1. About information security

1.1. Understanding and using this Manual

Objective

1.1.1.   The New Zealand Information Security Manual details processes and controls essential for the protection of all New Zealand Government information and systems. Controls and processes representing good practice are also provided to enhance the baseline controls. Baseline controls are minimum acceptable levels of controls and are often described as "systems hygiene".

Context

Scope

1.1.2.   This manual is intended for use by New Zealand Government departments, agencies and organisations. Crown entities, local government and private sector organisations are also encouraged to use this manual.

1.1.3.   This section provides information on how to interpret the content and the layout of content within this manual.

1.1.4.   Information that is Official Information or protectively marked UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE or RESTRICTED is subject to a single set of controls in this NZISM. These are essential or minimum acceptable levels of controls (baseline controls) and have been consolidated into a single set for simplicity, effectiveness and efficiency.

1.1.5.   All baseline controls will apply to all government systems, related services and information. In addition, information classified CONFIDENTIAL, SECRET or TOP SECRET has further controls specified in this NZISM.

1.1.6.   Where the category "All Classifications" is used to define the scope of rationale and controls in the Manual, it includes any information that is Official Information, UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET or any endorsements, releasability markings or other qualifications appended to these categories and classifications.

The purpose of this Manual

1.1.7.   The purpose of this manual is to provide a set of essential or baseline controls and additional good and recommended practice controls for use by government agencies. The use or non-use of good practice controls MUST be based on an agency's assessment and determination of residual risk related to information security.

1.1.8.   This manual is updated regularly. It is therefore important that agencies ensure that they are using the latest version of this Manual.

Target audience

1.1.9.   The target audience for this manual is primarily security personnel and practitioners within, or contracted to, an agency. This includes, but is not limited to:

- security executives;
- security and information assurance practitioners;
- IT Security Managers;
- Departmental Security Officers; and
- service providers.

Structure of this Manual

1.1.10.   This manual seeks to present information in a consistent manner. There are a number of headings within each section, described below.

- Objective – the desired outcome when controls within a section are implemented.
- Context – the scope, applicability and any exceptions for a section.
- References – references to external sources of information that can assist in the interpretation or implementation of controls.
- Rationale & Controls
    - Rationale – the reasoning behind controls and compliance requirements.
    - Control – risk reduction measures with associated compliance requirements.

1.1.11.   This section provides a summary of key structural elements of this manual. The detail of processes and controls is provided in subsequent chapters. It is important that reference is made to the detailed processes and controls in order to fully understand key risks and appropriate mitigations.

The New Zealand Government Security Classification System

1.1.12.   The requirements for classification of government documents and information are based on the **Cabinet Committee Minute EXG (00) M 20/7** and **CAB (00) M42/4G(4)**. The Protective Security Requirements (PSR) INFOSEC2 require agencies to use the NZ Government Security Classification System and the NZISM for the classification, protective marking and handling of information assets. For more information on classification, protective marking and handling instructions, refer to the Protective Security Requirements, NZ Government Security Classification System.

Key definitions

Accreditation Authority

1.1.13. The Agency Head is generally the Accreditation Authority for that agency for all systems and related services up to and including those classified RESTRICTED. See also Chapter 3 – Roles and Responsibilities and Section 4.4 – Accreditation Framework.

1.1.14. Agency heads may choose to delegate this authority to a member of the agency's executive. The Agency Head remains accountable for ICT risks accepted and the information security of their agency.

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

1.1.16. For multi-national and multi-agency systems the Accreditation Authority is determined by a formal agreement between the parties involved. Consultation with the Office of the Government Chief Digital Officer (GCDO) may also be necessary.

1.1.17. For agencies with systems that process, store or communicate NZEO or information compartmented for national security reasons, the Director-General of the GCSB is the Accreditation Authority irrespective of the classification level of that information.

Certification and Accreditation Processes

1.1.18. Certification and accreditation of information systems is the fundamental governance process by which the risk owners and agency head derive assurance over the design, implementation and management of information systems and related services provided to or by government agencies. This process is described in detail in Chapter 4 – System Certification and Accreditation.

1.1.19. Certification and Accreditation are two distinct processes.

1.1.20. Certification is the formal assertion that an information system and related services comply with minimum standards and agreed design, including any security requirements.

1.1.21. In all cases, certification and the supporting documentation or summary of other evidence will be prepared by, or on behalf of, the host or lead agency. The certification is then provided to the Accreditation Authority.

1.1.22. Accreditation is the formal authority to operate an information system and related services, and requires the recognition and acceptance of associated risk and residual risks.

1.1.23. A waiver is NOT an exception (see below). A waiver is the formal acknowledgement that a particular compliance requirement of the NZISM cannot currently be met. A waiver is granted by the Accreditation Authority on the basis that full compliance with the NZISM is achieved or compensating controls are implemented within a time specified by the Accreditation Authority. Waivers are valid in the short term only and full accreditation cannot be granted until all conditions of the waiver have been met. The need for a waiver may occur when specified controls cannot be practically implemented because of technology, resource or other serious limitations. It is essential that risk is managed through the application of specified conditions.

1.1.24. An exception is NOT a waiver (see preceding paragraph). An exception is the formal acknowledgement that a requirement of the NZISM cannot be met and that a dispensation from the particular compliance requirement is granted by the Accreditation Authority. This exception is valid for the term of the Accreditation Certificate or some lesser time as determined by the Accreditation Authority. This may occur, for example, the system is to be in use for a very short time (usually measured in hours), or the requirement cannot be met and there is no viable alternative. It is essential that any consequential risk is acknowledged and appropriate measures are taken to manage any increased risk.

1.1.25. The requirements described above are **summarised** in the table below. Care MUST be taken when using this table as there are numerous endorsements, caveats and releasability instructions in the New Zealand Government Security Classification System that may change where the authority for accreditation lies.

Information Classification	MUST and MUST NOT controls	SHOULD and SHOULD NOT controls	Accreditation Authority
Information classified ■ RESTRICTED and below, including and Official UNCLASSIFIED Information	Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high risk and mitigation is essential. If the control *cannot* be directly implemented, suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority *may* grant a Waiver or Exception from a specific requirement *if* the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be *individually* risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	Control represents good and recommended practice. Non-use may be medium to high risk. Non-use of controls is formally recorded, compensating controls selected as required and residual risk acknowledged to be within the agency's risk appetite and formally agreed and signed off by the Accreditation Authority.	Agency Head/Chief Executive/Director General (or formal delegate)

All systems or services classified 🟩 **CONFIDENTIAL and above.**	This is a baseline for any use of High Assurance Cryptographic Equipment (HACE) or the establishment of any compartments or the handling of any endorsed information (see below). The Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high or very high risk and mitigation is essential. If the control **cannot** be directly implemented and suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority **may** grant a Waiver or Exception from a specific requirement **if** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be **individually** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	This is a baseline for any use of High Assurance Cryptographic Equipment (HACE) or the establishment of any compartments or the handling of any endorsed information (See below). Control represents good and recommended practice. Non-use may be high risk Non-use of controls is formally recorded, compensating controls selected as required and residual risk formally acknowledged to be within the agency's risk appetite and agreed and signed off by the Accreditation Authority	Agency Head/Chief Executive/Director General (or formal delegate)
All use of High Assurance Cryptographic Equipment (HACE) **All systems or services with compartmented or caveated information classified** 🟩 **CONFIDENTIAL and above.**	Accreditation based on work conducted by the agency and authority to operate by the Agency Head. Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high or very high risk and mitigation is essential. If the control **cannot** be directly implemented and suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority **may** grant a Waiver or Exception from a specific requirement **if** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be **individually** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	Accreditation based on work conducted by the agency and authority to operate by the Agency Head. Control represents good and recommended practice. Non-use may be high risk Non-use of controls is formally recorded, compensating controls selected as required and residual risk formally acknowledged to be within the agency's risk appetite and agreed and signed off by the Accreditation Authority.	Director GCSB (or formal delegate)

"All Classifications" category

1.1.26. The "All Classifications" category is used to describe the applicability of controls for any information that is Official Information or protectively marked UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET, including any caveats or releasability endorsements associated with the respective document classification.

Compartmented Information

1.1.27. Compartmented information is information requiring special protection through separation or is "compartmented" from other information stored and processed by the agency.

Concept of Operations (ConOp) Document

1.1.28. Systems, operations, campaigns and other organisational activities are generally developed from an executive directive or organisational strategy. The ConOp is a document describing the characteristics of a proposed operation, process or system and how they may be employed to achieve particular objectives. It is used to communicate the essential features to all stakeholders and obtain agreement on objectives and methods. ConOps should be written in a non-technical language to facilitate agreement on understanding and knowledge and provide clarity of purpose. ConOp is a term widely used in the military, operational government agencies and other defence, military support and aerospace enterprises.

Information

1.1.29. The New Zealand Government requires information important to its functions, resources and classified equipment to be adequately safeguarded to protect public and national interests and to preserve personal privacy. Information is defined as any communication or representation of knowledge such as facts, data, and opinions in any medium or form, electronic as well as physical. Information includes any text, numerical, graphic, cartographic, narrative, or any audio or visual representation.

Information Asset

1.1.30. An information asset is any information or related equipment that has value to an agency or organisation. This includes equipment, facilities, patents, intellectual property, software and hardware. Information Assets also include services, information, and people, and characteristics such as reputation, brand, image, skills, capability and knowledge.

Information Assurance (IA)

1.1.31. Confidence in the governance of information systems and that effective measures are implemented to manage, protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Security

1.1.32. Although sometimes described as cyber security, Information security is considered a higher level of abstraction than cyber security relating to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".

1.1.33. A number of specialised security areas contribute to information security within government; these include: physical security, personnel security, communications security and information and communications technology (ICT) security along with their associated governance and assurance measures.

Information Systems

1.1.34. The resources and assets for the collection, storage, processing, maintenance, use sharing, dissemination, disposition, display, and transmission of information. This includes necessary and related services provided as part of the information system, for example; Telecommunication or Cloud Services.

Information Systems Governance

1.1.35. An integral part of enterprise governance consists of the leadership and organisational structures and processes to ensure that the agency's information systems support and sustain the agency's and Government's strategies and objectives. Information Systems Governance is the responsibility of the Agency Head and the Executive team.

Secure Area

1.1.36. In the context of the NZISM a secure area is defined as any area, room, group of rooms, building or installation that processes, stores or communicates information classified CONFIDENTIAL, SECRET, TOP SECRET or any compartmented or caveated information at these classifications. A secure area may include a SCIF (see below). The physical security requirements for such areas are specified in the Protective Security Requirements (PSR) Security Zones.

Security Posture

1.1.37. The Security Posture of an organisation describes and encapsulates the security status and overall approach to identification and management of the security of an organisation's networks, information, systems, processes and personnel. It includes risk assessment, threat identification, technical and non-technical policies, procedures, controls and resources that safeguard the organisation from internal and external threats.

Sensitive Compartmented Information Facility (SCIF)

1.1.38. Any accredited area, room, or group of rooms, buildings, or installation where Sensitive Compartmented Information (SCI) is stored, used, discussed, processed or communicated. The Accreditation Authority for a SCIF is the Director GCSB or formal delegate.

System Owner

1.1.39. A System Owner is the **person** within an agency responsible for the information resource and for the maintenance of system accreditation. This may include such outsourced services such as telecommunications or cloud. Their responsibilities are described in more detail in Section 3.4 – System Owners.

Interpretation of controls

Controls language

1.1.40. The definition of controls in this manual is based on language as defined by the Internet Engineering Task Force (IETF)'s Request For Comment (RFC) 2119 to indicate differing degrees of compliance.

Applicability of controls

1.1.41. Whilst this manual provides controls for specific technologies, not all systems will use all of these technologies. When a system is developed, the agency will determine the appropriate scope of the system and which controls within this manual are applicable.

1.1.42. If a control within this manual is outside the scope of the system then non-compliance processes *do not apply*. However, if a control is within the scope of the system yet the agency chooses *not to implement* the control, then they are required to follow the non-compliance procedures as outlined below in order to provide appropriate governance and assurance.

1.1.43. The procedures and controls described in the NZISM are designed, not only to counter or prevent known common attacks, but also to protect from emerging threats.

Identification and Selection of controls

1.1.44. In all cases controls have been selected as the most effective means of mitigating identified risks and threats. Each control has been carefully researched and risk assessed against a wide range of factors, including useability, threat levels, likelihood, rapid technology changes, sustainability, effectiveness and cost.

Controls with a "MUST" or "MUST NOT" requirement

1.1.45. A control with a "MUST" or "MUST NOT" requirement indicates that use, or non-use, of the control is essential in order to effectively manage the identified risk, unless the control is demonstrably not relevant to the respective system. These controls are baseline controls, sometimes described as systems hygiene controls.

1.1.46. The rationale for non-use of baseline controls MUST be clearly demonstrated to the Accreditation Authority as part of the certification process, before approval for exceptions is granted. MUST and MUST NOT controls take precedence over SHOULD and SHOULD NOT controls.

Controls with a "SHOULD" or "SHOULD NOT" requirement

1.1.47. A control with a "SHOULD" or "SHOULD NOT" requirement indicates that use, or non-use, of the control is considered good and recommended practice. Valid reasons for not implementing a control could exist, including:

    a. A control is not relevant in the agency;

    b. A system or ICT capability does not exist in the agency; or

    c. A process or control(s) of equal strength has been substituted.

1.1.48. While some cases may require a simple record of fact, agencies must recognise that non-use of any control, without due consideration, may increase residual risk for the agency. This residual risk needs to be agreed and acknowledged by the Accreditation Authority. In particular an agency should pose the following questions:

    a. Is the agency willing to accept additional risk?

    b. Have any implications for All-of-Government systems been considered?

    c. If, so, what is the justification?

1.1.49. A formal auditable record of this consideration and decision is required as part of the IA governance and assurance processes within an agency.

Non-compliance

1.1.50. Non-compliance is a risk to the agency and may also pose risks to other agencies and organisations. Good governance requires these risks are clearly articulated, measures are implemented to manage and reduce the identified risks to acceptable levels, that the Accreditation Authority is fully briefed, acknowledges any residual and additional risk and approves the measures to reduce risk.

1.1.51. In some circumstances, full compliance with this manual may not be possible, for example some legacy systems may not support the configuration of particular controls. In such circumstances, a risk assessment should clearly identify *compensating* controls to reduce risks to an acceptable level. Acceptance of risk or residual risk, without due consideration is NOT adequate or acceptable.

1.1.52. It is recognised that agencies may not be able to immediately implement all controls described in the manual due to resource, budgetary, capability or other constraints. Good practice risk management processes will acknowledge this and prepare a timeline and process by which the agency can implement all appropriate controls described in this manual.

1.1.53. Simply acknowledging risks and not providing the means to implement controls *does not* represent effective risk management.

1.1.54. Where multiple controls are not relevant or an agency chooses not to implement multiple controls within this manual the system owner may choose to logically group and consolidate controls when following the processes for non-compliance.

Rationale Statements

1.1.55. A short rationale is provided with each group of controls. It is intended that this rationale is read in conjunction with the relevant controls in order to provide context and guidance.

Risk management

Risk Management Standards

1.1.56. For security risk management to be of true value to an agency it MUST relate to the specific circumstances of an agency and its systems, as well as being based on an industry recognised approach or risk management guidelines. For example, guidelines and standards produced by Standards New Zealand and the International Organization for Standardization (ISO).

1.1.57. The International Organization for Standardization has published an international risk management standard, including principles and guidelines on implementation, outlined in ISO 31000:2018 - Risk Management - Guidelines. Refer to the tables below for additional reference materials.

The NZISM and Risk Management

1.1.58. The ISM encapsulates good and recommended best-practice in managing technology risks and mitigating or minimising threat to New Zealand government information systems.

1.1.59. Because there is a broad range of systems across government and the age and technological sophistication of these systems varies widely, there is no single governance, assurance, risk or controls model that will accommodate all agencies information and technology security needs.

1.1.60. The NZISM contains guidance on governance and assurance processes and technological controls based on comprehensive risk and threat assessments, research and environmental monitoring.

1.1.61. The NZISM encourages agencies to take a similar risk-based approach to information security. This approach enables the flexibility to allow agencies to conduct their business and maintain resilience in the face of a changing threat environment, while recognising the essential requirements and guidance provided by the NZISM.

References

1.1.62. **Key Standards**

Reference	Title	Publisher	Source
	The NZISM and additional information, tools and discussion topics can be accessed from the GCSB website	GCSB	https://www.gcsb.govt.nz https://www.nzism.gcsb.govt.nz
	Protective Security Requirements (PSR)	NZSIS	https://www.protectivesecurity.govt. nz

ISO/IEC 27000:2018	Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary (fifth edition)	ISO / IEC Standards NZ	https://www.iso27001security.com/html/27000.html https://www.standards.co.nz
CNSS Instruction No. 4009 6 April 2015	National Information Assurance (IA) Glossary, (US)	Committee on National Security Systems (CNSS)	https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
NISTIR 7298 Revision 3, July 2019	Glossary of Key Information Security Terms	NIST	https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final

1.1.63. **Additional Guidance**

Topic	Documentation	Source
Approved Products	Common Criteria ISO/IEC 15408, parts 1,2 & 3	ISO http://www.iso.org
	AISEP Evaluated Products List	ASD https://www.cyber.gov.au/publications/evaluated-products-list
	Other Evaluated Products Lists	NSA http://www.nsa.gov NCSC UK http://www.ncsc.gov.uk/ CSEC https://www.cse-cst.gc.ca Common Criteria https://www.commoncriteriaportal.org/products
Archiving of information	Public Records Act 2005 (as amended)	Archives New Zealand or http://www.legislation.govt.nz
	Archives, Culture, and Heritage Reform Act 2000 (as amended)	Archives New Zealand or http://www.legislation.govt.nz
Business continuity	ISO 22301:2019, Security and Resilience - Business Continuity Management Systems - Requirements	Standards New Zealand http://www.standards.govt.nz
Cable security	NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB CONFIDENTIAL document available on application to authorised personnel
Emanation security	NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB CONDFIDENTIAL document available on application to authorised personnel
Information classification	Protective Security Requirements (New Zealand Government Security Classification System Handling Requirements for protectively marked information and equipment)	NZSIS http://www.protectivesecurity.govt.nz
Information security management	ISO/IEC 27001:2013	ISO / IEC http://www.iso27001security.com/html/27001.html Standards New Zealand http://www.standards.govt.nz
	ISO/IEC 27002:2016	ISO / IEC http://www.iso27001security.com/html/27002.html Standards New Zealand http://www.standards.govt.nz
	Other standards and guidelines in the ISO/IEC 270xx series, as appropriate	ISO / IEC http://www.iso27001security.com/ Standards New Zealand http://www.standards.govt.nz

Key management – commercial grade	ISO/IEC 11770 Parts 1-6: Information Technology – Security Techniques – Key Management	ISO / IEC https://www.iso.org/standards.html Standards New Zealand http://www.standards.govt.nz
Cryptographic Security	NZCSS 300: New Zealand Communications Security Standard No 300 (Document classified RESTRICTED)	GCSB RESTRICTED document available on application to authorised personnel
Management of electronic records that may be used as evidence	ISO/IEC 27037:2012, Guidelines for Identification, Information Technology – Security Techniques - Collection, Aquisition and Preservation of Digital Evidence	ISO / IEC https://www.iso.org/standard/44381.html
Personnel security	PSR, Protective Security Requirements	NZSIS http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/personnel-security/
Physical security	PSR, Protective Security Requirements	NZSIS http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/physical-security/
Privacy requirements	Privacy Act 1993 (the Privacy Act)	Office of The Privacy Commissioner http://www.privacy.org.nz
Risk management	ISO 31000:2018 - Risk Management -- Guidelines	Standards New Zealand http://www.standards.govt.nz
	ISO 27005:2011, Information Security Risk Management	Standards New Zealand http://www.standards.govt.nz
	HB 436:2013, Risk Management Guidelines	Standards New Zealand http://www.standards.govt.nz
	ISO/IEC Guide 73, Risk Management – Vocabulary – Guidelines for use in Standards	Standards New Zealand http://www.standards.govt.nz
	NIST SP 800-30 rev. 1 - Guide for conducting Risk Assessments	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
Security Management	HB167, Security Risk Management	Standards New Zealand http://www.standards.govt.nz
Security And Intelligence Legislation	Intelligence and Security Act 2017	http://www.legislation.govt.nz
	Telecommunications (Interception Capability and Security) Act 2013 (as amended)	http://www.legislation.govt.nz

Rationale & Controls

1.1.64.   Non-compliance

1.1.64.R.01.   Rationale

Controls for classified systems and information within this manual with a "MUST" or "MUST NOT" compliance requirement **cannot** be effectively *individually* risk managed by agencies without jeopardising their own, multi-agency or All-of-Government information assurance.

1.1.64.R.02.   Rationale

Controls within this manual with a "SHOULD" and "SHOULD NOT" requirement may be risk managed by agencies. As the individual control security risk for non-compliance is not as high as those controls with a 'MUST' or 'MUST NOT' requirement, the Accreditation Authority can consider the justification for the acceptance of risks, consider any mitigations then acknowledge and accept any residual risks.

