copying, faxing or voice messaging functionality in the one device. These devices are often designed to connect to computer and telephone networks simultaneously.
multilevel gateway	A gateway that enables access, based on authorisation, to data at many classification and releasability levels where each data unit is individually marked according to its security domain.
need-to-know	The principle of telling a person only the information that they require to fulfil their role.
Network Access Control	Policies used to control access to a network and actions on a network, including authentication checks and authorisation controls.
network device	Any device designed to facilitate the communication of information destined for multiple system users. For example: cryptographic devices, firewalls, routers, switches and hubs.
network infrastructure	The infrastructure used to carry information between workstations and servers or other network devices. For example: cabling, junction boxes, patch panels, fibre distribution panels and structured wiring enclosures.
network protection device	A sub-class of network device used specifically to protect a network. For example, a firewall.
no-lone zone	An area in which personnel are not permitted to be left alone such that all actions are witnessed by at least one other person.
non-volatile media	A type of media which retains its information when power is removed.
off-hook audio protection	A method of mitigating 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 could be achieved through the use of a hold feature, mute feature, push-to-talk handset or equivalent.
official information	The combination of unclassified information and classified information.
OpenPGP Message Format	An open-source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
optional controls	Controls in this manual with a 'recommended' compliance requirement.
patch cable	A metallic (copper) or fibre optic cable used for routing signals between two components in an enclosed container or rack.

patch panel	A group of sockets or connectors that allow manual configuration changes, generally by means of connecting cables to the appropriate connector. Cables could be metallic (copper) or fibre optic.
Perfect Forward Security	Additional security for security associations in that if one security association is compromised subsequent security associations will not be compromised.
peripheral switch	A device used to share a set of peripherals between a number of computers.
privacy marking	Privacy markings are used to indicate that official information has a special handling requirement or a distribution that is restricted to a particular audience.
privileged user	A system user who can alter or circumvent system security protections. This can also apply to system users who could have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
protective marking	A marking that is applied to unofficial, unclassified or classified information to indicate the security measures, or lack thereof for unofficial information, that needs to be applied to the information to ensure that it is appropriately protected.
Protective Security Policy Framework	National protective security policy produced by the Attorney-General's Department that aims to provide a common approach to the implementation of protective security across government.
public domain information	Official information authorised for unlimited public access or circulation, such as publications and websites.
public switched telephone network	A public network where voice is communicated using analog communications.
push-to-talk	Handsets that have a button which must be pressed by the user before audio can be communicated, thus providing fail-safe off-hook audio protection.
quality of service	A process to prioritise network traffic based on availability requirements.
reaccreditation	A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the continued operation of a system.
reclassification	An administrative decision to change the security measures afforded to information based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the security measures for media containing classified information often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the security measures protecting the information.
remote access	Access to a system from a location not under the physical control of the system owner.
removable media	Storage media that can be easily removed from a system and is designed for removal.
rogue wireless access point	A WAP operating outside of the control of an agency.

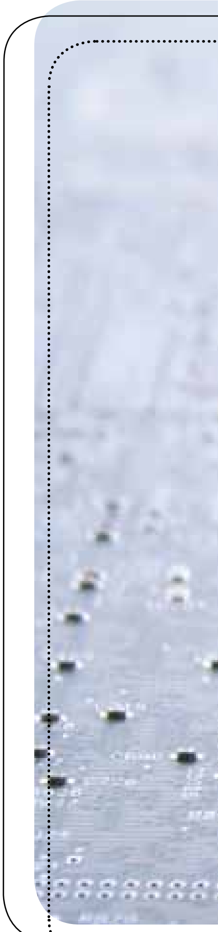
seconded foreign national	A representative of a foreign government on exchange or long-term posting.
secured space	An area that has been certified to physical security requirements as either a Secure Area, Partially Secure Area or Intruder Resistant Area to allow for the processing of classified information.
Secure Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of Multipurpose Internet Mail Extension-encoded email messages including attachments.
Secure Shell	A network protocol that can be used to securely log into a remote workstation, executing commands on a remote workstation and securely transfer files between workstations.
security association	A collection of connection-specific parameters containing information about a one-way connection in IPSec that is required for each protocol used.
security association lifetimes	The duration security association information is valid for.
Security Construction and Equipment Committee	A standing interdepartmental committee responsible for the evaluation and endorsement of security equipment for use by Australian Government agencies. The SCEC is chaired by ASIO and reports to the Protective Security Policy Committee.
security domains	A security domain is a system or collection of systems operating under a security policy that defines the classification and releasability of the information processed in the domain. It can be exhibited as a classification, a community of interest or releasability within a certain classification.
Security Equipment Catalogue	A catalogue produced by the SCEC that lists security equipment that has been tested and endorsed as meeting relevant SCEC standards.
security executive	A member of the Senior Executive Service who is responsible for protective security.
security of information arrangement	A formal arrangement between the Australian Government and a foreign government on the protection of classified information exchanged between the two parties. Details of security of information arrangements can be obtained from the Attorney-General's Department.
security posture	The level of security risk to which a system is exposed. A system with a strong security posture is exposed to a low level of security risk while a system with a weak security posture is exposed to a high level of security risk.
security risk management plan	A plan that identifies security risks and appropriate risk treatments.
security target	An artefact of Common Criteria evaluations. It contains the information security requirements of an identified target of evaluation and specifies the functional and assurance security measures offered by that target of evaluation to meet the stated requirements.
server	A computer (including mainframes) used to run programs that provide services to multiple users. For example, a file server, email server or database server.
softphone	A software application that allows a workstation to act as a VoIP phone, using either a built-in or an externally connected microphone and speaker.