1.1.64.R.03.   Rationale

Deviations from the procedures and controls in the NZISM may represent risks in themselves. It is important that governance and assurance is supported by evidence, especially where deviations from the procedures and controls in the NZISM are accepted. In this case a formal approval or signoff by the Accreditation Authority is essential. Ultimately, the Agency Head remains accountable for the ICT risks and information security of their agency.

1.1.64.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:127]

System owners seeking a dispensation for non-compliance with any baseline controls in this manual MUST be granted a dispensation by their Accreditation Authority. Where High Assurance Cryptographic Systems (HACS) are implemented, the Accreditation Authority will be the Director-General GCSB or a formal delegate.

1.1.65.   Justification for non-compliance

1.1.65.R.01.   Rationale

Without sufficient justification and consideration of security risks by the system owner when seeking a dispensation, the agency head or their authorised delegate will lack the appropriate range of information to the make an informed decision on whether to accept the security risk and grant the dispensation or not.

1.1.65.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:131]

System owners seeking a dispensation for non-compliance with baseline controls MUST complete an agency risk assessment which documents:

- the reason(s) for not being able to comply with this manual;
- the effect on any of their own, multi-agency or All-of-Government system;
- the alternative mitigation measure(s) to be implemented;
- The strength and applicability of the alternative mitigations;
- an assessment of the residual security risk(s); and
- a date by which to review the decision.

1.1.66.   Consultation on non-compliance

1.1.66.R.01.   Rationale

When an agency stores information on their systems that belongs to a foreign government they have an obligation to inform and seek agreement from that third party when they do not apply all appropriate controls in this manual. These third parties will place reliance on the application of controls from the NZISM. If the agency fails to implement all appropriate controls, the third party will be unaware that their information may have been placed at a heightened risk of compromise. As such, the third party is denied the opportunity to consider their own additional risk mitigation measures for their information in light of the agency's desire to risk manage controls from this manual.

1.1.66.R.02.   Rationale

Most New Zealand Government agencies will store or processes information on their systems that originates from another New Zealand Government Agency. The use of the NZ Government Security Classification System, and implementation of its attendant handling instructions, provides assurance to the originating agency that the information is adequately safeguarded.

1.1.66.R.03.   Rationale

Additional controls, not described or specified in this manual, are welcomed as a means of improving and strengthening security of information systems, provided there are no obvious conflicts or contradictions with the controls in this manual. A comprehensive risk assessment of the additional controls is a valuable means of determining the effectiveness of additional controls.

1.1.66.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:137]

If a system processes, stores or communicates classified information from another agency, that agency MUST be consulted before a decision to be non-compliant with the NZ Government Security Classification System is made.

1.1.66.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:138]

If a system processes, stores or communicates classified information from a foreign government, that government MUST be consulted before a decision to be non-compliant with NZISM controls is made.

1.1.67.   All-of-Government Systems

1.1.67.R.01.   Rationale

All-of-Government systems, because they are connected to multiple agencies, have the potential to cause significant and widespread disruption should system failures, cyber-attacks or other incidents occur.

1.1.67.R.02.   Rationale

Any deviation from the baseline controls specified in the NZISM MUST be carefully considered and their implication and risk for all government systems understood and agreed by all interested parties.

1.1.67.R.03.   Rationale

Interested parties may include the lead agency, the Government CIO and key service providers, such as with cloud services.

1.1.67.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:143]

If a system processes, stores or communicates data and information with multiple agencies or forms part of an All-of-Government system, interested parties MUST be formally consulted before non-compliance with any baseline controls.

1.1.68.   Reviewing non-compliance

1.1.68.R.01.   Rationale

As part of the process of providing justification for a dispensation to the Accreditation Authority, an assessment of the degree of compliance, identification of areas of non-compliance and determination of residual security risk is undertaken by the agency or lead agency. This assessment is based on the risk environment at the time the dispensation is sought. As the risk environment will continue to evolve over time it is important that agencies revisit the assessment on an annual basis 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 of an acceptable level.

1.1.68.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:146]

Agencies SHOULD review decisions to be non-compliant with any controls at least annually.

1.1.69.   Recording non-compliance

1.1.69.R.01.   Rationale

Without appropriate records of decisions to risk manage controls from this manual, agencies have no record of the status of information security within their agency. Furthermore, a lack of such records will hinder any governance, compliance or auditing activities that may be

conducted.

1.1.69.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:151]

Agencies MUST retain a copy and maintain a record of the supporting risk assessment and decisions to be non-compliant with any baseline controls from this manual.

1.1.69.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:152]

Where good and recommended practice controls are NOT implemented, agencies MUST record and formally recognise that non-use of any controls without due consideration may increase residual risk for the agency. This residual risk MUST be agreed and acknowledged by the Accreditation Authority.

1.2. Applicability, Authority and Compliance

Objective

1.2.1.   Agencies understand and follow the requirements of the New Zealand Information Security Manual. Protection of government information and systems is a core accountability.

Context

Scope

1.2.2.   The NZISM provides guidance and specific ICT controls that form part of a suite of requirements produced by GCSB relating to information security. Its role is to promote a consistent approach to information assurance and information security across all New Zealand Government agencies. It is based on security risk assessments for any information that is processed, stored or communicated by government systems with corresponding risk treatments (control sets) to reduce the level of security risk to an acceptable level.

Applicability

1.2.3.   This manual applies to:

- New Zealand Government departments, agencies and organisations as listed in:
  - Parts 1 and 2 of Schedule 1 to the Ombudsmen Act 1975 (as amended); and
  - Schedule 1 to the Official Information Act 1982.

- any other organisations that have entered into a formal Agreement with the New Zealand Government to have access to classified information.

Authority

1.2.4.   The Intelligence and Security Act 2017 provides that one of the functions of the GCSB is to co-operate with, and provide advice and assistance to, any public authority whether in New Zealand or overseas, or to any other entity authorised by the Minister responsible for the GCSB on any matters relating to the protections, security and integrity of communications; and information structures of importance to the Government of New Zealand. The NZISM is one aspect of the GCSB's advice and assistance to government agencies on information security.

1.2.5.   This function furthers the objective of the GCSB to contribute to:

- The national security of New Zealand; and
- The international relations and well-being of New Zealand; and
- The economic well-being of New Zealand.

1.2.6.   The NZISM is intended to structure and assist the implementation of government policy that requires departments and agencies to protect the privacy, integrity and confidentiality of the information they collect, process, store and archive. While these overarching requirements are mandatory for departments and agencies, compliance with the NZISM is not required as a matter of law. The controls in the NZISM could be made binding on departments and agencies, either by legislation, or Cabinet direction.

1.2.7.   The Protective Security Requirements Framework provides a specific authority and mandate through a Cabinet Directive **CAB MIN (14) 39/38.**

Compliance by smaller agencies

1.2.8.   As smaller agencies may not always have sufficient staffing or budgets to comply with all the requirements of this manual, they may choose to consolidate their resources with another larger host agency to undertake a joint approach.

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

1.2.10. 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 information security responsibilities.

Legislation and other government policy

1.2.11. While this manual does contain examples of relevant legislation (see Tables 1.1.59 and 1.1.60), there is no comprehensive consideration of such issues. Accordingly, agencies should rely on their own inquiries in that regard.

1.2.12. All controls within this manual may be used as the basis for internal and external annual audit programmes, any review or investigation by the Controller and Auditor-General or referenced for assurance purposes by the Government Chief Digital Officer (GCDO).

Rationale & Controls

1.2.13.   Compliance

1.2.13.R.01.   Rationale

In complying with the latest version of this manual agencies awareness of the current threat environment for government systems and the associated acceptable level of security risk is vital. Furthermore, if a system is designed to an out-dated standard, agencies may need

additional effort to obtain accreditation for their systems.

1.2.13.R.02.   Rationale

GCSB continuously monitors technology developments in order to identify business risks, technology risks and security threats. If a significant risk is identified, research may be undertaken, additional controls identified and implementation timeframes specified.

1.2.13.C.01.   Control**System Classification(s): All Classifications; Compliance: MUST** [CID:177]

Agencies undertaking system design activities for in-house or out-sourced projects MUST use the latest version of this manual for information security requirements.

1.2.13.C.02.   Control**System Classification(s): All Classifications; Compliance: MUST** [CID:178]

When GCSB makes a determination that newly introduced standard, policy or guideline within this manual, or any additional information security policy, is of particular importance, agencies MUST comply with any new specified requirements and implementation timeframes.

2. Information Security within Government

2.1. Government Engagement

Objective

2.1.1.   Security personnel are aware of and use information security services offered within the New Zealand Government.

Context

Scope

2.1.2.   This section covers information on organisations involved in providing information security advice to agencies.

Government Communications Security Bureau

2.1.3.   GCSB is required to perform various functions, including the provision of material, advice and other assistance to New Zealand government departments on matters relating to the security of classified information that is processed, stored or communicated by electronic or similar means. GCSB also provides assistance to New Zealand government departments in relation to cryptography, communications and computer technologies.

2.1.4.   An agency can contact GCSB for advice and assistance relating to the implementation of the NZISM by emailing nzism@gcsb.govt.nz or phone the GCSB's Information Assurance Directorate on (04) 472-6881.

2.1.5.   An agency can contact GCSB to provide feedback on the NZISM via email as above.

2.1.6.   Agencies can also contact GCSB for advice and assistance on the reporting and management of information security incidents. GCSB's response will be commensurate with the nature and urgency of the information security incident. There is a 24 hour, seven day a week service available if necessary.

2.1.7.   Finally, agencies can contact GCSB for advice and assistance on the purchasing, provision, deployment, operation and disposal of High Assurance Cryptographic Equipment (HACE). The cryptographic liaison can be contacted by email at products.systems@gcsb.govt.nz.

Other organisations

2.1.8.   The table below contains a brief description of the other organisations which have a role in relating to information security within government.

Organisation	Services
Archives New Zealand	Provides information on the archival of government information.
Auditor General	Independent assurance over the performance and accountability of public sector organisations.
Audit New Zealand	Performance audits and better practice guides for areas including information security.
Department of Internal Affairs	Guidance on risk management, Authentication Standards, One.govt and i-govt services.
Department of Prime Minister and Cabinet	National security advice to government.
Ministry of Business, Innovation & Employment (MBIE)	Development, coordination and oversight of New Zealand Government policy on electronic commerce, online services and the Internet.
Ministry of Foreign Affairs and Trade	Policy and advice for security overseas.
National Cyber Security Centre (NCSC)	Provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.
New Zealand Police	Law enforcement in relation to electronic crime and other high tech crime.
New Zealand Security Intelligence Service	Personnel and Physical security advice Maintenance of the New Zealand Government Security Classification System.
Office of the Government Chief Information Officer (DIA)	Advice, guidance and management for sector and All-of-Government systems and ICT processes. ICT assurance (including privacy and security).

Privacy Commissioner	Advice on how to comply with the Privacy Act and related legislation.
State Services Commission	Monitoring of Public Service organisations and Chief Executives' performance.
DIA	Government Chief Privacy Office (GCPO).
NZCERT	General reporting of Cyber Security problems.

References

2.1.9. The following websites can be used to obtain additional information about the security of government systems:

Organisation		Source
Government Communications Security Bureau		https://www.gcsb.govt.nz
Archives New Zealand		https://www.archives.govt.nz
Audit New Zealand		https://www.auditnz.govt.nz
Auditor General		https://www.oag.govt.nz
Department of Internal Affairs		https://www.dia.govt.nz https://www.digital.govt.nz
Department of Prime Minister and Cabinet		https://www.dpmc.govt.nz
Ministry of Business, Innovation & Employment (MBIE)		https://www.mbie.govt.nz
Ministry of Foreign Affairs and Trade		https://www.mfat.govt.nz
National Cyber Security Centre (NCSC)		https://www.ncsc.govt.nz
New Zealand Security Intelligence Service		https://www.nzsis.govt.nz
New Zealand Police		https://www.police.govt.nz
Privacy Commissioner		https://www.privacy.org.nz
Protective Security Requirements		https://www.protectivesecurity.govt.nz
Standards NZ		https://www.standards.co.nz
State Services Commission		https://www.ssc.govt.nz

Rationale & Controls

2.1.10. Organisations providing information security services

2.1.10.R.01. Rationale

If security personnel are unaware of the role government organisations play with regards to information security they could be missing out on valuable insight and assistance in developing an effective information security posture for their agency.

2.1.10.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:199]

Security personnel SHOULD familiarise themselves with the information security roles and services provided by New Zealand Government organisations.

2.2. Industry Engagement and Outsourcing

Objective

2.2.1. Industry handling classified information implements the same security measures as government agencies.

Context

Scope

2.2.2. This section covers information on outsourcing information technology services and functions to contractors as well as providing those partners with classified information in order to undertake their contracted duties.

Cloud computing

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

PSR References

2.2.4. Additional information on third party providers is provided in the PSR.

Reference	Title	Source
PSR Mandatory Requirements	GOV4, GOV5, INFOSEC1, INFOSEC2, PERSEC1, PERSEC2, PERSEC3, and PERSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/
PSR content protocols	Management protocol for information security Management protocol for personnel security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/
PSR requirements sections	Supply chain security	https://www.protectivesecurity.govt.nz/governance/supply-chain-security/
Managing specific scenarios	Outsourcing, Offshoring and supply chains Outsourced ICT facilities	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/outsourced-ict-facilities/

Rationale & Controls

2.2.5. Outsourcing information technology services and functions

2.2.5.R.01. Rationale

In the context of this section, outsourcing is defined as contracting an outside entity to provide essential business functions and processes that could be undertaken by the Agency itself.

Outsourcing may present elevated levels of risk and additional risks. Outsourcing therefore, requires greater consideration, demonstrable governance, and higher levels of assurance before committing to such contracts.

2.2.5.R.02. Rationale

A distinction is drawn between important business functions and the purchase of services such as power, water, building maintenance, stationery and telecommunications. These services are not usually provided by the agency itself.

Purchased services, as identified above, do NOT require accreditation or a third party review as defined in the NZISM. However, normal contract due diligence should be exercised before committing to these supply contracts.

2.2.5.R.03. Rationale

Contractors can be provided with classified information as long as their systems are accredited to an appropriate classification in order to process, store and communicate that information. Contractors and all staff with access to the classified systems must also be cleared to the level of the information being processed. This ensures that when they are provided with classified information that it receives an appropriate level of protection.

2.2.5.R.04. Rationale

New Zealand, in common with most developed countries, has agreements with other nations on information exchange on a variety of topics, including arms control, border control, biosecurity, policing and national security. The lead agency in each sector will usually be the controlling agency for each agreement. While the detail and nature of these agreements is sometimes classified, the agreements invariably require the protection of any information provided, to the level determined by the originator. Agencies that receive such information will be fully briefed by the relevant controlling agency or authority, before information is provided. It is important to note that there is no single list or source of such agreements.

2.2.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:216]

Agencies engaging industry for the provision of off-site information technology services and functions MUST accredit the systems used by the contractor to at least the same minimum standard as the agency's systems. This may be achieved through a third party review report utilising the ISAE 3402 Assurance Reports on Controls at a Third Party Service Organisation.

2.2.5.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:217]

Agencies SHOULD NOT engage industry for the provision of off-site information technology services and functions in countries that New Zealand does not have a multilateral or bilateral security agreement with for the protection of classified information of the government of New Zealand. If there is any doubt, the agency's CISO should be consulted.

2.2.6. Independence of ITSMs from outsourced companies

2.2.6.R.01. Rationale

If an agency engages an organisation for the provision of information technology services and functions, and where that organisation also provides the services of an Information Technology Security Manager, they need to ensure that there is no actual or perceived conflict of interest (See also Section 3.3 - Information Technology Security Manager).

2.2.6.R.02. Rationale

When an agency engages a company for the provision of information technology services and functions having a central point of contact for information security matters within the company will greatly assist with incident response and reporting procedures.

2.2.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:221]

Where an agency has outsourced information technology services and functions, any ITSMs within the agency SHOULD be independent of the

company providing the information technology services and functions.

2.2.6.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:222]

Where an agency has outsourced information technology services and functions, they SHOULD ensure that the outsourced organisation provides a single point of contact within the organisation for all information assurance and security matters.

2.2.7. Developing a contractor management program

2.2.7.R.01. Rationale

The development of a contractor management program will assist the agency in undertaking a coordinated approach to the engagement and use of contractors for outsourcing and provision of information technology services and functions.

2.2.7.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:225]

Agencies SHOULD develop a program to manage contractors that have been accredited for the provision of off-site information technology services and functions.

2.3. Approach to Cloud Services

Objective

2.3.1. Agencies understand and manage their approach to cloud services securely, effectively and efficiently.

Context

Scope

2.3.2. This section provides guidance on approaches to cloud services.

2.3.3. It is important that agencies identify cloud systems risks and that Official Information and agency information systems are protected in accordance with Cabinet Directives, the Protective Security Requirements (PSR), the New Zealand Goverment Security Classification System, the NZISM and with other government security requirements and guidance.

2.3.4. Reference should also be made to the following sections in the NZISM:

- Chapter 4 – System Certification and Accreditation
- Chapter 5 – Information Security Documentation
- Chapter 13 – Decommissioning and Disposal
- Chapter 16 – Access Control
- Chapter 17 – Cryptography
- Chapter 19 – Gateway Security
- Chapter 20 – Data Management
- Chapter 22 – Enterprise Systems Security

2.3.5. Detailed controls for Cloud Computing are provided in Section 22.1 – Cloud Computing.

Mandates, Directives and Requirements

2.3.6. In 2012, Cabinet directed government agencies to adopt public cloud services in preference to traditional IT systems. Offshore-hosted office productivity services were excluded **[CAB Min (12) 29/8A]**

2.3.7. In August 2013, the Government introduced their approach to cloud computing, establishing a 'cloud first' policy and an All-of-Government direction to cloud services development and deployment. This is enabled by the Cabinet Minute **[CAB Min (13) 37/6B]**. Under the 'cloud first' policy state service agencies are expected to adopt approved cloud services either when faced with new procurements, or a contract extension decision.

2.3.8. Cabinet also incorporated the cloud risk assessment process into the system-wide ICT assurance framework **[CAB Min (13) 20/13]**.

2.3.9. The New Zealand Government ICT Strategy released in October 2015 requires agencies to outsource their IT functions using common capabilities and public cloud services where this was feasible and practical.

2.3.10. In 2014 The Government Chief Information Officer published Cloud Computing Information Security and Privacy Considerations. This guidance is designed to assist agencies systematically identify, analyse, and evaluate information security and privacy risks related to individual public cloud services.

2.3.11. In July 2016, new measures were confirmed to accelerate the adoption of public cloud services by New Zealand's government agencies. The new measures complement existing policies and risk assessment processes and provide appropriate checks and balances.

Background

2.3.12. The adoption of cloud technologies and services, the hosting of critical data in the cloud and the risk environment requires that agencies exercise caution. Many cloud users are driven by the need for performance, scalability, resource sharing and cost saving so a comprehensive risk assessment is essential in identifying and managing jurisdictional, sovereignty, governance, assurance, technical and security risks.

2.3.13. Security requirements and drivers in the cloud differ significantly from traditional data centre environments requiring new security models and architectures. Key factors include:

- The dynamic nature of the cloud and its related infrastructure;
- No customer ownership or control of infrastructure;
- Limited visibility of architectures and transparency of operations;
- Shared (multi-tenanted) physical and virtual environments; and
- May require re-architecting of agency system to optimise use of cloud services.

2.3.14. While there is potential for significant benefit, flexibility and cost saving, any use of cloud services carries risk. All cloud computing decisions should be

made on a case-by-case basis after a proper risk assessment, the agency technology architecture is developed and security is properly considered and incorporated.

2.3.15. There is also likely to be a significant mismatch in service-level agreements (SLAs) between existing systems and outsourcing arrangements and those of cloud-based services.

2.3.16. It is important to note that although agencies can outsource operational**responsibilities** to a service provider for implementing, managing and maintaining security controls, they cannot outsource their **accountability** for ensuring their data is appropriately protected, including any system or service decommissioning or termination.

2.3.17. The GCDO has developed a risk and assurance framework for cloud computing, which agencies are required to follow when they are considering using cloud services.

References

2.3.18. Additional guidance on cloud services can be found at:

Reference	Title	Publisher	Source
CAB Min (12) 29/8A	Managing The Government's Adoption of Cloud Computing	Cabinet Office	https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Uploads/Documents/CabMin12-cloud-computing.pdf
CAB Min (13) 20/13	Improving Government Information and Communications Technology Assurance	Cabinet Office	https://ssc.govt.nz/assets/Legacy/resources/sec-min-1320_13.pdf
	Cloud Computing – Information Security and Privacy Considerations April 2014	DIA	https://www.digital.govt.nz/assets/Documents/1Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf
	Government ICT Strategy 2015 (updated 2019)	DIA	https://www.digital.govt.nz/digital-government/strategy/strategy-summary/
	Accelerating the Adoption of Public Cloud Services	DIA	https://www.digital.govt.nz/dmsdocument/15-accelerating-the-adoption-of-public-cloud-services/html
	Cloud Risk Assessment Tool [Excel Spreadsheet]	DIA	https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Guidance-and-Resources/Cloud-ICT-Assurance/Cloud-Risk-Assessment-Tool-v1-1-1.xlsx
	Risk Assessment Process	DIA	https://www.digital.govt.nz/dmsdocument/3~Risk-Assessment-Process-Information-Security.pdf

PSR References

2.3.19. Additional information on third party providers is provided in the PSR.

Reference	Title	Source
PSR Mandatory Requirements	GOV4, GOV5, INFOSEC1, INFOSEC2, PERSEC1, PERSEC2, PERSEC3 and PERSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/
PSR content protocols	Management protocol for information security Management protocol for personnel security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/
PSR requirements sections	Supply chain security	https://www.protectivesecurity.govt.nz/governance/supply-chain-security/

Managing specific scenarios	Outsourcing, Offshoring and supply chains Outsourced ICT facilities Cloud Computing	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/outsourced-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/cloud-computing/

Rationale & Controls

2.3.20. Risk Assessment

2.3.20.R.01. Rationale

The adoption of cloud technologies will introduce a wide range of technology and information system risks *in addition* to the risks that already exist for agency systems. It is vital that these additional risks are identified and assessed in order to select appropriate controls and countermeasures. Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied. The geographic location of agency data should be identified as this may include offshore data centres.

2.3.20.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:255]

Agencies intending to adopt cloud technologies or services MUST conduct a comprehensive risk assessment, in accordance with the guidance provided by the GCDO before implementation or adoption.

2.3.20.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:256]

Agencies MUST ensure cloud risks for any cloud service adopted are identified, understood and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.

2.3.21. Security Architecture

2.3.21.R.01. Rationale

The adoption of cloud technologies will introduce a wide range of technology and information system risks in *addition* to the risks that already exist for agency systems. It is vital that these additional risks are identified and assessed in order to select appropriate controls and countermeasures.

2.3.21.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:259]

Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.

2.3.22. Selection of Services

2.3.22.R.01. Rationale

A number of cloud related service, contracts and other arrangements have been negotiated on behalf of the New Zealand Government with a number of cloud service providers. Agencies must consider these services before negotiating individual contracts or supply contract with cloud service providers.

2.3.22.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4935]

Agencies MUST consider the use of any All of Government contracts with cloud service providers before negotiating individual contracts.

2.3.23. System Decommissioning and Contract Termination

2.3.23.R.01. Rationale

It is important that agencies understand how and where their data is processed, managed, stored, backed up and archived within the cloud service provider's environment (systems architecture). This may result in multiple copies of agency data in several data centres, possibly also in several countries.

2.3.23.R.02. Rationale

When an agency system or service is decommissioned or a service provider's contract terminated, it is important that agencies ensure data is returned to the agency and no copies are retained by the service provider.

2.3.23.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:263]

Agency system architectures and supply arrangements and contracts SHOULD include provision for the safe return of agency data in the event of system or service termination or contract termination.

3. Information security governance - roles and responsibilities

3.1. The Agency Head

Objective

3.1.1. The agency head endorses and is accountable for information security within their agency.

Context

Scope

3.1.2. This section covers the role of an agency head with respect to information security.

Chief executive officer /or other title

3.1.3.　In some agencies and bodies, the person responsible for the agency or body may also be referred to as the CEO, Director General, Director or similar title specific to that agency. In such cases the policy for the agency head is equally applicable.

Devolving authority

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

3.1.5.　The Agency Head is also the Accreditation Authority for that agency. See also Section 4.4 – Accreditation Framework.

3.1.6.　Smaller agencies may not be able to satisfy all segregation of duty requirements because of scalability and small personnel numbers. In such cases, potential conflicts of interest should be clearly identified, declared and actively managed for the protection of the individual and of the agency.

3.1.7.　Refer also to *Compliance By Smaller Agencies* in 1.2.8 for information on joint approaches and resource pooling.

Rationale & Controls

3.1.8.　Delegation of authority

3.1.8.R.01.　Rationale

When an agency head chooses to delegate their authority as the Agency's Accreditation Authority they should do so with careful consideration of all the associated risks, as they remain responsible for the decisions made by their delegate.

3.1.8.R.02.　Rationale

The CISO is the most appropriate choice for delegated authority as they should be a senior executive and hold specialised knowledge in information security and security risk management.

3.1.8.C.01.　Control System Classification(s): All Classifications; Compliance: MUST [CID:282]

Where the agency head devolves their authority the delegate MUST be at least a member of the Senior Executive Team or an equivalent management position.

3.1.8.C.02.　Control System Classification(s): All Classifications; Compliance: SHOULD [CID:283]

When the agency head devolves their authority the delegate SHOULD be the CISO.

3.1.8.C.03.　Control System Classification(s): All Classifications; Compliance: SHOULD [CID:284]

Where the head of a smaller agency is not able to satisfy all segregation of duty requirements because of scalability and small personnel numbers, all potential conflicts of interest SHOULD be clearly identified, declared and actively managed.

3.1.9.　Support for information security

3.1.9.R.01.　Rationale

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 within their agency.

3.1.9.R.02.　Rationale

If an incident, breach or disclosure of classified information occurs in preventable circumstances, the relevant agency head will ultimately be held accountable.

3.1.9.C.01.　Control System Classification(s): All Classifications; Compliance: MUST [CID:288]

The agency head MUST provide support for the development, implementation and ongoing maintenance of information security processes within their agency.

3.2. The Chief Information Security Officer

Objective

3.2.1.　The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency.

Context

Scope

3.2.2.　This section covers the role of a CISO with respect to information security within an agency.

Appointing a CISO

3.2.3.　The requirement to appoint a member of the Senior Executive Team or an equivalent management position, to the role of CISO does not require a new dedicated position be created in each agency.

3.2.4.　The introduction of the CISO role and associated responsibilities is aimed at providing a more meaningful title for a subset of the security executive's responsibilities that relate to information security within their agency.

3.2.5.　The CISO should bring accountability and credibility to information security management and appointees should be suitably qualified and experienced.

3.2.6.　Where multiple roles are held by the CISO, for example CIO, or manager of a business unit, conflicts of interest may occur where operational imperatives conflict with security requirements. Good practice separates these roles. Where multiple roles are held by an individual, potential conflicts of interest should be clearly identified and a mechanism implemented to allow independent decision making in areas where conflict may occur.

PSR references

3.2.7.

Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV1, GOV3, GOV4, GOV8, INFOSEC1, INFOSEC2, INFOSEC4, PERSEC1, PERSEC2, PERSEC3, and PERSEC4	https://www.protectivesecurity.govt.nz/ https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/
PSR content protocols	Management protocol for information security Management protocol for personnel security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/
PSR requirements sections	Build security awareness Self assessment & reporting Protective security roles & responsibilities Roles and responsibilities for information security	https://www.protectivesecurity.govt.nz/governance/build-security-awareness/ https://www.protectivesecurity.govt.nz/self-assessment-and-reporting/ https://www.protectivesecurity.govt.nz/governance/protective-security-roles-and-responsibilities/ https://www.protectivesecurity.govt.nz/governance/protective-security-roles-and-responsibilities/roles-and-responsibilities-for-information-security/

Rationale & Controls

3.2.8.   Requirement for a CISO

3.2.8.R.01.   Rationale

The role of the CISO is based on industry and governance good practice and has been introduced to ensure that information security is managed at the senior executive level within agencies. Without a CISO there is a risk that an agency may not be resourced to effectively manage information security.

3.2.8.R.02.   Rationale

The CISO within an agency is responsible predominately for facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives within the agency.

3.2.8.R.03.   Rationale

The CISO is also responsible for providing strategic level guidance for the agency security program and ensuring compliance with national policy, standards, regulations and legislation.

3.2.8.R.04.   Rationale

Some agencies may outsource the CISO function. In such cases conflicts of interest, availability and response times should be identified and carefully managed so the agency is not disadvantaged. Conflicts of interest may also be apparent where the outsourced CISO deals with other vendors.

3.2.8.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:307]

The CISO MUST be:

- cleared for access to all classified information processed by the agency's systems, and
- able to be briefed into any compartmented information on the agency's systems.

3.2.8.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:308]

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

3.2.8.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:309]

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

3.2.8.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:310]

The CISO SHOULD be responsible for overseeing the management of security personnel within the agency.

3.2.8.C.05.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:311]

Where the role of the CISO is outsourced, potential conflicts of interest in availability, response times or working with vendors SHOULD be identified and carefully managed.

3.2.9.   Responsibilities – Reporting

3.2.9.R.01.   Rationale

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

3.2.9.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:314]

The CISO SHOULD report directly to the agency head on matters of information security within the agency.

3.2.10. Responsibilities – Security programs

3.2.10.R.01.   Rationale

Without a comprehensive strategic level information security and security risk management program an agency will lack high-level direction on information security issues and may expose the agency to unnecessary risk.

3.2.10.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:317]

The CISO SHOULD develop and maintain a comprehensive strategic level information security and security risk management program within the agency aimed at protecting the agency's official and classified information.

3.2.10.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:318]

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

3.2.10.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:319]

The CISO SHOULD create and facilitate the agency security risk management process.

3.2.11. Responsibilities – Ensuring compliance

3.2.11.R.01.   Rationale

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

3.2.11.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:322]

The CISO SHOULD be responsible for ensuring compliance with the information security policies and standards within the agency.

3.2.11.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:323]

The CISO SHOULD be responsible for ensuring agency compliance with the NZISM through facilitating a continuous program of certification and accreditation based on security risk management.

3.2.11.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:324]

The CISO SHOULD be responsible for the implementation of information security measurement metrics and key performance indicators within the agency.

3.2.12. Responsibilities – Coordinating security

3.2.12.R.01.   Rationale

One of the core roles of the CISO is to ensure appropriate communication between business and information security teams within their agency. This includes interpreting 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.

3.2.12.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:327]

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, and comprises key business and ICT executives.

3.2.12.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:328]

The CISO SHOULD be responsible for coordinating information security and security risk management projects between business and information security teams.

3.2.12.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:329]

The CISO SHOULD work with business teams to facilitate security risk analysis and security risk management processes, including the identification of acceptable levels of risk consistently across the agency.

3.2.13. Responsibilities – Working with ICT projects

3.2.13.R.01.   Rationale

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

3.2.13.R.02.   Rationale

As the CISO is responsible for the overall management of information security within an agency, they are best placed to recommend to the accreditation authority the acceptance of residual security risks associated with the operation of agency systems.

3.2.13.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:333]

The CISO SHOULD provide strategic level guidance for agency ICT projects and operations.

3.2.13.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:334]

The CISO SHOULD liaise with agency architecture teams to ensure alignment between security and agency architectures.

3.2.14. Responsibilities – Working with vendors

3.2.14.R.01.   Rationale

Having the CISO coordinate the use of external information security resources will ensure that a consistent approach is being applied across the agency.

3.2.14.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:337]

The CISO SHOULD coordinate the use of external information security resources to the agency including contracting and managing the resources.

3.2.15.   Responsibilities – Budgeting

3.2.15.R.01.   Rationale

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

3.2.15.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:341]

The CISO SHOULD be responsible for controlling the information security budget.

3.2.16.   Responsibilities – Information security incidents

3.2.16.R.01.   Rationale

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

3.2.16.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:345]

The CISO SHOULD be fully aware of all information security incidents within the agency.

3.2.17.   Responsibilities – Disaster recovery

3.2.17.R.01.   Rationale

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.

3.2.17.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:348]

The CISO SHOULD coordinate the development of disaster recovery policies and standards within the agency to ensure that business-critical services are supported appropriately and that information security is maintained in the event of a disaster.

3.2.18.   Responsibilities – Training

3.2.18.R.01.   Rationale

To ensure personnel within an agency are actively contributing to the information 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 within the agency they will need to oversee the development and operation of the program.

3.2.18.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:351]

The CISO SHOULD be responsible for overseeing the development and operation of information security awareness and training programs within the agency.

3.2.19.   Responsibilities – Providing security knowledge

3.2.19.R.01.   Rationale

The CISO is not expected to be a technical expert on information security matters; however, knowledge of national and international standards and good practice will assist in communicating with technical experts within their agency on information security matters.

3.2.19.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:354]

The CISO SHOULD provide authoritative security advice and have familiarity with a range of national and international standards and good practice.

3.3. Information Technology Security Managers

Objective

3.3.1.   Information Technology Security Managers (ITSM) provide information security leadership and management within their agency.

Context

Scope

3.3.2.   This section covers the role of an ITSM with respect to information security within an agency.

Information technology security managers

3.3.3.   ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. The main area of responsibility of an ITSM is that of the administrative and process controls relating to information security within the agency.

Rationale & Controls

3.3.4.   Requirement for ITSMs

3.3.4.R.01.   Rationale

When agencies outsource their ICT services, ITSMs should be independent of any company providing ICT services. This will prevent any conflict of interest for an ITSM in conducting their duties.

3.3.4.R.02.   Rationale

Ensure that the agency has a point of presence at sites to assist with monitoring information security for systems and responding to any information security incidents.

3.3.4.C.01.   Control

System Classification(s): All Classifications; Compliance: MUST [CID:367]

Agencies MUST appoint at least one ITSM within their agency.

3.3.4.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:368]

ITSMs MUST be:

- cleared for access to all classified information processed by the agency's systems; and
- able to be briefed into any compartment information on the agency's systems.

3.3.4.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:369]

Where an agency is spread across a number of geographical sites, it is recommended that the agency SHOULD appoint a local ITSM at each major site.

3.3.4.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:370]

The ITSM role SHOULD be undertaken by personnel with an appropriate level of authority and training based on the size of the agency or their area of responsibility within the agency.

3.3.4.C.05.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:371]

ITSMs SHOULD NOT have additional responsibilities beyond those needed to fulfil the role as outlined within this manual.

3.3.5.   Responsibilities – Security programs

3.3.5.R.01.   Rationale

As ITSMs undertake operational management of information security within an agency they can provide valuable input to the development of the information security program by the CISO.

3.3.5.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:375]

ITSMs SHOULD work with the CISO to develop an information security program within the agency.

3.3.5.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:376]

ITSMs SHOULD undertake and manage projects to address identified security risks.

3.3.6.   Responsibilities – Working with ICT projects

3.3.6.R.01.   Rationale

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

3.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:379]

ITSMs MUST be responsible for assisting system owners to obtain and maintain the accreditation of their systems.

3.3.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:380]

ITSMs SHOULD identify systems that require security measures and assist in the selection of appropriate information security measures for such systems.

3.3.6.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:381]

ITSMs SHOULD consult with ICT project personnel to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software.

3.3.6.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:382]

ITSMs SHOULD work with agency enterprise architecture teams to ensure that security risk assessments are incorporated into system architectures and to identify, evaluate and select information security solutions to meet the agency's security objectives.

3.3.6.C.05.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:383]

ITSMs SHOULD work with system owners, systems certifiers and systems accreditors to determine appropriate information security policies for their systems and ensure consistency with the Protective Security Requirements (PSR) and in particular the relevant NZISM components.

3.3.6.C.06.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:384]

ITSMs SHOULD be included in the agency's change management and change control processes to ensure that risks are properly identified and controls are properly applied to manage those risks.

3.3.6.C.07.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:385]

ITSMs SHOULD notify the Accreditation Authority of any significant change that may affect the accreditation of that system.

3.3.7.   Responsibilities – Working with vendors

3.3.7.R.01.   Rationale

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

3.3.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:388]

ITSMs SHOULD liaise with vendors and agency purchasing and legal areas to establish mutually acceptable information security contracts and service-level agreements.

3.3.8. Responsibilities – Implementing security

3.3.8.R.01. Rationale

The CISO will set the strategic direction for information security within the agency, whereas ITSMs are responsible for managing the implementation of information security measures within the agency.

3.3.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:391]

ITSMs MUST be responsible for ensuring the development, maintenance, updating and implementation of Security Risk Management Plans (SRMPs), Systems Security Plans (SecPlan) and any Standard Operating Procedures (SOPs) for all agency systems.

3.3.8.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:392]

ITSMs SHOULD conduct security risk assessments on the implementation of new or updated IT equipment or software in the existing environment and develop treatment strategies if necessary.

3.3.8.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:393]

ITSMs SHOULD select and coordinate the implementation of controls to support and enforce information security policies.

3.3.8.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:394]

ITSMs SHOULD provide leadership and direction for the integration of information security strategies and architecture with agency business and ICT strategies and architecture.

3.3.8.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:395]

ITSMs SHOULD provide technical and managerial expertise for the administration of information security management tools.

3.3.9. Responsibilities – Budgeting

3.3.9.R.01. Rationale

As ITSMs are responsible for the operational management of information security projects and functions within their agency, they will be aware of their funding requirements and can assist the CISO to develop information security budget projections and resource allocations.

3.3.9.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:398]

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.

3.3.10. Responsibilities – Reporting

3.3.10.R.01. Rationale

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

3.3.10.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:401]

ITSMs SHOULD coordinate, measure and report on technical aspects of information security management.

3.3.10.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:402]

ITSMs SHOULD monitor and report on compliance with information security policies, as well as the enforcement of information security policies within the agency.

3.3.10.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:403]

ITSMs SHOULD provide regular reports on information security incidents and other areas of particular concern to the CISO.

3.3.10.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:404]

ITSMs SHOULD assess and report on threats, vulnerabilities, and residual security risks and recommend remedial actions.

3.3.11. Responsibilities – Auditing

3.3.11.R.01. Rationale

As system owners may not understand the results of audits against their systems ITSMs will need to assist them in understanding and responding to reported audit failures. ITSM's should also refer to 5.8 Independent Assurance Reports.

3.3.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:407]

ITSMs SHOULD assist system owners and security personnel in understanding and responding to audit failures reported by auditors.

3.3.12. Responsibilities – Disaster recovery

3.3.12.R.01. Rationale

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

3.3.12.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:410]

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.

3.3.13. Responsibilities – Training

3.3.13.R.01. Rationale

The CISO will oversee the development and operation of information security awareness and training programs within the agency. ITSMs will arrange delivery of that training to personnel within the agency.

3.3.13.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:413]

ITSMs SHOULD provide or arrange for the provision of information security awareness and training for all agency personnel.

3.3.13.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:414]

ITSMs SHOULD develop technical information materials and workshops on information security trends, threats, good practices and control mechanisms as appropriate.

3.3.14. Responsibilities – Providing security knowledge

3.3.14.R.01. Rationale

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

3.3.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:418]

ITSMs SHOULD maintain a current and up-to-date security knowledge base comprising of a technical reference library, security advisories and alerts, information on information security trends and practices, and relevant laws, regulations, standards and guidelines.

3.3.14.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:419]

ITSMs SHOULD provide expert guidance on security matters for ICT projects.

3.3.14.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:420]

ITSMs SHOULD provide technical advice for the information security steering committee, change management committee and other agency and inter-agency committees as required.

3.3.15. Responsibilities

3.3.15.R.01. Rationale

ITSMs are generally considered the information security experts within an agency and as such their contribution to improving the information security of systems, providing input to agency ICT projects, assisting other security personnel within the agency, contributing to information security training and responding to information security incidents is a core aspect of their work.

3.3.15.R.02. Rationale

An ITSM is likely to have the most up to date 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.

3.3.15.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:424]

The ITSM SHOULD keep the CISO and system owners informed with up-to-date information on current threats.

3.4. System Owners

Objective

3.4.1. System owners obtain and maintain accreditation of their systems, including any directly related services such as cloud.

Context

Scope

3.4.2. This section covers the role that system owners undertake with respect to information security.

Assertions in Certification and Accreditation

3.4.3. Originating in financial auditing, assertions are now widely used as the basis for assurance processes covering a wide range of business activities and the related technology.

3.4.4. Assertions are formal statements by management or system owners. They are claims on the completeness, accuracy and validity of events, presentations, disclosure, transactions and related assurance, risk and governance aspects of certification and accreditation.

3.4.5. It is the responsibility of the management (or system owner) to prepare and validate assertions relating to the governance, assurance and security of information systems, in accordance with national policy and related standards.

3.4.6. When such assertions are made it means management (or system owners) have presented and disclosed information appropriately giving a true, fair and balanced view of the activities. In preparing assertions, implicit and explicit claims are made on the validity and completeness of the assertions.

3.4.7. Assertions are typically characterised as follows:

Transactions and events

- Occurrence — the activities recorded have actually taken place.
- Completeness — all aspects are properly recorded.
- Accuracy — the assets and activities are accurately allocated and recorded.
- Cutoff — the activities have been recorded in the correct time period.
- Classifications — are accurate and appropriate.

Position on project completion

- Existence — assets, liabilities and equity balances exist.
- Rights and Obligations — the entity legally controls rights to its assets and its liabilities and accurately records obligations.
- Completeness — all aspects are properly recorded.
- Valuation and Allocation — costs and assets appropriately valued and allocated.

Presentation and disclosure

- Occurrence — the events and implementations have actually occurred.
- Rights and Obligations — contracts, licences, support and supply agreements
- Completeness — all disclosures have been included in the statements.
- Classification — statements are clear and appropriately presented.
- Accuracy and Valuation — information is disclosed at the appropriate amounts.