software component	An element of a system, including but not limited to, a database, operating system, network or web application.
solid state drives	Non-volatile media that uses flash memory media to retain its information when power is removed and, unlike non-volatile magnetic media, contains no moving parts.
split tunnelling	Functionality that allows personnel to access both a public network and a VPN connection at the same time, such as a system and the Internet.
SSH-agent	An automated or script-based Secure Shell session.
standard operating environment	A standardised build of an operating system and associated software that is deployed on multiple devices. A SOE can be used for servers, workstations, laptops and mobile devices.
standard operating procedures	Instructions for complying with a SSP. For example, how to update virus signature files.
system	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
system owner	The person responsible for the information resource.
system classification	The classification of a system is the highest classification of information which the system is approved to store or process.
system security plan	A plan documenting the controls for a system.
system user	A general user or a privileged user of a system.
target of evaluation	The functions of a product subject to evaluation under the Common Criteria.
technical surveillance counter-measures	The process of surveying facilitates to detect the presence of technical surveillance devices and to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility.
telephone	A device that converts between sound waves and electronic signals that can be communicated over a distance.
telephone system	A system designed primarily for the transmission of voice traffic.
TEMPEST	A short name referring to investigations and studies of compromising emanations.
TEMPEST rated ICT equipment	ICT equipment that has been specifically designed to minimise TEMPEST emanations.
traffic flow filter	A device that has been configured to automatically filter and control the form of network data.
transfer gateway	A gateway that facilitates the transfer of information, in one or multiple directions (low to high or high to low), between different security domains.
transport mode	An IPSec mode that provides a secure connection between two endpoints by encapsulating an IP payload.
trusted source	A person or system formally identified as being capable of reliably producing information meeting certain defined parameters, such as a maximum data classification and reliably reviewing information produced by others to confirm compliance with certain defined parameters.
tunnel mode	An IPSec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.

unclassified information	Information that is assessed as not requiring a classification.
unclassified systems	Systems that process, store or communicate information produced by the Australian Government that does not require a classification.
unsecured space	An area that has not been certified to physical security requirements to allow for the processing of classified information.
virtual private network	The tunnelling of a network's traffic through another network, separating the VPN traffic from the underlying network. A VPN can encrypt traffic if necessary.
volatile media	A type of media, such as RAM, which gradually loses its information when power is removed.
wear levelling	A technique used in flash memory that is used to prolong the life of the media. Data can be written to and erased from an address on flash memory a finite number of times. The wear levelling algorithm helps to distribute writes evenly across each memory block, thereby decreasing the wear on the media and increasing its lifetime. The algorithm ensures that updated or new data is written to the first available free block with the least number of writes. This creates free blocks that previously contained data.
whitelist	A set of inclusive accepted items that confirm the item being analysed is acceptable. It is the opposite of a blacklist which confirms that items are not acceptable.
Wi-Fi Protected Access	Certifications of the implementations of protocols designed to replace WEP. They refer to components of the 802.11i security standard.
Wired Equivalent Privacy	A deprecated 802.11 security standard.
wireless access point	A device which enables communications between wireless clients. It is typically also the device which connects the wireless local area network to the wired local area network.
wireless communications	The transmission of data over a communications path using electromagnetic waves rather than a wired medium.
wireless local area network	A network based on the 802.11 set of standards. Such networks are often referred to as wireless networks.
workstation	A stand-alone or networked single-user computer.
X11 Forwarding	X11, also known as the X Window System, is a basic method of video display used in a variety of operating systems. X11 forwarding allows the video display from one network node to be shown on another node.

Index

NOTE: numbers in bold indicate the principal entry for a subject.



Information Security
Defence Signals Directorate

www.dsd.gov.au