Rationale & Controls

3.4.8. Requirement for system owners

3.4.8.R.01.　　Rationale

The system owner is responsible for the overall operation of the system, including any directly related support or outsourced service such as cloud. They may delegate the day-to-day management and operation of the system to a system manager or managers.

3.4.8.R.02.　　Rationale

All systems should have a system owner in order to ensure IT governance processes are followed and that business requirements are met.

3.4.8.R.03.　　Rationale

It is strongly recommended that a system owner be a member of the Senior Executive Team or in an equivalent management position, however this does not imply that the system manager(s) should also be at such a level.

3.4.8.C.01.　　Control System Classification(s): All Classifications; Compliance: MUST [CID:442]

Each system MUST have a system owner who is responsible for the operation and maintenance of the system.

3.4.8.C.02.　　Control System Classification(s): All Classifications; Compliance: SHOULD [CID:443]

System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.

3.4.9. Accreditation responsibilities

3.4.9.R.01.　　Rationale

The system owner is responsible for the operation of their system and as such they need to ensure that systems are accredited to meet the agency's operational requirements. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken in an appropriate manner, documented adequately and that any necessary reaccreditation activities are completed.

3.4.9.C.01.　　Control System Classification(s): All Classifications; Compliance: MUST [CID:446]

System owners MUST obtain and maintain accreditation of their system(s).

3.4.10. Documentation responsibilities

3.4.10.R.01.　　Rationale

While the system owner is responsible for ensuring the development, maintenance and implementation of Systems Information Security documentation, in particular the Security Risk Management Plans (SRMPs), System Security Plans (SecPlans) and Standard Operating Procedures (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. Refer to Chapter 5 - Information Security documentation and Chapter 4 - System Certification and Accreditation.

3.4.10.C.01.　　Control System Classification(s): All Classifications; Compliance: MUST [CID:449]

System owners MUST ensure the development, maintenance and implementation of complete, accurate and up to date Information Security documentation for systems under their ownership. Such actions MUST be documented.

3.4.10.C.02.　　Control System Classification(s): All Classifications; Compliance: MUST [CID:450]

System Owners MUST involve the ITSM in the redevelopment and updates of the Information Security documentation.

3.5. System Users

Objective

3.5.1.　　System users comply with information security policies and procedures within their agency.

Context

Scope

3.5.2.　　This section covers the role that system users undertake with respect to information security.

Types of system users

3.5.3.　　This section covers responsibilities for all system users i.e. users with general access (general users), and users with privileged access (privileged users).

3.5.4. Responsibilities of system users

3.5.4.R.01.   Rationale

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

3.5.4.R.02.   Rationale

Security policies, procedures and mechanisms aim to cover all situations that may arise within an agency. However there may be legitimate reasons for a system user to bypass security policies, procedures or mechanisms. If this is the case, the system user MUST seek formal authorisations from the CISO or the ITSM (if this authority has been specifically delegated to the ITSM) before any actions are undertaken.

3.5.4.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:466]

All system users MUST comply with the relevant security policies and procedures for the systems they use.

3.5.4.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:467]

All system users MUST:

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

3.5.4.C.03.   Control System Classification(s): All Classifications; Compliance: MUST [CID:468]

System users that need to bypass security policies, procedures or mechanisms for any reason MUST seek formal authorisation from the CISO or the ITSM if this authority has been specifically delegated to the ITSM.

4. System Certification and Accreditation

4.1. The Certification and Accreditation Process

Objective

4.1.1.   Executives and Security Practitioners understand and enforce the use of the Certification and Accreditation (C&A) process and its role in information security governance and assurance.

Context

Scope

4.1.2.   This section provides a short, high-level description of the C&A process.

4.1.3.   This section must be read in conjunction with the Roles and Responsibilities described in Chapter 3. Subsequent sections of this chapter describe elements of the C&A process in more detail.

The Process

4.1.4.   Certification and Accreditation is a fundamental governance and assurance process, designed to provide the Board, Chief Executive and senior executives confidence that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met. It is essential for credible and effective information assurance governance.

4.1.5.   C&A has two important stages where certification must be completed before accreditation can take place. It is based on an assessment of risk, the application of controls described in the NZISM and determination of any residual risk.

4.1.6.   Certification and Accreditation are separate and distinct elements, demonstrate segregation of duties and assist in managing any potential conflicts of interest. These are important attributes in good governance systems.

4.1.7.   The acceptance of residual risk lies with the Chief Executive of each agency, or lead agency where sector, multi-agency or All-of-Government (AoG) systems are implemented.

4.1.8.   An exception applies where High Assurance Cryptographic Equipment (HACE) is required or caveated or compartmented information is processed, stored or communicated. In this case the Director-General, GCSB is the Accreditation Authority.

4.1.9.   The complete C&A process has several elements and stages, illustrated in the Block Diagram at the end of this section.

Key Participants

4.1.10.   There are four groups of participants:

- **System Owners**, responsible for the design, development, system documentation and system maintenance, including any requests for recertification or reaccreditation.
- The **Certification Authority**, responsible for the review of information and documentation provided by the system owner to ensure the ICT system complies with minimum standards and the agreed design.
- The **Assessor** or Auditor, who will conduct inspections, audits and review as instructed by the Certification Authority.
- The **Accreditation Authority** will consider the recommendation of the Certification Authority. If the level of residual risk is acceptable, the Accreditation Authority will issue the system accreditation (the formal authority to operate a system).

Certification

4.1.11. Certification is the assertion that an ICT system including any related or support services such as Telecommunications or cloud comply with the minimum standards and controls described in the NZISM, any relevant legislation and regulation and other relevant standards. It is based on a comprehensive evaluation or systems audit. This process is described in Section 4.2 – Conducting Certifications.

4.1.12. Certification is evidence that due consideration has been paid to risk, security, functionality, business requirements and is a fundamental part of information systems governance and assurance.

Certification Authorities

4.1.13. For all agency information systems the certification authority is the CISO unless otherwise delegated by the Agency Head.

4.1.14. For external organisations or service providers supporting agencies, the certification authority is the CISO of the agency.

4.1.15. For multi-national, multi-agency, and AoG systems the certification authority is determined by a formal agreement between the parties involved. Within NZ this is usually the lead agency.

Accreditation

4.1.16. Accreditation is the formal authority to operate a system, evidence that governance requirements have been addressed and that the Chief Executive has fulfilled the requirement to manage risk on behalf of the organisation and stakeholders. This element of the C&A process is described in Section 4.4 – Accreditation Framework.

4.1.17. Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged, including the acceptance of any residual risk.

Accreditation Authority

4.1.18. For agencies the Accreditation Authority is the agency head or their delegate.

4.1.19. For multi-national, multi-agency systems or AoG systems, the Accreditation Authority is determined by a formal agreement between the parties involved.

4.1.20. 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.

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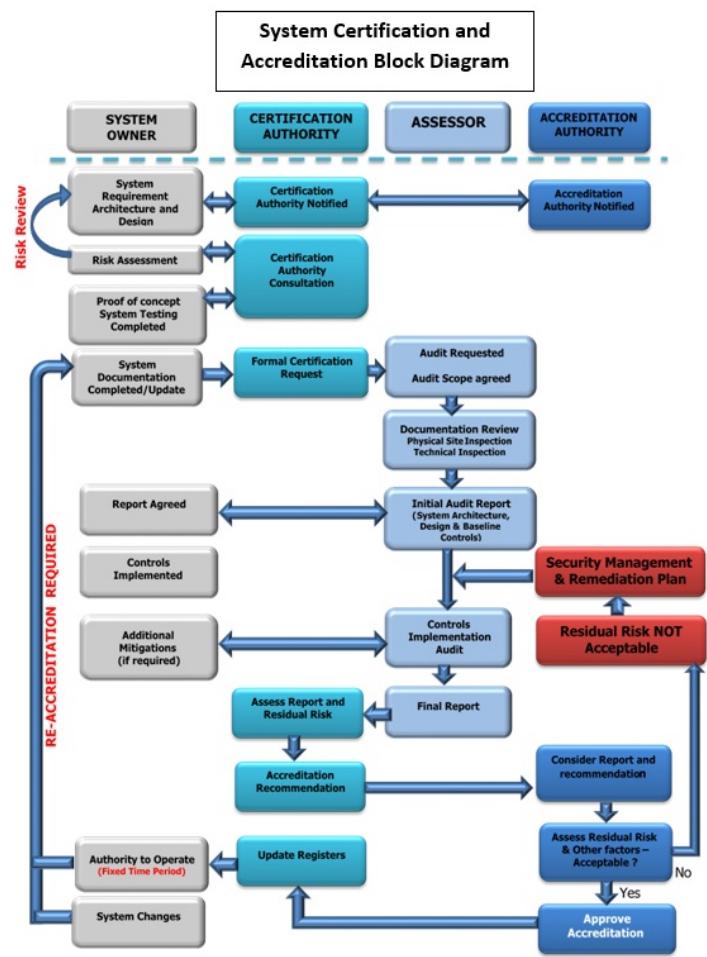
Conflicts of Interest

4.1.22. A conflict of interest is a situation in which a person has duties or responsibilities to more than one person, organisation or elements of a process, but is placed in a position where they cannot do justice to all. This includes, for example, when an individual's vested interests or concerns are inconsistent with organisational outcomes, or when an official has conflicting responsibilities. In the context of the C&A process, a conflict of interest can occur when an individual has multiple roles, such as being both the system owner and the Accreditation Authority.

4.1.23. A conflict of interest has the potential to undermine impartiality and integrity of a process and the people involved in a process. It will also undermine the integrity of governance and information assurance derived from the C&A process.

4.1.24. Conflicts of interest are normally managed though segregation of duties, the division of **roles** and **responsibilities** in order to reduce the ability or opportunity for an individual to compromise a critical process. Segregation of duties also reduces errors of interpretation or judgement and better manages risk.

4.1.25. It is important to note that in the C&A process in the NZISM, the Certification Authority, System Owner and Accreditation Authority are *independent* of each other. In smaller agencies, the Assessor may also be the Certification Authority. Ideally this role will also be segregated.

Penetration Testing

4.1.26. Penetration tests are an effective method of identifying vulnerabilities that in a system or network testing existing security measures and testing the implementation of controls. Penetration testing is also very useful in validating the effectiveness of the defensive mechanisms. This testing provides an increased level of assurance when system certification and accreditation is undertaken. It also demonstrates prudent risk management.

4.1.27. A penetration test usually involves the use of intrusive methods or attacks conducted by trusted individuals, methods similar to those used by intruders or hackers. Care must be taken not to adversely affect normal operations while these tests are conducted.

4.1.28. Organisations may conduct their own tests and regular simple tests are effective in maintaining the organisation's security posture. Because of the level of expertise required to effectively conduct more complex testing, comprehensive penetration tests are often outsourced to specialist organisations.

4.1.29. Penetration tests can range from simple scans of IP addresses in order to identify devices or systems offering services with known vulnerabilities, to exploiting known vulnerabilities that exist in an unpatched operating system, applications or other software. The results of these tests or attacks are recorded, analysed, documented and presented to the owner of the system. Any deficiencies should then be addressed.

System Certification and Accreditation Diagram

4.1.30.

System Certification and Accreditation Block Diagram

References

4.1.31. Additional information relating to systems governance, certification and accreditation can be found at:

Reference	Title	Publisher	Source
ISO/IEC 27000:2018	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	ISO	https://www.standards.co.nz https://www.iso.org
ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems -- Requirements	ISO	https://www.standards.co.nz https://www.iso.org
ISO/IEC 27002:2013	Information technology - Security techniques - Code of practice for information security controls	ISO	https://www.standards.co.nz https://www.iso.org
ISO/IEC_27006:2015	Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems	ISO	https://www.iso27001security.com/html/27006.html https://www.standards.co.nz
ISO/IEC_27007:2020	Information Technology – Security Techniques - Guidelines for information security management systems auditing	ISO	https://www.iso27001security.com/html/27007.html https://www.standards.co.nz
NIST SP 800-37 Rev. 1, Feb 2010	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

NIST SP 800-171, Feb 2020	**Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
	Mitre Engineering Guide - Create and Assess Certification and Accreditation Strategies	MITRE	http://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/test-and-evaluation/
	RAND National Defense Research Institute - Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation	RAND Corporation	http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG951.pdf
	An Introduction to Certification and Accreditation	SANS Institute	https://www.sans.org/reading-room/whitepapers/accreditation/introduction-certification-accreditation-1259
	A Certification and Accreditation Plan for Information Systems Security Programs (Evaluating the Eff)	SANS Institute	https://www.sans.org/reading-room/whitepapers/accreditationcertification-accreditation-plan-information-systems-security-programs-evaluating-ef-597
	Office of the Auditor-General - Managing conflicts of interest: Guidance for public entities	Office of the Auditor-General	https://www.oag.govt.nz/2007/conflicts-public-entities/docs/oag-conflicts-public-entities.pdf
	Managing Conflict of Interest in the Public Service - OECD GUIDELINES AND COUNTRY EXPERIENCES	OECD	http://www.oecd.org/gov/ethics/48994419.pdf
	Data Security Standard (DSS) Information Supplement, March 2008, PCI Security Standards Council,	PCI Security Standards	https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf
	SANS Institute InfoSec Reading Room, Conducting a Penetration Test on an Organization,	SANS Institute	http://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67
	Commercially Available Penetration Testing Best Practice Guide, 8 May 2006, CPNI,	CPNI	http://www.cpni.gov.uk/Documents/Publications/2006/2006030-GPG_Penetration_testing.pdf
	Beyond Best Practices: Web Application Security in the Real World, OWASP, June 2004,	OWASP	Link to App Sec 2004 Dave Aitel Beyond Best Practices
International Standard on Assurance Engagements (ISAE) 3402	**Assurance Reports on Controls at a Service Organization**	International Federation of Accountants (IFAC)	http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf

PSR references

4.1.32. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV6, GOV7, GOV8, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/

PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Take a risk based approach to information security Applying Business impact levels Reporting incidents and conducting security investigations Self assessment and reporting Validate your security measures	https://www.protectivesecurity.govt.nz/information-security/take-a-risk-based-approach-to-information-security/ https://www.protectivesecurity.govt.nz/governance/business-impact-levels/ https://www.protectivesecurity.govt.nz/governance/reporting-incidents-and-conducting-security-investigations/ https://www.protectivesecurity.govt.nz/self-assessment-and-reporting/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/validate-your-security-measures/
Managing specific scenarios	Physical Security for ICT systems Secure your ICT facilities Transacting online with the public	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/transacting-online-with-the-public/

4.2. Conducting Certifications

Objective

4.2.1.   The security posture of the organisation has been incorporated into its system security design, controls are correctly implemented, are performing as intended and that changes and modifications are reviewed for any security impact or implications.

Context

Scope

4.2.2.   This section covers information on the process of undertaking a certification as part of the accreditation process for a system.

Certification

4.2.3.   Certification is the assertion that a given ICT system complies with minimum standards and the agreed design. It is based on a comprehensive evaluation and may involve:

- development and review of security documentation;
- assurance over externally provided services such as Telecommunications and Cloud;
- a physical inspection;
- a technical review of the system and environment; and/or
- technical testing.

4.2.4.   Certification is a **prerequisite** for accreditation. The Accreditation Authority for a specific system MUST NOT accredit that system until all relevant certifications have been provided.

Certification outcome

4.2.5.   The outcome of certification is a certificate to the system owner acknowledging that the system has been appropriately audited and that the findings have been found to be of an acceptable standard.

Certification authorities

4.2.6.   For all agency information systems the certification authority is the CISO unless otherwise delegated by the Agency Head.

4.2.7.   For external organisations or service providers supporting agencies, the certification authority is the CISO of the agency.

4.2.8.   For multi-national, multi-agency, and AoG systems the certification authority is determined by a formal agreement between the parties involved. Within NZ this is usually the lead agency.

References

4.2.9.   Additional information relating to system auditing is contained in:

Reference	Title	Publisher	Source
ISO/IEC 27006:2015	Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems	ISO/IEC	https://www.iso27001security.com/html/27006.html https://www.standards.co.nz

ISO/IEC 27007:2020	Information Technology – Security Techniques - Guidelines for information security management systems auditing	ISO/IEC	https://www.iso27001security.com/html/27006.html https://www.standards.co.nz
ISO/IEC 19011:2018	Guidelines for auditing management systems	ISO/IEC	https://www.iso.org/standard/70017.html

Rationale & Controls

4.2.10. Certification Audit

4.2.10.R.01.   Rationale

The purpose of a Certification Audit is to assess the actual implementation and effectiveness of controls for a system against the agency's risk profile, security posture, design specifications, agency policies and compliance with the Protective Security Requirements (PSR) and in particular the relevant NZISM components.

4.2.10.R.02.   Rationale

The extent and scope of the Certification Audit should consider the feasibility and cost-effectiveness of the audit against the risks and benefits of the system under review. Major or high-risk systems will require more detailed and extensive review than low-risk or minor systems. See also Section 4.3 Conducting Audits.

4.2.10.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:535]

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

4.2.11. Certification decision

4.2.11.R.01.   Rationale

To award certification for a system the certification authority will need to be satisfied that the selected controls are appropriate, are consistent with the Protective Security Requirements (PSR) and in particular the relevant NZISM components, have been properly implemented and are operating effectively.

4.2.11.R.02.   Rationale

To cater for the different responsibilities for physical and technical Certification & Accreditation, separate reports and recommendations may be required.

4.2.11.R.03.   Rationale

Certification acknowledges only that controls were appropriate, properly implemented and are operating effectively. Certification does NOT imply that the residual security risk is acceptable or an approval to operate has been granted.

4.2.11.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:540]

The certification authority MUST accept that the controls are appropriate, effective and comply with the Protective Security Requirements (PSR) and in particular the relevant NZISM components, in order to award certification.

4.2.12. Residual security risk assessment

4.2.12.R.01.   Rationale

The purpose of the residual security risk assessment is to assess the risks, controls and residual security risk relating to the operation of a system. In situations where the system is non-conformant, the system owner may have taken corrective actions. The residual risk may not be great enough to preclude a certification authority recommending to the Accreditation Authority that accreditation be awarded but the risk MUST be acknowledged and appropriate qualifications or limitations documented.

4.2.12.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:543]

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.

4.3. Conducting Audits

Objective

4.3.1.   The effectiveness of information security measures for systems is periodically reviewed and validated.

Context

Scope

4.3.2.   This section covers information on the process of undertaking a certification and accreditation audit.

Audit objectives, scope and criteria

4.3.3.   The aim of an audit is to review and assess:

- the risk identification and assessment;
- design and complexity (including the system and security architectures);
- any available assurance reports on support or outsourced services;
- controls selection;
- actual implementation and effectiveness of controls for a system; and
- supporting information security documentation.

4.3.4.   Only information that is verifiable should be accepted as audit evidence. Audit evidence should be recorded.

Audit outcome

4.3.5.   The outcome of an audit is a report of compliance and control effectiveness for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

4.3.6.   Part of this audit is an assessment of whether the control systems adequately identify and address risk and information security requirements.

Who can assist with an audit

4.3.7.   A number of other agencies and personnel within agencies are often consulted during an audit. Agencies or personnel that can be consulted on physical security aspects of information security may include:

- The NZSIS for Physical Security;
- GCSB for TOP SECRET sites and Sensitive Compartmented Information Facilities (SCIFs);
- MFAT for systems located at overseas posts and missions;
- The Chief Security Officer (CSO) may be consulted on personnel and physical security aspects of information security;
- The CISO, ITSM or communications security officer may be consulted on COMSEC aspects of information security; and
- The ITSM and System Owner on aspects of secure system design configuration and operation.

Independent audits

4.3.8.   An audit may be conducted by agency auditors or an independent security organisation.

Audit Evidence

4.3.9.   Audit evidence can be obtained from documentation described in Chapter 5 – Information Security Documentation.

Other sources may include:

Source	
Agency Strategies and Statements of Intent.	Any additional process documentation referenced in the documentation described in the NZISM Chapter 5.
Third party service provider agreements.	Independent risk assessments or security evaluations, such as penetration tests by an internal team or an external organization.
The agency risk identification and assessment process.	Any internal audit reports, assessments and reviews.
Any statements of applicability.	Any relevant incident reports.

Audit evidence reliability

4.3.10.   The reliability of audit evidence is influenced by its source, nature and the circumstances under which the evidence is gathered. In general terms documentary evidence is more reliable than oral evidence, self-generated evidence less reliable than evidence gathered elsewhere and externally generated evidence is more reliable than internally generated evidence as internally generated evidence may be more susceptible to selective presentation.

4.3.11.   Confirmation should be obtained that:

- Risk owners have been identified; and
- Each risk owner has sufficient accountability and authority to manage their identified risks.

4.3.12.   Audit evidence can be gathered through the following methods in order of preference:

Method	Description
Inspection	Physical inspections can provide an independent confirmation of the physical condition of the site or systems, its implementation and its management.
Analytical review	Reviews of records and documents will provide evidence of varying degrees of reliability depending on their nature and source. A review of the risk identification and selection of risk treatments is invaluable.
Enquiry	Here audit evidence is gathered by interview. Enquiries can be formal or informal and oral or written. It is essential that the auditor creates a written record of any enquiries conducted.
Observation	Observation of operations or procedures being performed by others with the aim of determining the manner of its performance only at that particular time. This may include checks on system configurations, change management processes or other key elements.
Computations	Rarely used for non-financial records but may include, for example, asset registers and validation of holdings of accountable equipment and software.

Audit evidence sufficiency

4.3.13. The Sufficiency is the measure of the quality (not the quantity) of audit evidence. It is important, however, that a balance is struck between the extent of the audit, the nature of the system under review, agency risk and the cost, effort and benefit of the audit. Sufficient evidence should be obtained to allow the auditor to be able to draw reasonable conclusions on which to base the audit opinion. For evidence to be deemed sufficient, the following aspects should be considered:

- Materiality. Materiality is the threshold where any distorted, missing and incorrect information is likely to have an impact on the risk and security of a system. Where it becomes clear that there are material deficiencies in the evidence presented more substantive tests may be required or the audit suspended until corrective action has been taken by the agency.

- Risk assessment: It is almost impossible to validate every risk identification and selection of risk treatments. For larger systems a more practical approach may be to validate the identification and treatment of major risks and use sampling techniques for the balance.

- Economy: Before gathering or requesting additional audit evidence, it is important to consider whether or not it is feasible or cost-effective to generate this evidence against the benefits, assessed value and time required.

References

4.3.14. Further references can be found at:

Reference	Title	Publisher	Source
ISO 19011:2018	**Guidelines for auditing management systems**	ISO	https://www.iso.org
ISO/IEC 27000:2018	**Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary**	ISO	https://www.standards.co.nz https://www.iso.org
ISO/IEC 27001:2013	**Information technology -- Security techniques -- Information security management systems -- Requirements**	ISO	https://www.iso27001security.com/html/27006.html https://www.standards.co.nz https://www.iso.org
ISO/IEC 27002:2013	**Information technology - Security techniques - Code of practice for information security controls**	ISO	https://www.standards.co.nz https://www.iso.org
ISO/IEC 27006:2015	**Information Technology – Security Techniques- Requirements for bodies providing audit and certification of information security management systems**	ISO	https://www.standards.co.nz https://www.iso.org
ISO/IEC 27007:2020	**Information Technology – Security Techniques - Guidelines for information security management systems auditing**	ISO	https://www.standards.co.nz https://www.iso.org
International Standard On Auditing (New Zealand) 500	**Audit Evidence**	External Reporting Board, NZ Audit and Assurance Standards Board	https://www.xrb.govt.nz/standards-for-assurance-practitioners/auditing-standards/isa-nz-500/

PSR references

4.3.15.

Reference	Title	Source
PSR Mandatory Requirements	GOV3, GOV8, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/
PSR content protocols	Management protocol for information security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/
PSR requirements sections	Self assessment & reporting	https://www.protectivesecurity.govt.nz/self-assessment-and-reporting/
Managing specific scenarios	Transacting online with the public	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/transacting-online-with-the-public/

Rationale & Controls

4.3.16. Independence of auditors

4.3.16.R.01.   Rationale

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

4.3.16.C.01.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:562]

Agencies SHOULD ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority.

4.3.17.   Audit preparation

4.3.17.R.01.   Rationale

Ensuring that the system owner has approved the system architecture and associated information security documentation will assist auditors in determining the scope of work for the first stage of the audit.

4.3.17.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:565]

Prior to undertaking the audit the system owner MUST approve the system architecture and associated information security documentation.

4.3.18.   Audit (first stage)

4.3.18.R.01.   Rationale

Auditing against the risk assessment and subsequent controls selection is preferable to a 'checklist' approach where all controls in the NZISM are checked for selection and implementation irrespective of applicability.

4.3.18.R.02.   Rationale

The purpose of the first stage of the audit is to determine that the system and security architecture (including information security documentation) is based on sound information 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.

4.3.18.R.03.   Rationale

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

4.3.18.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:569]

The SecPol, SRMP, SecPlan, SOPs and IRP documentation MUST be reviewed by the auditor to ensure that it is comprehensive and appropriate for the environment the system is to operate within.

4.3.18.C.02.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:570]

The Information Security Policy (SecPol) MUST be reviewed by the auditor to ensure that all applicable controls specified in this manual are addressed.

4.3.18.C.03.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:571]

The system and security architecture (including information security documentation) SHOULD be reviewed by the auditor to ensure that it is based on sound information security principles and meets information security requirements, including the NZISM.

4.3.18.C.04.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:572]

The Information Security Policy (SecPol) SHOULD be reviewed by the auditor to ensure that policies have been developed or identified by the agency to protect classified information that is processed, stored or communicated by its systems.

4.3.18.C.05.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:573]

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; and
- any additional controls implemented as a result of the SRMP.

4.3.19.   Implementing controls

4.3.19.R.01.   Rationale

System testing is most effective on working systems. Desk checks have limited effectiveness in these situations.

4.3.19.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:576]

Prior to undertaking any system testing in support of the certification process, the system owner MUST implement the controls for the system.

4.3.20.   Audit (second stage)

4.3.20.R.01.   Rationale

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 correctly and are operating effectively.

4.3.20.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:579]

The implementation of controls MUST be assessed to determine whether they have been implemented correctly and are operating effectively.

4.3.20.C.02.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:580]

The auditor MUST ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.

4.3.20.C.03.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:581]

The physical security certification SHOULD be less than three (3) years old at the time of the audit.

4.3.21.   Report of compliance

4.3.21.R.01.   Rationale

The report of compliance assists the certification authority in conducting a residual security risk assessment to 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.

4.3.21.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:584]

The auditor MUST produce a report of compliance for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

4.4. Accreditation Framework

Objective

4.4.1.   Accreditation is the formal authority for a system to operate, and an important element in fundamental information system governance. Accreditation requires risk identification and assessment, selection and implementation of baseline and other appropriate controls and the recognition and acceptance of residual risks relating to the operation of a system including any outsourced services such as Telecommunications or Cloud. Accreditation relies on the completion of system certification procedures.

Context

Scope

4.4.2.   This section covers information on the accreditation framework for systems.

4.4.3.   All types of government held information are covered, including Official Information and information subject to privacy requirements.

Rationale & Controls

4.4.4.   Accreditation framework

4.4.4.R.01.   Rationale

The development of an accreditation framework within the agency will ensure that accreditation activities are conducted in a repeatable and consistent manner across the agency and that consistency across government systems is maintained. This requirement is a fundamental part of a robust governance model and provides a sound process to demonstrate good governance of information systems.

4.4.4.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:595]

Agencies MUST develop an accreditation framework for their agency.

4.4.5.   Accreditation

4.4.5.R.01.   Rationale

Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged by an appropriate authority. As such, when systems are awarded accreditation the Accreditation Authority accepts that the residual security risks relating to the system are appropriate for the information that it processes, stores or communicates.

4.4.5.R.02.   Rationale

Once systems have been accredited, conducting on-going monitoring activities will assist in assessing changes to its environment and operation and to determine the implications for the security risk profile and accreditation status of the system.

4.4.5.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:599]

Agencies MUST ensure that each of their systems is awarded accreditation.

4.4.5.C.02.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:600]

Agencies MUST ensure that all systems are awarded accreditation before they are used operationally.

4.4.5.C.03.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:601]

Agencies MUST ensure that all systems are awarded accreditation prior to connecting them to any other internal or external system.

4.4.5.C.04.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:602]

Agencies SHOULD ensure information security monitoring, logging and auditing is conducted on all accredited systems.

4.4.6.   Determining authorities

4.4.6.R.01.   Rationale

Determining the certification and accreditation authorities for multi-national and multi-agency systems via a formal agreement between the parties will ensure that the system owner has identified appropriate points of contact and that risk is appropriately managed. See Section 4.5 – Conducting Accreditations.

4.4.6.C.01.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:605]

For multi-national and multi-agency systems, the Certification and Accreditation Authorities SHOULD be determined by a formal agreement between the parties involved.

4.4.7. Notifying authorities

4.4.7.R.01. Rationale

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

4.4.7.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:608]

Prior to beginning the accreditation process the system owner SHOULD advise the certification and accreditation authorities of their intent to seek certification and accreditation for their system.

4.4.7.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:609]

Agencies SHOULD confirm governance arrangements with the certification authorities, and with the accreditation authorities.

4.4.8. Due diligence

4.4.8.R.01. Rationale

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. This is vital where different classification systems are applied, such as in the use of multiple national classification systems.

4.4.8.R.02. Rationale

Methods that an agency may use to ensure that other agencies and third parties comply with the agency's information security expectations include:

- assurance and confirmation that the certification and accreditation process described in the NZISM is adhered to;
- conducting or utilising any third party reviewed assurance reports;
- conducting an accreditation of the system being connected to; and/or
- seeking a copy of existing accreditation deliverables in order to make their own accreditation determination.

4.4.8.R.03. Rationale

Ultimately, the agency MUST accept any security risks associated with connecting their system to the other party's system. This includes the risks of other party's system potentially being used as a platform to attack their system or "spilling" information requiring subsequent clean up processes.

4.4.8.R.04. Rationale

Special care MUST be taken for multi- national, multi-agency and All-of-Government systems.

4.4.8.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:615]

Where an agency's system exchanges information with a third-party system, the agency MUST ensure that the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification or privacy requirements of their information and that the third party is authorised to receive that information.

4.4.8.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:616]

An agency MUST ensure that a third party is aware of the agency's information security expectations and national security requirements by defining expectations in documentation that includes, but is not limited to:

- contract provisions;
- a memorandum of understanding;
- non-disclosure agreements.

4.4.8.C.03. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:617]

An agency MUST ensure that a third party complies with the agency's information security expectations through a formal process providing assurance to agency management that the operation of information security within the third party meets, and continues to meet, these expectations.

4.4.8.C.04. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:618]

Agencies SHOULD review accreditation deliverables when determining whether the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification of their information.

4.4.9. Processing restrictions

4.4.9.R.01. Rationale

When security is applied to systems, protective measures are put in place based on the highest classification that will be processed, stored or communicated by the system. As such, any classified information placed on the system above the level for which it has been accredited will receive an inappropriate level of protection and could be exposed to a greater risk of compromise.

4.4.9.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:621]

Agencies MUST NOT allow a system to process, store or communicate classified information above the classification for which the system has received accreditation.

4.4.10. Accrediting systems bearing a compartment marking

4.4.10.R.01. Rationale

When processing compartmented information on a system, agencies need to ensure that the system has received accreditation.

Rationale

Compartments are invariably established for the additional protection of information of National security significance, over and above the protection provided by the primary classification. It is extremely unlikely that such compartments would be established at a classification below CONFIDENTIAL.

4.4.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:624]

A system that processes, stores or communicates compartmented information MUST be accredited by the GCSB.

4.4.11. Requirement for New Zealand control

4.4.11.R.01. Rationale

NZEO systems process, store and communicate information that is particularly sensitive to the government of New Zealand. When agencies are dealing with New Zealand Eyes Only (NZEO) information they need to be aware of the requirement for a New Zealand national to remain in control of the system and information at all times. It is, therefore, essential that control of such systems is maintained by New Zealand citizens working for the government of New Zealand.

4.4.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:627]

Agencies MUST ensure that systems processing, storing or communicating NZEO information remain under the control of a New Zealand national working for the New Zealand government, at all times.

4.4.12. Reaccreditation

4.4.12.R.01. Rationale

Agencies should reaccredit their systems at least every two years; however, they can exercise an additional one year's grace if they follow the procedures in this manual for non-compliance with a 'SHOULD' requirement, namely conducting a comprehensive security risk assessment, obtaining sign-off by senior management and formal acceptance of residual risk.

4.4.12.R.02. Rationale

Accreditations should be commenced at least six months before due date to allow sufficient time for the certification and accreditations processes to be completed. Once three years has elapsed between accreditations, the authority to operate the system (the accreditation) will lapse and the agency will need to either reaccredit the system or request a dispensation to operate without accreditation. It should be noted that operating a system without accreditation is considered extremely risky. This will be exacerbated when multiple agency or All-of-Government systems are involved.

4.4.12.R.03. Rationale

Additional reasons for conducting reaccreditation activities could include:

- changes in the agency's information security policies or security posture;
- detection of new or emerging threats to agency systems;
- the discovery that controls are not operating as effectively as planned;
- a major information security incident; and
- a significant change to systems, configuration or concept of operation for the accredited system.

4.4.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:632]

Agencies MUST ensure that the period between accreditations of each of their systems does not exceed three years.

4.4.12.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:633]

Agencies MUST notify associated agencies where multiple agencies are connected to agency systems operating with expired accreditations.

4.4.12.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:634]

Agencies MUST notify the Government CIO where All-of-Government systems are connected to agency systems operating with expired accreditations.

4.4.12.C.04. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:635]

Agencies MUST NOT operate a system without accreditation or with a lapsed accreditation unless the accreditation authority has granted a dispensation.

4.4.12.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:636]

Agencies SHOULD ensure that the period between accreditations of each of their systems does not exceed two years.

4.5. Conducting Accreditations

Objective

4.5.1. As a governance good practice, systems are accredited before they are used operationally.

Context

Scope

4.5.2. This section covers information accreditation processes.

Accreditation aim

4.5.3. The aim of accreditation is to give formal recognition and acceptance of the residual security risk to a system and the information it processes, stores or communicates as part of the agency's governance arrangements.

Accreditation outcome

4.5.4. The outcome of accreditation is an approval to operate issued by the Accreditation Authority to the system owner.

Accreditation Authorities

4.5.5. For agencies the Accreditation Authority is the agency head or their formally authorised delegate.

4.5.6. For organisations supporting agencies the Accreditation Authority is the head of the supported agency or their authorised delegate.

4.5.7. For multi-national and multi-agency systems the Accreditation Authority is determined by a formal agreement between the parties involved.

4.5.8. For agencies with systems that process, store or communicate endorsed or compartmented information, or the use of High Assurance Cryptographic Equipment (HACE), the Director-General GCSB is the Accreditation Authority.

4.5.9. 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.

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

4.5.11. More information on the delegation of the agency head's authority can be found in Section 3.1 - Agency Head.

Accreditation outcomes

4.5.12. Accreditation is awarded when the systems comply with the NZISM, the Accreditation Authority understands and accepts the residual security risk relating to the operation of the system and the Accreditation Authority gives formal approval for the system to operate.

4.5.13. In some cases the Accreditation Authority may not accept the residual security risk relating to the operation of the system. This outcome is predominately caused by security risks being insufficiently considered and documented within the SRMP resulting in an inaccurate scoping of security measures within the SecPlan. In such cases the Accreditation Authority may request that the SRMP and SecPlan be amended and security measures reassessed before accreditation is awarded.

4.5.14. In awarding accreditation for a system the Accreditation Authority may choose to define a reduced timeframe before reaccreditation, less than that specified in this manual, or place restrictions on the use of the system which are enforced until reaccreditation or until changes are made to the system within a specified timeframe.

Exception for undertaking certification

4.5.15. In exceptional circumstances the Accreditation Authority may elect not to have a certification conducted on a system before making an accreditation decision. The test to be satisfied in such circumstances is that if the system is not operated immediately it would have a devastating and potentially long lasting effect on the operations of the agency. This exception MUST be formally recorded and accepted.

4.5.16. Certification MUST occur as soon as possible as this is an essential part of the governance and assurance mechanism.

Rationale & Controls

4.5.17. Certification

4.5.17.R.01.   Rationale

Certification is an essential component of the governance and assurance process and assists and supports risk management.

4.5.17.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:666]

All systems MUST be certified as part of the accreditation process.

4.5.18. Accreditation decision

4.5.18.R.01.   Rationale

In order to determine the agency's security posture, a system accreditation:

- examines the risks to systems identified in the certification process;
- reviews the controls applied to manage those risks; and then
- determines the acceptability of any residual risk.

4.5.18.R.02.   Rationale

The accreditation process should also examine compliance with national policy, relevant international standards and good practice so that residual risk is managed prudently and pragmatically.

4.5.18.R.03.   Rationale

It is especially important that All-of-Government systems and effects on systems of other agencies are also considered in the examination of risk and determination of residual risk.

4.5.18.R.04.   Rationale

To assist in making an accreditation decision the Accreditation Authority may choose to review:

- Information Security Documentation as described in Chapter 5;
- any interaction with systems of other agencies or All-of-Government systems;
- compliance audit reports;
- the accreditation recommendation from the certification authority;
- supporting documentation for any decisions to be non-compliant with any controls specified in this manual;
- any additional security risk reduction strategies that have been implemented; and
- any third party reviews or assurance reports available.

4.5.18.R.05.   Rationale

The Accreditation Authority may also choose to seek the assistance of one or more technical experts in understanding the technical components of information presented to them during the accreditation process to assist in making an informed accreditation decision.

4.5.18.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:673]

The Accreditation Authority MUST accept the residual security risk relating to the operation of a system in order to award accreditation.

4.5.18.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:674]

The Accreditation Authority MUST advise other agencies where the accreditation decision may affect those agencies.

4.5.18.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:675]

The Accreditation Authority MUST advise the GCDO where the accreditation decision may affect any All-of-Government systems.

5. Information security documentation

5.1. Documentation Fundamentals

Objective

5.1.1. Information security documentation is produced for systems, to support and demonstrate good governance.

Context

Scope

5.1.2. This section is an overview of the information security documentation that each agency will need to develop. More specific information on each document can be found in subsequent sections of this chapter.

5.1.3. While this section describes a number of different but essential documents, it may be more advantageous and efficient to provide agency wide documentation for some elements (for example Physical Security) which can then be re-used for all agency systems.

5.1.4. Similarly some consolidation may be appropriate, for example, SOPs IRPs and EPs can easily be combined into a single document.

Note: For smaller agencies and smaller systems it is acceptable that all documentation elements are combined into a single document provided each documentation element is clearly identifiable.

Note: Agencies may choose to name the documentation in different terms. This is acceptable provided the required level of detail is captured. Naming conventions presented in the NZISM are not mandatory.

Information Security Documentation

5.1.5. Information Security Documentation requirements are summarised in the table below.

Title	Abbreviation	Reference
Information Security Policy	SecPol	5.1.7
Systems Architecture	-	5.1.8
Security Risk Management Plan	SRMP	5.1.9
System Security Plan	SecPlan	5.1.10
Site Security Plan	SitePlan	8.2.7
Standard Operating Procedures	SOPs	5.1.11
Incident Response Plan	IRP	5.1.12
Emergency Procedures	EP	5.1.13
Independent Assurance reports for externally provided services	-	5.8

PSR references

5.1.6. Additional information on third party providers is provided in the PSR.

Reference	Title	Source
PSR Mandatory Requirements	GOV4, GOV5, INFOSEC1, INFOSEC2, PERSEC1, PERSEC2, PERSEC3 and PERSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/

PSR content protocols	Management protocol for information security Management protocol for personnel security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/
PSR requirements sections	Supply chain security	https://www.protectivesecurity.govt.nz/governance/supply-chain-security/
Managing specific scenarios	Outsourcing, Offshoring and supply chains Outsourced ICT facilities Cloud Computing	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/outsourced-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/cloud-computing/

Rationale & Controls

5.1.7. Information Security Policy (SecPol)

5.1.7.R.01. Rationale

The SecPol is an essential part of information security documentation as it outlines the high-level policy objectives. The SecPol can form part of the overall agency security policy.

5.1.7.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:692]

Agencies MUST have a SecPol for their agency. The SecPol is usually sponsored by the Chief Executive and managed by the CISO or Chief Information Officer (CIO). The ITSM should be the custodian of the SecPol. The SecPol should include an acceptable use policy for any agency technology equipment, systems, resources and data.

5.1.8. Systems Architecture

5.1.8.R.01. Rationale

The systems architecture illustrates the design of the system (including any outsourced services), consistency with the SecPol and provides the basis for the Security Risk Management Plan (SRMP).

5.1.8.R.02. Rationale

In this context Systems Architecture includes Security Architecture.

5.1.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:696]

All systems MUST have a documented Systems Architecture.

5.1.9. Security Risk Management Plan (SRMP)

5.1.9.R.01. Rationale

The SRMP is considered to be a good practice approach to identifying and reducing identified security risks. Depending on the documentation framework chosen, multiple systems can refer to, or build upon, a single SRMP.

5.1.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:699]

Agencies MUST ensure that every system is covered by a Security Risk Management Plan, which includes identification of **risk owners**.

5.1.10. System Security Plan (SecPlan)

5.1.10.R.01. Rationale

The SecPlan describes the implementation and operation of controls within the system derived from the NZISM and the SRMP. Depending on the documentation framework chosen, some details common to multiple systems can be consolidated in a higher level SecPlan.

5.1.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:702]

Agencies MUST ensure that every system is covered by a SecPlan.

5.1.11. Standard Operating Procedures (SOPs)

5.1.11.R.01. Rationale

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

5.1.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:705]

Agencies MUST ensure that Standard Operating Procedures (SOPs) are developed for systems.

5.1.12. Incident Response Plan (IRP)

5.1.12.R.01. Rationale

The purpose of developing an IRP is to ensure that information security incidents are appropriately managed. In most situations the aim of the response will be to contain the incident and prevent the information security incident from escalating. The preservation of any evidence relating

to the information security incident for criminal, forensic and process improvement purposes is also an important consideration.

5.1.12.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:708]

Agencies MUST develop an Incident Response Plan and supporting procedures.

5.1.12.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:709]

Agency personnel MUST be trained in and periodically exercise the Incident Response Plan.

5.1.13.   Emergency Procedures (EP)

5.1.13.R.01. Rationale

Classified information and systems are secured if a building emergency or evacuation is required.

5.1.13.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:712]

Agencies SHOULD document procedures relating to securing classified information and systems when required to evacuate a facility in the event of an emergency.

5.1.14.   Developing content

5.1.14.R.01. Rationale

Ensuring personnel developing information security documentation are sufficiently knowledgeable of information security issues and business requirements will assist in achieving the most useful and accurate set of documentation.

5.1.14.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:715]

Agencies SHOULD ensure that information security documentation is developed by personnel with a good understanding of policy requirements, the subject matter, essential processes and the agency's business and operations

5.1.15.   Documentation content

5.1.15.R.01. Rationale

As the SRMP, Systems Architecture, SecPlan, SOPs and IRP are developed as a documentation suite for a system it is essential that they are logically connected and consistent within themselves and with other agency systems. Furthermore, each documentation suite developed for a system will need to be consistent with the agency's overarching SecPol.

5.1.15.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:718]

Agencies SHOULD ensure that their SRMP, Systems Architecture, SecPlan, SOPs and IRP are logically connected and consistent for each system, other agency systems and with the agency's SecPol.

5.1.16.   Documentation framework

5.1.16.R.01. Rationale

The implementation of an overarching information security document framework ensures that all documentation is accounted for, complete and maintained appropriately. Furthermore, it can be used to describe linkages between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

5.1.16.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:721]

Agencies SHOULD create and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other.

5.1.16.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:722]

Where an agency lacks an existing, well-defined documentation framework, they SHOULD use the document names defined in this manual.

5.1.17.   Documentation Consistency

5.1.17.R.01. Rationale

Consistency in approach, terminology and documentation simplifies the use and interpretation of documentation for different systems and agencies.

5.1.17.R.02. Rationale

Factors which should be taken into account when determining the classification of systems documentation include:

- Highest classification of information stored, processed or communicated over that system;
- Sensitivity including existence of the facility;
- Inclusion of vulnerability information, security mechanisms or special processing capability in the systems documentation;
- Potential data aggregation;
- Risk and threat levels; and
- Scope and use of the system.

5.1.17.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:726]

Where an agency uses alternative documentation names to those defined within this manual for their information security documentation they SHOULD convert the documentation names to those used in this manual.

5.1.18.   Documentation Classification

5.1.18.R.01. Rationale

Systems documentation will usually reflect the importance or sensitivity of particular systems.

5.1.18.C.01.   Control

System Classification(s): All Classifications; Compliance: MUST [CID:729]

Agencies MUST ensure that their SecPol, SRMP, SecPlan, SOPs and IRP are appropriately classified.

5.1.19.   Outsourcing development of content

5.1.19.R.01.   Rationale

Agencies outsourcing the development of information security documentation need to be aware of the contents of the documentation produced. As such, they will still need to review and control the documentation contents to make sure it is appropriate and meets their requirements.

5.1.19.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:732]

When information security documentation development is outsourced, agencies SHOULD:

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

5.1.20.   Obtaining formal sign-off

5.1.20.R.01.   Rationale

Without appropriate sign-off of information security documentation within an agency, the security personnel will have a reduced ability to ensure appropriate security procedures are selected and implemented. Having sign-off at an appropriate level assists in reducing this security risk as well as ensuring that senior management is aware of information security issues and security risks to the agency's business.

5.1.20.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:735]

All information security documentation SHOULD be formally approved and signed off by a person with an appropriate level of seniority and authority.

5.1.20.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:736]

Agencies SHOULD ensure that:

- all high-level information security documentation is approved by the CISO and the agency head or their delegate; and
- all system-specific documents are reviewed by the ITSM and approved by the system owner.

5.1.21.   Documentation Maintenance

5.1.21.R.01.   Rationale

The threat environment and agencies' businesses are dynamic. If an agency fails to keep their information security documentation up to date to reflect the changing environment, they do not have a means of ascertaining that their security measures and processes continue to be effective.

5.1.21.R.02.   Rationale

Changes to risk and technology may dictate a reprioritisation of resources in order to maximise the effectiveness of security measures and processes.

5.1.21.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:767]

Agencies SHOULD develop a regular schedule for reviewing all information security documentation.

5.1.21.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:768]

Agencies SHOULD ensure that information security documentation is reviewed:

- at least annually; or
- in response to significant changes in the environment, business or system; and
- with the date of the most recent review being recorded on each document.

5.2. Information Security Policies

Objective

5.2.1.   Information security policies (SecPol) set the strategic direction for information security.

Context

Scope

5.2.2.   This section relates to the development of Information Security Policies and any supporting plans. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

5.2.3.   The Information Security Policy (SecPol)

5.2.3.R.01.   Rationale

To provide consistency in approach and documentation, agencies should consider the following when developing their SecPol:

- policy objectives;
- how the policy objectives will be achieved;
- the guidelines and legal framework under which the policy will operate;
- stakeholders;

- education and training;
- what resourcing will be available to support the implementation of the policy;
- what performance measures will be established to ensure that the policy is being implemented effectively; and
- a review cycle.

5.2.3.R.02.   Rationale

In developing the contents of the SecPol, agencies may also consult any agency-specific directives that are applicable to information security within their agency.

5.2.3.R.03.   Rationale

Agencies should also avoid outlining controls for systems within their SecPol. The controls for a system will be determined by this manual and based on the scope of the system, along with any additional controls as determined by the SRMP, and documented within the SecPlan.

5.2.3.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:780]

The Information Security Policy (SecPol) SHOULD document the information security guidelines, standards and responsibilities of an agency.

5.2.3.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:781]

The Information Security Policy (SecPol) SHOULD include 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 information security incident management;
- change management; and
- information security awareness and training.

5.3. Security Risk Management Plans

Objective

5.3.1.   Security Risk Management Plans (SRMP) identify security risks and appropriate treatment measures for systems.

Context

Scope

5.3.2.   This section relates to the development of SRMPs, focusing on risks associated with the security of systems. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

5.3.3.   SRMPs may be developed on a functional basis, systems basis or project basis. For example, where physical elements will apply to all systems is use within that agency, a single SRMP covering all physical elements is acceptable. Generally each system will require a separate SRMP.

5.3.4.   The agency's risk identification and assessment process should include:

- How risks are found, recognised and described; and
- How sources of possible risks are to be considered.

References

5.3.5.   Information on the development of SRMPs can be found in:

Reference	Title	Publisher	Source
HB 436:2013	**Risk Management Guidelines**	Standards New Zealand	https://www.standards.co.nz
ISO/IEC 27005:2011	**Information Security Risk Management**	ISO/IEC	https://www.iso.org
ISO/IEC 22301:2019	**Business Continuity**	ISO/IEC	https://www.iso.org
ISO/IEC 31000:2018	**Risk Management - Guidelines**	ISO/IEC	https://www.iso.org
ISO/IEC 31010:2009	**Risk Management – Risk Assessment Techniques**	ISO/IEC	https://www.iso.org
ISO/IEC Guide 73:2009	**Risk Management - Vocabulary**	ISO/IEC	https://www.iso.org
ISO/IEC 19011:2018	**Guidelines for auditing management systems**	ISO/IEC	https://www.iso.org

ISO/IEC 27000:2018	Information technology - Security techniques - Information security management systems - Overview and vocabulary	ISO/IEC	https://www.iso.org
ISO/IEC 27001:2013	Information technology - Security techniques - Information security management systems - Requirements	ISO/IEC	https://www.iso27001security.com/html/27006.html
ISO/IEC 27006:2015	Information technology - Security techniques - Requirements for boies providing audit and certification of information security management systems	ISO/IEC	https://www.iso.org
ISO/IEC 27007:2020	Information technology - Security techniques - Guidelines for information security management systems auditing	ISO/IEC	https://www.iso.org
ISO/IEC TR 27008:2019	Guidelines for auditors on information security controls	ISO/IEC	https://www.iso.org
ISO/IEC 27017	Code of practice for information security	ISO/IEC	https://www.iso.org
ISO/IEC 27018:2014	Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	ISO/IEC	https://www.iso.org

Rationale & Controls

5.3.6. Agency and system specific security risks

5.3.6.R.01.   Rationale

While a baseline of security risks with associated levels of security risk and corresponding risk treatments are provided in this manual, agencies will almost certainly have variations to those considered during the security risk assessment. Such variations could be in the form of differing risk sources and threats, assets and vulnerabilities, or exposure and severity. In such cases an agency will need to follow its own risk management procedures to determine its risk appetite and associated risk acceptance, risk avoidance and risk tolerance thresholds. Risk owners **must** be identified.

5.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:802]

Agencies SHOULD determine agency and system specific security risks that could warrant additional controls to those specified in this manual.

5.3.7. Contents of SRMPs

5.3.7.R.01.   Rationale

Risks within an agency can be managed if they are not known, and if they are known, failing to treat or accept them is also a failure of risk management. For this reason SRMPs consist of two components, a security risk assessment and a corresponding treatment strategy.

5.3.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:805]

The Security Risk Management Plan SHOULD contain a security risk assessment and a corresponding treatment strategy.

5.3.8. Agency risk management

5.3.8.R.01.   Rationale

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.

5.3.8.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:808]

Agencies SHOULD incorporate their SRMP into their wider agency risk management plan.

5.3.9. Risk Management standards

5.3.9.R.01.   Rationale

For security risk management to be of true value to an agency there must be direct relevance to the specific circumstances of an agency and its systems, as well as being based on an industry recognised approach or risk management guidelines. For example, guidelines and standards produced by Standards New Zealand and the International Organization for Standardization.

The Protective Security Requirements requires that agencies adopt risk management approaches in accordance with ISO 31000:2018. Refer to PSR governance requirement GOV2.

Rationale

The International Organization for Standardization has developed an international risk management standard, including principles and guidelines on implementation, outlined in ISO 31000:2018, Risk Management – Guidlines. The terms and definitions for this standard can be found in ISO/IEC Guide 73, Risk Management – Vocabulary – Guidelines. The ISO/IEC 2700x series of standards also provides guidance.

5.3.9.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:812]

Agencies SHOULD develop their SRMP in accordance with international standards for risk management.

5.4. System Security Plans

Objective

5.4.1. System Security Plans (SecPlan) specify the information security measures for systems.

Context

Scope

5.4.2. This section relates to the development of SecPlans. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

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

Stakeholders

5.4.4. There can be many stakeholders involved in defining a SecPlan, 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;
- CISO, ITSM and system owners;
- system certifiers and accreditors;
- information management planning areas; and
- infrastructure management.

Rationale & Controls

5.4.5. Contents of SecPlans

5.4.5.R.01. Rationale

The NZISM 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 will need to determine which controls are in scope of the system and translate those controls to the SecPlan. These controls will then be assessed on their implementation and effectiveness during an information security assessment as part of the accreditation process.

5.4.5.R.02. Rationale

In performing accreditations against the latest baseline of this manual, agencies are ensuring that they are taking the most recent threat environment into consideration. GCSB 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.

5.4.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:828]

Agencies MUST select controls from this manual to be included in the SecPlan based on the scope of the system with additional system specific controls being included as a result of the associated SRMP. Encryption Key Management requires specific consideration; refer to Chapter 17 – Cryptography.

5.4.5.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:829]

Agencies SHOULD use the latest baseline of this manual when developing, and updating, their SecPlans as part of the certification, accreditation and reaccreditation of their systems.

5.4.5.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:831]

Agencies SHOULD include a Key Management Plan in the SecPlan.

5.5. Standard Operating Procedures

Objective

5.5.1. Standard Operating Procedures (SOPs) ensure security procedures are followed in an appropriate and repeatable manner.

Context

Scope

5.5.2. This section relates to the development of security related SOPs. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

5.5.3. Development of SOPs

5.5.3.R.01.   Rationale

In order to ensure that personnel undertake their duties in an appropriate manner, with a minimum of confusion, it is important that the roles of ITSMs, system administrators and system users are covered by SOPs. Furthermore, taking steps to ensure that SOPs are consistent with SecPlans will reduce the potential for confusion resulting from conflicts in policy and procedures.

5.5.3.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:844]

Agencies SHOULD develop SOPs for each of the following roles:

- ITSM;
- system administrator; and
- system user.

5.5.4. ITSM SOPs

5.5.4.R.01.   Rationale

The ITSM SOPs are intended to cover the management and leadership of information security functions within the agency.

5.5.4.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:849]

The following procedures SHOULD be documented in the ITSMs 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.
Information security incidents	Detecting, reporting and managing potential information security incidents.
	Establishing the cause of any information security incident, whether accidental or deliberate.
	Actions to be taken to recover and minimise the exposure from an information security incident.
	Additional actions to prevent reoccurrence.
Data transfers	Managing the review of media containing classified information that is to be transferred off-site.
	Managing the review of incoming media for malware or unapproved software.
IT equipment	Managing the disposal & destruction of unserviceable IT equipment and media.
System Patching	Advising and recommending system patches, updates and version changes based on security notices and related advisories.
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.
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.

5.5.5. System Administrator SOPs

5.5.5.R.01.   Rationale

The system administrator SOPs focus on the administrative activities related to system operations.

5.5.5.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:865]

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.
Incident response	Detecting, reporting and managing potential information security incidents.
	Establishing the cause of any information security incident, whether accidental or deliberate.
	Actions to be taken to recover and minimise the exposure from information security incident.
	Additional actions to prevent reoccurrence.

5.5.6. System User SOPs

5.5.6.R.01.   Rationale

The system user SOPs focus on day to day activities that system users need to be made aware of, and comply with, when using systems.

5.5.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:884]

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

Topic	Procedures to be included
Acceptable Use	Acceptable uses of the system(s).
End of day	How to secure systems at the end of the day.
Information security incidents	What to do in the case of a suspected or actual information security incident.
Media control	Procedures for handling and using media.
Passwords	Choosing and protecting passwords.
Temporary absence	How to secure systems when temporarily absent.

5.5.7. Agreement to abide by SOPs

5.5.7.R.01.   Rationale

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

5.5.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:889]

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

5.6. Incident Response Plans

Objective

5.6.1.   Incident Response Plans (IRP) outline actions to take in response to an information security incident.

Context

Scope

5.6.2.   This section relates to the development of IRPs to address information security, and not physical incidents within agencies. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

5.6.3. Contents of IRPs

5.6.3.R.01.   Rationale

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

5.6.3.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:902]

Agencies MUST include, as a minimum, the following content within their IRP:

- broad guidelines on what constitutes an information security incident;
- the minimum level of information security incident response and investigation training for system users and system administrators;
- the authority responsible for initiating investigations of an information security incident;
- the steps necessary to ensure the integrity of evidence supporting an information security incident;

- the steps necessary to ensure that critical systems remain operational;
- when and how to formally report information security incidents; and
- national policy requirements for incident reporting (see Chapter 7 – Information Security Incidents).

5.6.3.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:904]

Agencies SHOULD include the following content within their IRP:

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

5.7. Emergency Procedures

Objective

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

Context

Scope

5.7.2.   This section covers information relating to the securing of classified information and systems as part of the procedures for evacuating a facility in the event of an emergency.

5.7.3.   The safety of personnel is of paramount importance.

Rationale & Controls

5.7.4.   Evacuating facilities

5.7.4.R.01.   Rationale

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

5.7.4.R.02.   Rationale

During an evacuation, the safety of staff is of primary importance. Where it is immediately obvious to wardens and/or staff that the securing of classified information and systems prior to the evacuation of a facility would lead to, or exacerbate, serious injury or loss of life to personnel, the facility may be evacuated without personnel following the necessary procedures to secure classified information and systems.

5.7.4.R.03.   Rationale

Where facilities are evacuated and classified information and systems have NOT been secured, the Chief Warden or Floor Warden MUST be notified as soon as possible. Steps should be taken to secure the site as soon as it is safe to do so.

5.7.4.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:922]

Agencies MUST include in procedures for personnel evacuating a facility the requirement to secure classified information and systems prior to the evacuation.

5.8. Independent Assurance Reports

Objective

5.8.1.   To provide assurance to System Owners, Certifiers, Practitioners and Accreditors and to assist system designers, enterprise and security architects where assurance reviews cannot be directly undertaken on service providers.

Context

Scope

5.8.2.   Independent assurance reports are also variously referred to as third party assurance reporting, third party reviews, attestation reports and SAS 70 reports. It is important to note that SAS 70 has been superseded by the ISAE 3402 and SSAE 16 standards encompassing Type I and 2 and SOC 1, 2 and 3 reports. For reviews conducted in New Zealand the ISAE (NZ) 3402 or ISAE (NZ) 3000 standards are used. These various standards and report types are discussed later in this section. Agencies are likely to encounter a variety of report types, depending on the country of residence or country of jurisdiction of the service provider, or the geographic location of the data centre.

Purpose

5.8.3.   Many organisations are outsourcing key components of their business such as telecommunications, data storage and cloud based services. Managing third-party relationships is particularly challenging with services provided from outside New Zealand. The global nature of these services and the global nature of associated risks must be recognised by organisations. As outsourced services are becoming more integrated with organisation's operations, they will have a larger impact on organisation's governance, assurance and control frameworks. It is important to note that risk ownership and accountability remains with agencies and respective risk owners, even when responsibility for specific functions have been outsourced.

5.8.4.   Independent assurance reports provide customers and other interested parties with information on policies, procedures and controls related to the service provider's internal frameworks, control objectives and controls in cases where physical inspections and reviews by customers are impractical or not feasible. Service providers may also use the findings of such reports for their own purposes. These reports are used to understand the adequacy and effectiveness of the service provider's frameworks, control objectives, controls and implementation of controls. They allow:

- Business owners to identify and understand the risks associated with the service delivery;
- System owners to more fully assess system risks;
- System designers and security architects to make informed judgements on system structures, controls, defensive measures, and enterprise integration; and
- Regulators, certifiers and accreditors to obtain assurance over the service providers internal control structures and assess the suitability of system structures, controls and defensive measures.

5.8.5. An independent assurance review or third-party audit is invariably undertaken by independent auditors who are not employees of the service provider or their customers. There are two common types of independent third-party reviews: attestation reviews and direct non-attestation reviews.

5.8.6. Attestation reviews, such as an ISAE 3402 review (see below), are generally conducted by accounting or consulting organisations and are based upon recognised attestation standards issued by professional bodies such as the American Institute of Certified Public Accounts (AICPA) or the New Zealand External Reporting Board (XRB).

5.8.7. Direct or non-attestation reviews include those performed by IT consultants or others and may not follow standards referred to previously. They may be based upon other external standards or industry developed criteria such as ISO 2700x, ISACA's COBIT, the IIA, NIST, or the Cloud Security Alliance (CSA).

Assurance

5.8.8. Assurance is derived from an assessment of:

- A description of the service provider's business and control environment;
- Terms and conditions of the service contract or other legally binding agreement;
- Assertions supplied by the service provider (self-assessments);
- An independent validation of service provider assertions;
- Independent testing of controls implementation and effectiveness;
- Assurance in the service design and security architecture; and
- Assurance in the service components.

5.8.9. In general terms, the more ICT services that are outsourced in an agency, the less direct control and visibility the CE and management have over enterprise operations. Therefore, there is an increased reliance on assurance reporting from suppliers. Unless this is recognised in service contracts or legal agreements, agencies may find they are unable to obtain sufficient levels of assurance over the business services and enterprise operations.

Assurance Standards and schemes

ISAE (NZ) 3000

5.8.10. ISAE (NZ) 3000 (Revised) is issued by the External Reporting Board (XRB) of the New Zealand Audit and Assurance Standards Board and is the umbrella standard for other (non-financial) assurance engagements conducted in New Zealand. The standard covers a wide variety of engagements, ranging from assurance on statements about the effectiveness of internal control, for example, to assurance on sustainability reports and possible future engagements addressing integrated reporting. It is a principle-based standard that underpins current and future subject-specific ISAEs (NZ).

ISAE (NZ) 3402

5.8.11. In New Zealand the XRB issued the ISAE (NZ) 3402 in 2014, revised in 2016. This standard has essentially the same requirements as the international standard ISAE 3402 (see below), with some New Zealand specific adaptations. Australia, Singapore and many other jurisdictions have adopted this approach in the issue of this standard with some jurisdiction specific adaptations.

ISAE 3402

5.8.12. The most commonly used international standard for independent assurance reports is the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB), part of the International Federation of Accountants (IFAC).

5.8.13. Based on its predecessor standard SAS 70 (1992), ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organisations and their auditors (user auditors) on the controls at a service organisation that are likely to impact or be a part of the user organisation's system of internal control over financial reporting.

5.8.14. Auditing and associated consulting firms were required to use ISAE 3402 for all related work after June 2011.

ISAE 3402 Report Types

5.8.15. The ISAE 3402 provides for a report on controls at a point in time (Type 1 Report) or covering a specified period of time, usually between six and twelve months (Type 2 Report).

5.8.16. A Type 1 report is of limited use as it cannot cover the operating effectiveness of controls and is generally used for new operations where there is no evidence or documented history.

5.8.17. A Type 2 report not only includes the service organisation's description of controls, but also includes detailed testing of the service organisation's controls over a minimum six month period.

5.8.18. It is important to note that the descriptions Type 1 and Type 2 represent an audit approach and should not be confused with SOC 1, 2 and 3 reports under SSAE 16 (see below).

ISAE 3402 Report Uses and Limitations

5.8.19. This standard is used to obtain reasonable assurance about whether:

- The service organisation's description of its system fairly presents the system as designed and implemented throughout a specified period or a specific date;
- The controls related to the control objectives stated in the service organisation's description of its system were suitably designed throughout the specified period or at the specified date;
- Where included in the scope of the engagement, the controls were implemented and operated effectively to provide reasonable assurance that

the control objectives stated in the service organisation's description of its system were achieved throughout the specified period.

5.8.20. This ISAE applies only when the service organisation is responsible for, or otherwise able to make an assertion about, the suitable design of controls. It does not cover situations where:

- reporting only whether controls at a service organisation operated as described; or
- reporting on controls at a service organisation other than those related to a service relevant to user entities.

ISAE 3402 Report Content

5.8.21. The ISAE 3402 report usually comprises:

- The service auditor's report;
- Assertions by the service provider;
- A description of control objectives and controls provided by the service organisation;
- Results of any tests and other information provided by the independent auditor; and
- Any other information provided by the service provider.

US Standard SSAE 16

5.8.22. The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). It includes additional requirements to the superseded SAS 70 standard by requiring management to provide a written assertion (see below) regarding the design and operating effectiveness of the controls being reviewed. It is possible that agencies may encounter an SSAE16 based report for a US-based entity.

5.8.23. SSAE 16 is the US equivalent of the international ISAE 3402 and came into effect on
15 June 2011. While the SSAE 16 and ISAE 3402 standards have a common purpose and intent, , there are nine very specific requirements in SSAE 16, not covered in ISAE 3402:

- Intentional acts by the service providers staff;
- Anomalies;
- Direct assistance;
- Subsequent events;
- Statement restricting use of the service auditor's report;
- Disclaimer of Opinion;
- Documentation completion;
- Engagement acceptance and continuance; and
- Elements of the SSAE 16 report that are not required in the ISAE 3402 report.

5.8.24. These differences are summarised in the table below:

	SSAE 16	ISAE 3402
Use of report	Report specifically states it is restricted to intended users.	Report intended for user entities and their auditors but may include other restrictive use conditions.
Intentional Acts	Consideration of the impact of intention acts.	No requirement stated.
Subsequent Events	Auditors must consider Type 2 events after the report date.	Events after the report date are not considered.
Reporting	Sample deviations may not be discarded even when considered non-representative.	Sample deviations are assessed and may be discarded as not representative of the sample population.

5.8.25. The SSAE 16 standard specifies Type 1 and 2 audits (as does ISAE 3402).

5.8.26. A Type 1 is a report on a description of a service organisation's system and the suitability of the design of controls. A Type 1 report will test the design effectiveness of defined controls by examining a sample of one item per control. This provides a basic level of assurance that the organisation has some controls in place. It does not measure the completeness or effectiveness of these controls and represents a point in time.

5.8.27. A Type2 report is a report on policies and procedures placed in operation and tests of operating effectiveness for a specified period of time. A Type 2 report undertakes the tests in a Type 1 report together with an evaluation of the operating effectiveness of the controls for a period of at least six consecutive calendar months.

AICPA Service Organisation Control Reporting (SOC Reports)

5.8.28. Service Organization Control (SOC) Reports, often known as SOC 1, SOC 2, and SOC 3 Reports, are derived from a framework published by the American Institute of Certified Public Accountants (AICPA) for reporting on controls at service organisations.

5.8.29. In New Zealand, SOC 1 reports follow the ISAE (NZ) 3402 standard and SOC 2 reports are follow the ISAE (NZ) 3000 standard, in conjunction with the NZ Standard for Assurance Engagements SAE 3150, for assurance engagements on controls.

5.8.30. Each of the three SOC reports are designed to meet specific needs and reporting requirements for service organisations themselves, rather than being designed to provide assurance to third parties (customers). It is important to note that these reports follow the US (SSAE 16) and Canadian accounting standards, rather than the international ISAE 3402.

SOC 1 Report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting.
Reporting on controls relevant to internal control over financial reporting and usually conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 and AT 801 – Reporting on Controls at a Service Organization. A SOC 1 report can be based on a Type 1 or a Type 2 audit.

SOC 2 Report— Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. SOC 2 Reporting follows the AICPA AT Section 101 (not SSAE 16) and encompasses controls at service organisations on security, availability, processing Integrity, confidentiality and privacy. SOC 2 reports assist in comparing two or more data centres or service providers.

SOC 3 Report— Trust Services Report for Service Organizations. As well as reporting on controls relevant to security, availability, processing integrity, confidentiality and privacy a SOC 3 report provides the same level of assurance about controls over security, availability, processing integrity, confidentiality and/or privacy as a SOC 2 report. The key difference is that a SOC 3 report is intended for general release and does not include the detailed description of the testing performed by the auditor. In place of the detailed description a summary opinion regarding the effectiveness of the controls in place at the data centre or service organisation is provided.

SOC Reports Summary

Report	Standards	Content	Audience
SOC1 – Type 1	ISAE (NZ) 3402/ SAE 3150 or SSAE 16/AT 801	Internal controls over financial reporting at a point in time.	User auditors, organisation finance team, management.
SOC1 – Type 2	ISAE (NZ) 3402/ SAE 3150 or SSAE 16/AT 801	Internal controls over financial reporting over a specified time period, minimum 6 months.	User auditors, organisation finance team, management.
SOC2 – Type 1	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality and privacy controls at a point in time.	Management, regulators, third parties under Non-Disclosure Agreement.
SOC2 – Type 2	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality, privacy controls and operating effectiveness over a specified time period, minimum 6 months.	Management, regulators, third parties under Non-Disclosure Agreement.
SOC3	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality, privacy controls and operating effectiveness.	Public/general use version of SOC 2, excludes details of testing. Is less detailed and has less technical content than a SOC 2 report.

Management Assertions

5.8.31. See Assertions in Certification and Accreditation (NZISM 3.4.3 to 3.4.7) for a short discussion on the nature and purpose of assertions.

5.8.32. The SSAE 16 requires a written assertion by management. Also known as a management's assertion or service organisation assertion it is essentially an assertion made by the service organisation representing and asserting to a number of elements, including:

- The description fairly presents the service organisation's system;
- That the control objectives were suitably designed (SSAE 16 Type 1) and operating effectively (SSAE 16 Type 2) during the dates and/or periods covered by the report; and
- The criteria used for making these assertions, (which are additional statements with supporting matter regarding risk factors relating to control objectives and underlying controls) were in place (Type 1) and were consistently applied (Type 2).

ISO/IEC 27001 Certification

5.8.33. ISO/IEC 27001 is an international standard that provides a framework for Information Security Management Systems. The standard is designed to help organisations of all sizes and types to select suitable and proportionate security controls for information. It provides a structured approach to assist in managing risk by identifying information security vulnerabilities and selecting appropriate controls.

5.8.34. This standard enables independent, external certification bodies to audit the ISMS and certify that the requirements of the standard have been met. Such certification is another means of deriving assurance over the operations of service providers. The requirements for certification are described in the ISO/IEC 27006:2015 standard. Certification is based on two reviews:

- Stage 1 audit (also called Documentation review) checking the systems documentation is compliant with ISO 27001;
- Stage 2 audit (also called Main audit) checking that all the organisation's activities are compliant with both ISO 27001 and the systems documentation.

Other Guidance

Cloud Security Alliance's Security, Trust and Assurance Registry (STAR) Attestation

5.8.35. STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider. It is based on the ISAE 3402 and SSAE 16 standards, supplemented by the criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

5.8.36. STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing service providers. The registry lists three levels of assurance:

1. Self-assessment;
2. Third party assessment based attestation or certification; and
3. Continuous monitoring based certification.

Note: Agencies should note that a self-assessment does not necessarily provide substantive assurance.

5.8.37. As at March 2017, the STAR scheme is still to be fully implemented although there are a number of cloud service providers listed in the registry.

5.8.38. Agencies can use this registry to further inform their judgement on the robustness of assurance over cloud service provider's internal operations and implementation of security controls.

Cloud Security Alliance's Cloud Controls Matric (CCM)

5.8.39. The CCM covers 16 control domains and provides fundamental security principles to guide cloud service providers and to assist prospective cloud customers in assessing the overall security risk of a cloud service provider.

5.8.40. The CCM references and maps its controls to internationally accepted industry standards, regulations, and control frameworks, such as ISO 27001/2/17/18, PCI: DSS v3, and AICPA 2014 Trust Service Principles and Criteria, Germany's BIS, Canada's PIPEDA, ISACA's COBIT, the US FedRAMP, HIPAA, Jericho Forum, NIST and the NZISM.

Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ)

5.8.41. The CAIQ is an extension to the CCM that provides exemplar control assertion questions that can be asked of service providers in the context of each CCM control, and can be tailored to suit each unique cloud customer's evidentiary requirements. GCDO maintain a mapping of the CAIQ questions to the *GCDO Cloud Security and Privacy Considerations* question set to further aid agencies in use of the CAIQ as an alternative to equivalent GCDO questions.

ISACA IT Audit and Assurance Program for Cloud Computing

5.8.42. Based on ISACA's IT Assurance Framework (ITAF), the Cloud Computing Assurance Program was developed as a comprehensive and good-practice model, aligned with the ISACA COBIT 5 framework. Building on the generic assurance program, the cloud computing guidance identifies a number of cloud specific risk areas encompassing:

- Greater dependency on third parties;
- Increased complexity of compliance with national and international laws and regulations;
- Reliance on the Internet as the primary conduit to the enterprise's data; and
- Risk due to the dynamic nature of cloud computing.

5.8.43. The ITAF assurance focus is on:

- The governance affecting cloud computing;
- The contractual compliance between the service provider and customer;
- Privacy and regulation issues concerning cloud computing; and
- Cloud computing specific attention points.

5.8.44. It is important to note that this cloud computing assurance review is not designed to provide assurance on the design and operational effectiveness of the cloud computing service provider's internal controls, as this assurance is often provided through ISAE 3604 or similar reviews.

5.8.45. The cloud computing assurance review focusses on the agency's or organisation's systems design and operational effectiveness in relation to cloud services. It is also important to note that this is dependent on the effectiveness of the underlying system design and controls and how well these are implemented and managed.

ASD Certified Cloud Services

5.8.46. The Australian Signals Directorate (ASD) conducts certification of cloud services based in Australia for Australian government use. ASD Certifications are based on the Australian Government Information Security Manual (ISM). It is important to note that there are detail differences between the Australian ISM and the NZISM and these documents have a different legislative and regulatory basis.

5.8.47. The ASD Cloud Computing Security documents describe security risk mitigations associated with cloud computing. Australian Government agencies are also required to perform due diligence reviews of the legal, financial and privacy risks associated with procuring cloud services, aspects which are not covered by the ASD certification.

NIST 800-53

5.8.48. The NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations is the US unified information security framework for US federal government agencies. The New Zealand equivalent is the NZISM.

5.8.49. The underlying mandates are in FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems and FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems. US federal government agencies are required to categorise and analyse their system in terms of FIPS 199 and 200 then apply appropriate controls from NIST 800-53.

FedRAMP

5.8.50. The US Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program intended to provide a standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services. This approach is designed to provide reusable cloud security assessments in order to reduce cost, resource and time. In addition it was intended to minimise cybersecurity risk for Federal Agencies as they move operations to the cloud, provide consistent baseline security policies and streamline the procurement process.

5.8.51. FedRAMP is a collaboration of cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

The FedRAMP programme is run by the FedRAMP Program Management Office as part of the GSA.

5.8.52. FedRAMP is mandatory for Federal Agency cloud deployments at all risk impact levels. Private cloud deployments from single agencies and fully implemented within federal facilities are an exception to this mandate. Quaterly reporting by each agency on their cloud portfolio is required.

5.8.53. FedRAMP authorises cloud systems in a three step process:

1. **Security Assessment:** The security assessment process uses a standardised set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls with additional controls specific to cloud deployments, in order to grant security authorisations. Cryptographic elements are governed by the FIPS 140-2 standards.

2. **Leveraging and Authorisation:** Federal agencies view security authorisation packages in the FedRAMP repository and leverage the security authorisation packages to grant a security authorisation at their own agency.

3. **Ongoing Assessment & Authorisation:** Once an authorisation is granted, ongoing assessment and authorisation activities are required to maintain the security authorisation.

5.8.54. Again it is important to note that the FedRAMP assessments are conducted on a different legislative and regulatory basis to assessments conducted in New Zealand. A variety of guidance, controls, templates and other documentation is available online from the GSA (see References - Assurance Guidance)

PCI DSS

5.8.55. The Payment Card Industry Security Standards Council was formed by major credit card organisations and is a global open body formed to develop and promote understanding of essential security standards for payment account security. It develops, maintains and promotes the Payment Card Industry Data Security Standards (PCI DSS). It also provides tools to assist the implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

5.8.56. This standard is designed to protect cardholder data (credit and debit cards) held by merchants, banks and other financial organisations. It applies to all organisations that accept, store, process and transmit credit cardholder data.

5.8.57. This standard is narrowly focussed and has specific applicability to New Zealand Government agencies that operate financial transaction services (e.g. AoG Banking services and citizen fee-paying services; such as vehicle registration, passport renewal, etc.). The PCI has published an information supplement on Third-Party Security Assurance (updated March 2016).

COSO

5.8.58. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initially developed the COSO Internal Control-Integrated Framework in 1992. A revised framework was published in 2013 which included guidance on "outsourced service providers" and how they impact risk assessment, controls, monitoring, information flows and assurance. The 2013 Framework incorporates how organisations should manage IT innovation in light of globalisation, complex business processes, regulatory demands and security risk assessments. It is frequently used as the basis for SSAE16 assignments and the production of SOC reports.

References – Assurance Standards

5.8.59. Further information on Assurance Standards can be found in:

Reference	Title	Publisher	Source
	International Standard on Assurance Engagements (ISAE) 3402 - Assurance Reports on Controls at a Service Organization	International Federation of Accountants (IFAC)	http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf
	Reporting on Controls at a Service Organization - SSAE No. 16	AICPA	http://www.aicpastore.com/AST/Main/CPA2BIZ_Primary/InformationManagementTechnologyAssurance/PRDOVR~PC-023035/PC-023035.jsp
	Service Organization Controls (SOC) Reports for Service Organizations	AICPA	http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx
	AT Section 101 Attest Engagements	AICPA	http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00101.pdf
	AT Section 801 Reporting on Controls at a Service Organization	AICPA	http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf
	COBIT 5 Framework	ISACA	http://www.isaca.org/cobit/Pages/CobitFramework.aspx
ISAE (NZ) 3000 (Revised)	Assurance Engagements Other than Audits or Reviews of Historical Financial Information	XRB	https://xrb.govt.nz/Site/Auditing_Assurance_Standards/Current_Standards/Other_Assurance_Engagements_Standards.aspx
ISAE (NZ) 3402	Assurance Reports on Controls at a Service Organisation	XRB	https://xrb.govt.nz/Site/Auditing_Assurance_Standards/Current_Standards/Other_Assurance_Engagements_Standards.aspx
SAE 3150	Standard on Assurance Engagements 3150	XRB	https://xrb.govt.nz/Site/Auditing_Assurance_Standards/Current_Standards/Other_Assurance_Engagements_Standards.aspx

NIST Special Publication 800-53 Revision 4	Security and Privacy Controls for Federal Information Systems and Organizations	NIST	http://csrc.nist.gov/publications/nistpubs
NIST Special Publication 500-299 (Draft)	NIST Cloud Computing Security Reference Architecture	NIST	http://csrc.nist.gov/publications/nistpubs
	Information Supplement: Third-Party Security Assurance	PCI Security Standards Council	https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf
ISO 19011:2018	Guidlines for Auditing Management Systems	ISO	https://www.iso.org/standard/50675.html
ISO/IEC 27000:2018	Information security management systems — Overview and vocabulary	ISO	http://www.iso.org/
ISO/IEC 27001:2013	Information security management systems — Requirements	ISO	http://www.iso.org/
ISO/IEC 27006:2015	Requirements for bodies providing audit and certification of information security management systems	ISO	http://www.iso.org/
ISO/IEC 27007:2020	Guidelines for information security management systems auditing	ISO	http://www.iso.org/
ISO/IEC TR 27008:2019	Guidelines for auditors on information security controls	ISO	http://www.iso.org/
ISO/IEC 27014	Governance of information security	ISO	http://www.iso.org/
ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO	http://www.iso.org/
ISO/IEC 27018:2014	ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	ISO	http://www.iso.org/

References – Assurance Guidance

5.8.60.

Title	Publisher	Source
FAQs — New Service Organization Standards and Implementation Guidance	American Institute of Certified Public Accountants (AICPA)	http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/faqs_service_orgs.pdf
The Federal Risk and Authorization Management Program (FedRAMP)	General Services Administration, US Federal Government	https://www.fedramp.gov/
FedRAMP Documents	General Services Administration, US Federal Government	https://www.fedramp.gov/documents/
FedRAMP Templates	General Services Administration, US Federal Government	https://www.fedramp.gov/templates/
Controls and Assurance in the Cloud Using COBIT 5	ISACA	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx
Special Publication 800-115 Technical Guide to Information Security Testing and Assessment	NIST	http://csrc.nist.gov/publications/nistpubs
Cloud Security Guidance	NCSC UK	https://www.ncsc.gov.uk/guidance/cloud-security-collection

Cloud Security Guidance: Implementing Cloud Security Principles	NCSC UK	https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
ASD Certified Cloud Services	ASD	http://www.asd.gov.au/infosec/irap/certified_clouds.htm
Security Framework for Governmental Clouds	ENISA	https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds
Good Practice Guide for securely deploying Governmental Clouds	ENISA	https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds
Security & Resilience in Governmental Clouds	ENISA	https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds
Assurance on non-financial information Existing practices and issues, July 2008, ISBN 978-1-84152-604-1	Institute of Chartered Accountants in England and Wales (ICAEW).	Assurance on non-financial information existing practices and issues (PDF)
IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, January 2013	The Institute of Internal Auditors (IIA)	The three lines of defense in effective risk management and control (PDF)
Cloud Security Alliance Reference Architecture	Cloud Security Alliance	https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.pdf
Cloud Controls Matrix v3.0.1 (6-6-16 Update)	Cloud Security Alliance	https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1	Cloud Security Alliance	https://cloudsecurityalliance.org/media/news/ccm-caiq-v3-0-1-soft-launch/
Security Guidance for Critical Areas of Focus in Cloud Computing V3.0	Cloud Security Alliance	https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
About CSA STAR Attestation	Cloud Security Alliance	https://cloudsecurityalliance.org/star/attestation/
Guidelines for CPAs Providing CSA STAR Attestation	Cloud Security Alliance	https://cloudsecurityalliance.org/download/guidelines-for-cpas-providing-csa-star-attestation/
CSA Security, Trust & Assurance Registry (STAR)	Cloud Security Alliance	https://cloudsecurityalliance.org/star/#star_m
Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures Version 3. 02 April 2016	PCI Security Standards Council	https://www.pcisecuritystandards.org/
Enterprise Risk Management — Integrated Framework	COSO	http://www.coso.org/documents/coso_erm_executivesummary.pdf
Internal Control – Integrated Framework	COSO	http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

Rationale & Controls

5.8.61.   Risk Assessment

5.8.61.R.01.   Rationale

The Security Risk Management Plan (SRMP – Section 5.3) encompasses all risks associated with the security of agency systems. The growth in outsourced services, particularly cloud services, has created situations where risk, controls and assurance cannot be directly examined and assessed. In such cases independent assurance reports are an effective means, possibly the only means, of obtaining some assurance on the service provider's operations.

5.8.61.R.02.   Rationale

No single independent assurance scheme/standard covers the full range of considerations and control requirements of the NZISM. Agencies may find duplication of aspects analysed if multiple schemes are applied. . It is also important to note that none of the common mature assurance schemes cover specific government requirements and handling of Official Information; such as the personnel aspects (PERSEC) of user and administration vetting and security clearances, or sovereignty aspects of the information/data. Careful selection and consideration is required when placing reliance on reports available for a particular outsourced or cloud service.

5.8.61.R.03.   Rationale

Reports from different assurance scheme have varying levels of detail as well as risk area coverage. Selection and usage of reports should be considered in the context of the intended service/system business and information value.

Understanding the business and technical risk context will drive the size and depth of a risk assessment, and the associated assurance process. Though even a lighter-weight risk assurance process will follow the C&A process model, such that the CE or authorised delegate is still formally accountable and responsible.

Re-use of assessments completed by other agencies is encouraged, noting the business or information value context may differ. To assist agencies and promote efficiency, the GCDO facilitates the sharing and re-use of existing cloud assessment materials among agencies.

5.8.61.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1019]

Agencies MUST conduct a risk assessment in order to determine the type and level of independent assurance required to satisfy certification and accreditation requirements.

5.8.61.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1020]

In all cases where assurance on service provider operations cannot be obtained directly, agencies SHOULD obtain independent assurance reports.

5.8.61.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1021]

In order to address identified risk areas, agencies SHOULD obtain relevant assurance reports and service provider certifications to inform a risk assessment and Certification activities as well as other aspects of the certification processes such as evidence of controls effectiveness and remediation plans.

5.8.62.   Independent Assurance

5.8.62.R.01.   Rationale

Independent assurance can be obtained directly from the service provider through Service Organisation Control (SOC) reports, as well as other internationally recognised assurance frameworks. It will be important to corroborate individual reports by comparison with other reporting mechanisms and independent certifications.

5.8.62.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1024]

Agencies MUST incorporate the results of any independent assurance reports into the agency Certification process, to understand the residual risk position and controls required to manage risk appropriately.

6. Information security monitoring

6.1. Information Security Reviews

Objective

6.1.1.   Information security reviews maintain the security of agency systems and detect gaps and deficiencies.

Context

Scope

6.1.2.   This section covers information on conducting reviews of any agency's information security posture and security implementation.

Information security reviews

6.1.3.   An information security review:

- identifies any changes to the business requirements or concept of operation for the subject of the review;
- identifies any changes to the security risks faced by the subject of the review;
- assesses the effectiveness of the existing counter-measures;
- validates the implementation of controls and counter-measures; and
- reports on any changes necessary to maintain an effective security posture.

6.1.4.   An information security review can be scoped to cover anything from a single system to an entire agency's systems.

References

6.1.5.   Additional information relating to system auditing is contained in:

Reference	Title	Publisher	Source

ISO/IEC 27006:2015	Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems	ISO/IEC	http://www.iso27001security.com/html/27006.html http://www.standards.co.nz
ISO/IEC 27007:2020	Information Technology – Security Techniques - Guidelines for information security management systems auditing	ISO/IEC	http://www.iso27001security.com/html/27007.html http://www.standards.co.nz
ISO/IEC 27008:2019	Information Technology – Security Techniques - Guidelines for Auditors on information security controls	ISO/IEC	http://www.iso27001security.com/html/27008.html http://www.standards.co.nz

PSR references

6.1.6.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/
PSR content protocols	Management protocol for information security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/
PSR requirements sections	Self assessment & reporting Review your security measures	https://www.protectivesecurity.govt.nz/self-assessment-and-reporting/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/validate-your-security-measures/

Rationale & Controls

6.1.7.   Conducting information security reviews

6.1.7.R.01.   Rationale

Annual reviews of an agency's information security posture can assist with ensuring that agencies are responding to the latest threats, environmental changes and that systems are properly configured in accordance with any changes to information security documentation and guidance.

6.1.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1040]

Agencies SHOULD undertake and document information security reviews of their systems at least annually.

6.1.8.   Managing Conflicts of Interest

6.1.8.R.01.   Rationale

Reviews may be undertaken by personnel independent of the target of evaluation or by an independent third party to ensure that there is no (perceived or actual) conflict of interest and that an information security review is undertaken in an objective manner.

6.1.8.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1043]

Agencies SHOULD have information security reviews conducted by personnel independent to the target of the review or by an independent third party.

6.1.9.   Focus of information security reviews

6.1.9.R.01.   Rationale

Incidents, significant changes or an aggregation of minor changes may require a security review to determine and support any necessary changes and to demonstrate good systems governance. An agency may choose to undertake an information security review:

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

6.1.9.R.02.   Rationale

In order to review risk, an information security review should analyse the threat environment and the highest classification of information that is stored, processed or communicated by that system.

6.1.9.R.03.   Rationale

Depending on the scope and subject of the information security review, agencies may gather information on areas including:

- agency priorities, business requirements and/or concept of operations;
- threat data;
- risk likelihood and consequence estimates;
- effectiveness of existing counter-measures;
- other possible counter-measures;
- changes to standards, policies and guidelines;
- recommended good practices; and
- significant system incidents and changes.

6.1.9.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1048]

Agencies SHOULD review the components detailed in the table below.

Component	Review
Information security documentation	The SecPol, Systems Architecture, SRMPs, SecPlans, SitePlan, SOPs the IRP, and any third party assurance reports.
Dispensations	Prior to the identified expiry date.
Operating environment	When an identified threat emerges or changes, an agency gains or loses a function or the operation of functions are moved to a new physical environment.
Procedures	After an information security incident or test exercise.
System security	Items that could affect the security of the system on a regular basis.
Threats	Changes in threat environment and risk profile.
NZISM	Changes to baseline or other controls, any new controls and guidance.

6.2. Vulnerability Analysis

Objective

6.2.1. Exploitable information system weaknesses can be identified by vulnerability analyses and inform assessments and controls selection.

Context

Scope

6.2.2. This section covers information on conducting vulnerability assessments on systems as part of the suite of good IT governance activities.

Changes as a result of a vulnerability analysis

6.2.3. It is important that normal change management processes are followed where changes are necessary in order to address security risks identified in a vulnerability analysis.

Rationale & Controls

6.2.4. Vulnerability analysis strategy

6.2.4.R.01. Rationale

Vulnerabilities may be unintentionally introduced and new vulnerabilities are constantly identified, presenting ongoing risks to information systems security.

6.2.4.R.02. Rationale

While agencies are encouraged to monitor the public domain for information related to vulnerabilities that could affect their systems, they should not remain complacent if no specific vulnerabilities relating to deployed products are disclosed.

6.2.4.R.03. Rationale

In some cases, vulnerabilities can be introduced as a result of poor information security practices or as an unintended consequence of activities within an agency. As such, even if no new public domain vulnerabilities in deployed products have been disclosed, there is still value to be gained from regular vulnerability analysis activities.

6.2.4.R.04. Rationale

Furthermore, monitoring vulnerabilities, conducting analysis and being aware of industry and product changes and advances, including NZISM requirements, provides an awareness of other changes which may adversely impact the security risk profile of the agency's systems.

6.2.4.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1063]

Agencies SHOULD implement a vulnerability analysis strategy by:

- monitoring public domain 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 that only allowed services are active and that disallowed services are prevented;
- using security checklists for operating systems and common applications; and
- examining any significant incidents on the agency's systems.

6.2.5. Conducting vulnerability assessments

6.2.5.R.01. Rationale

A baseline or known point of origin is the basis of any comparison and allows measurement of changes and improvements when further information security monitoring activities are conducted.

6.2.5.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1066]

Agencies SHOULD conduct vulnerability assessments in order to establish a baseline. This SHOULD be done:

- before a system is first used;
- after any significant incident;
- after a significant change to the system;
- after changes to standards, policies and guidelines;
- when specified by an ITSM or system owner.

6.2.6. Resolving vulnerabilities

6.2.6.R.01. Rationale

Vulnerabilities may occur as a result of poorly designed or implemented information security practices, accidental activities or malicious activities, and not just as the result of a technical issue.

6.2.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1069]

Agencies SHOULD analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment.

6.3. Change Management

Objective

6.3.1. To ensure information security is an integral part of the change management process, it should be incorporated into the agency's IT maintenance governance and management activities.

Context

Scope

6.3.2. This section covers information on identifying and managing routine and urgent changes to systems.

Identifying the need for change

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

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

Types of system change

6.3.4. A proposed change to a system could involve:

- an upgrade to, or introduction of IT equipment;
- an upgrade to, or introduction of software;
- environment or infrastructure change; or
- major changes to access controls.

PSR references

6.3.5. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/
PSR content protocols	Management protocol for information security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/

Rationale & Controls

6.3.6.   Change management

6.3.6.R.01.   Rationale

A considered and accountable process requires consultation with all stakeholders before any changes are implemented. In the case of changes that will affect the security or accreditation status of a system, the Accreditation Authority is a key stakeholder and will need to be consulted and grant approval for the proposed changes.

6.3.6.R.02.   Rationale

Change management processes are most likely to be bypassed or ignored when an urgent change needs to be made to a system. In these cases it is essential that the agency's change management process strongly enforces appropriate actions to be taken before and after an urgent change is implemented.

6.3.6.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1088]

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 or accreditation status of a system is submitted to the Accreditation Authority for approval; and
- all associated information security documentation is updated to reflect the change.

6.3.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1089]

Agencies SHOULD 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 or accreditation status is submitted to the Accreditation Authority for approval; and
- all associated information security documentation is updated to reflect the change.

6.3.7.   Change management process

6.3.7.R.01.   Rationale

Uncontrolled changes pose risks to information systems as well as the potential to cause operational disruptions. A change management process is fundamental to ensure a considered and accountable approach with appropriate approvals. Furthermore, the change management process provides an opportunity for the security impact of the change to be considered and if necessary, reaccreditation processes initiated.

6.3.7.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1093]

An agency's change management process MUST define appropriate actions to be followed before and after urgent changes are implemented.

6.3.7.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1094]

An agency's change management process SHOULD define appropriate actions to be followed before and after urgent changes are implemented.

6.3.7.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1095]

Agencies SHOULD follow this change management process outline:

- produce a written change request;
- submit the change request to all stakeholders for approval;
- document the changes to be implemented;
- test the approved changes;
- notification to user of the change schedule and likely effect or outage;
- implement the approved changes after successful testing;
- update the relevant information security documentation including the SRMP, SecPlan 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; and
- continually educate system users in regards to changes.

6.3.8.   Changes impacting the security of a system

6.3.8.R.01.   Rationale

The accreditation of a system accepts residual security risk relating to the operation of that system. Changes may impact the overall security risk for the system. It is essential that the Accreditation Authority is consulted and accepts the changes and any changes to risk.

6.3.8.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1098]

When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the

6.4. Business Continuity and Disaster Recovery

Objective

6.4.1.   To ensure business continuity and disaster recovery processes are established to assist in meeting the agency's business requirements, minimise any disruption to the availability of information and systems, and assist recoverability.

Context

Scope

6.4.2.   This section covers information on business continuity and disaster recovery relating specifically to systems.

References

6.4.3.   Additional information relating to business continuity is contained in:

Reference	Title	Publisher	Source
ISO/IEC 22301:2019	Societal Security – Business Continuity Management Systems - Requirements.	**ISO/IEC**	http://www.iso.org http://www.standards.co.nz
ISO/IEC 27001:2013	Information Technology – Security Techniques - Information Security Management Systems - Requirements	**ISO/IEC**	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
ISO/IEC 27002:2013	Information Technology – Security Techniques – Code of Practice for Information Security Controls	**ISO/IEC**	http://www.iso27001security.com/html/27002.html http://www.standards.co.nz
ISO/IEC 27005:2011	Information Technology – Security Techniques - Information Security Risk Management	**ISO/IEC**	http://www.iso27001security.com/html/27005.html http://www.standards.co.nz
ISO/IEC 27031:2011	Information Technology – Security Techniques - Guidelines for Information and Communication Technology readiness for Business Continuity	**ISO/IEC**	http://www.iso27001security.com/html/27005.html http://www.standards.co.nz
SAA/SNZ HB 221:2004	Business Continuity Management	**SAA/SNZ**	http://www.standards.co.nz

PSR references

6.4.4.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, GOV7, INFOSEC1 and PHYSEC1	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Business continuity management	https://www.protectivesecurity.govt.nz/governance/business-continuity-management/

Rationale & Controls

6.4.5.   Availability requirements

6.4.5.R.01.   Rationale

Availability and recovery requirements will vary based on each agency's business needs and are likely to be widely variable across government. Agencies will determine their own availability and recovery requirements and implement measures consistent with the agency's SRMP to achieve them as part of their risk management and governance processes.

6.4.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1120]

Agencies MUST determine availability and recovery requirements for their systems and implement measures consistent with the agency's

SRMP to support them.

6.4.6.   Backup strategy

6.4.6.R.01.   Rationale

Having a backup strategy in place is a fundamental part of business continuity planning. The backup strategy ensures that critical business information is recoverable if lost. Vital records are defined as any information, systems data, configurations or equipment requirements necessary to restore normal operations.

6.4.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1123]

Agencies SHOULD:

- Identify vital records;
- backup all vital records;
- store copies of critical information, with associated documented recovery procedures, offsite and secured in accordance with the requirements for the highest classification of the information; and
- test backup and restoration processes regularly to confirm their effectiveness.

6.4.7.   Business Continuity plan

6.4.7.R.01.   Rationale

It is important to develop a business continuity plan to assist in ensuring that critical systems and data functions can be maintained when the system is operating under constraint, for example, when bandwidth is unexpectedly limited below established thresholds.

6.4.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1126]

Agencies SHOULD develop and document a business continuity plan.

6.4.8.   Disaster recovery plan

6.4.8.R.01.   Rationale

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

6.4.8.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1129]

Agencies SHOULD develop and document a disaster recovery plan.

7. Information Security Incidents

7.1. Detecting Information Security Incidents

Objective

7.1.1.   To ensure that appropriate tools, processes and procedures are implemented to detect information security incidents, in order to minimise the impact of such incidents and as part of the suite of good IT governance activities.

Context

Scope

7.1.2.   This section covers information relating to detecting information security incidents. Detecting physical and personnel security incidents is out of scope of this section, unless there is an impact on information systems. Refer to Chapter 8 - Physical Security and Chapter 9 - Personnel Security.

7.1.3.   It is important to note that in most cases, information systems are likely to be affected.

7.1.4.   Additional information relating to detecting information security incidents, and topics covered in this section, can be found in the following sections of this manual:

- Section 6.1 - Information Security Reviews;
- Section 6.2 - Vulnerability Analysis;
- Section 7.2 – Reporting Information Security Incidents;
- Section 7.3 – Managing Information Security Incidents;
- Section 9.1 - Information Security Awareness and Training;
- Section 16.5 - Event Logging and Auditing;
- Section 17.9 – Key Management; and
- Section 18.4 - Intrusion Detection and Prevention.

References

7.1.5.   Standards and guidance published by Standards Bodies and industry groups include:

Title	Publisher	Source
ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management	ISO	https://www.iso.org/standard/60803.html

ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response	ISO	https://www.iso.org/standard/62071.html
Definitions of Security Incident	NIST	https://csrc.nist.gov/glossary/term/security-incident
Computer Security Incident Handling Guide Special Publication 800-61 Revision 2	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
Incident Definition	US-CERT	https://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition
New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)	GCSB/NCSC	https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf
Incident Handler's Handbook	SANS	https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
ITIL – A guide to incident management	ITIL	https://www.ucisa.ac.uk
Incident Management and Response	ISACA	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Incident-Management-and-Response.aspx
Cyber Security Incident Response Guide	CREST	https://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide-1.pdf
Good Practice Guide for Incident Management	ENISA	https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

PSR references

7.1.6.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV6, GOV7, INFOSEC1 and INFOSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/
PSR content protocols	Management protocol for information security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/
PSR requirements sections	Reporting incidents and conducting security investigations	https://www.protectivesecurity.govt.nz/governance/reporting-incidents-and-conducting-security-investigations/

Rationale & Controls

7.1.7.   Preventing and detecting information security incidents

7.1.7.R.01.   Rationale

Processes and procedures for the detection of information security incidents will assist in mitigating attacks using the most common vectors in systems exploits.

7.1.7.R.02.   Rationale

New or advanced attacks and exploits can frequently be detected through other metrics and effects, rather than direct identification.

7.1.7.R.03.   Rationale

Many potential information security incidents are noticed by personnel rather than automated or other software tools. Personnel should be well trained and aware of information security issues and indicators of possible information security incidents.

7.1.7.R.04.   Rationale

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

Tool	Description
Network and host Intrusion Detection Systems (IDSs)	Monitor and analyse network and host activity, usually relying on a list of known attack signatures to recognise/detect malicious activity and potential information security incidents.

Anomaly detection systems	Monitor network and host activities that do not conform to normal system activity.
Intrusion Prevention Systems (IPS) and Host Based Intrusion Prevention Systems (HIPS)	Some IDSs are combined with functionality to counter detected attacks or anomalous activity (IDS/IPS).
System integrity verification and integrity checking	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.
Log analysis	Involves collecting and analysing event logs using pattern recognition to detect anomalous activities.
White Listing	Lists the authorised activities and applications and permits their usage.
Black Listing	Lists the non-authorised activities and applications and prevents their usage.
Data Loss Prevention (DLP)	Data Egress monitoring and control.

7.1.7.R.05.   Rationale

Automated tools are only as good as their implementation and the level of analysis they perform. If tools are not configured to assess all areas of potential security risk then some vulnerabilities or attacks will not be detected. In addition, if tools are not regularly updated, including updates for new vulnerabilities and attack methods, their effectiveness will be reduced.

7.1.7.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1153]

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

- user awareness and training;
- counter-measures against malicious code, known attack methods and types;
- intrusion detection strategies;
- data egress monitoring & control;
- access control anomalies;
- audit analysis;
- system integrity checking; and
- vulnerability assessments.

7.1.7.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1154]

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

- user awareness and training;
- counter-measures against malicious code, known attack methods and types;
- intrusion detection strategies;
- data egress monitoring & control;
- access control anomalies;
- audit analysis;
- system integrity checking; and
- vulnerability assessments.

7.1.7.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1155]

Agencies SHOULD use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention versus resources allocated to detection of information security incidents.

7.2. Reporting Information Security Incidents

Objective

7.2.1.   To ensure reporting information security incidents is incorporated as an essential part of incident management, whether the reporting is within an agency or reports are provided to another government agency.

7.2.2.   This assists in maintaining an accurate threat environment picture for government systems, particularly when All-of-Government (AoG) or multi-agency systems are involved.

Context

Scope

7.2.3.   This section covers information relating specifically to the reporting of **information security** incidents. It does **not** cover the reporting of physical or personnel security incidents **unless** there is an impact on information systems.

7.2.4.   It is important to note that, in most cases, information systems are likely to be affected.

Requirement for information security incident reporting

7.2.5.   The requirement to report an information security incident report applies irrespective of whether incident management is internally managed or if an agency has outsourced some or all of its information technology functions and services.

7.2.6. The information security threat and intelligence landscape continues to evolve, partly driven by more advanced, capable, well-resourced and motivated adversaries, as well as the need to improve management and governance of information systems. To assist in managing these requirements, a standardised form of information exchange is essential.

7.2.7. The requirement for incident reporting has existed for many years, and guidance can be found in various standards and good practice guidance (see References at 7.2.16).

Historical Notes

7.2.8. While the requirement for incident reporting has been in place for many years, the reporting mechanism has changed over time:

- Incident categories, incident types and resolution types were previously defined in the Incident Object Description Exchange Format (IODEF) standard. IODEF was an e-GIF standard.
- IODEF was superseded by a group of protocols designed to automate and structure operational cybersecurity information sharing techniques on a global basis. International in scope and free for public use, TAXII, STIX and CybOX are community-driven technical specifications designed to enable automated information sharing.
- These protocols continued to evolve with CybOX absorbed into the protocol suite and no longer separately identified.
- An alternative to TAXII and STIX is VERIS (The vocabulary for Event Recording and Incident Sharing), a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner.
- Previously New Zealand's National Cyber Security Centre (NCSC) had adopted this suite of protocols as the basis for incident reports to the NCSC and for reports issued by the NCSC.
- It was found, however, that agencies were not always able to utilise these protocols and **the requirement for reporting using these protocols has been withdrawn by the NCSC**.

Background

7.2.9. Security Incidents are frequently also termed "a hack", "a breach", "a compromise" and "a cyber attack". The more colloquial terms may not correctly describe the nature and effect of the incident and should be used with care, if used at all. It is important to note that security incidents include physical incidents (such as lost documents) as well as "cyber" incidents.

7.2.10. The detection, recording, management and response to an incident depends primarily on effective prevention and detection mechanisms and a robust response plan. Effective detection and response mechanisms also provide an important record of events and assist in preventing repeat events, improving defences and streamlining response measures.

7.2.11. A key part of the detection and response is incident reporting, including internal security system reports as well as any essential external reporting. It is essential that response is timely and methodical in order to minimise the effects of the incident. In all cases it is vital that steps are taken to quickly contain the incident, minimise damage and implement measures to prevent or contain any reoccurrence.

7.2.12. Not every cybersecurity event is serious enough to warrant detailed investigation and reporting, for example a single login failure from an employee on premises. A persistent login failure is, however, more serious and may indicate a malicious access attempt. Thresholds should be established which will trigger an incident response. **In all cases incidents** should be recorded to support analysis and reporting.

Definition of a Cyber Security Incident

7.2.13. A cyber security incident is any event that jeopardises or may jeopardise the confidentiality, integrity, or availability of an information system or the information a system processes, stores, or communicates. This includes a violation or potential violation of security policies, security procedures, acceptable use policies or any relevant regulation or legislation.

7.2.14. It is also important to categorise incidents in order to better manage allocation of resources to the containment and remediation of the incident. A three-tier categorisation is suggested:

1. **Critical**: Incident affecting critical systems or information with potential to impact operations, revenue or customers.

2. **Serious**: Incident affecting noncritical systems or information, impact on operations, revenue or customers. Employee investigations that are time sensitive should typically be classified at this level.

3. **Low**: Possible incident affecting noncritical systems. Incidents or employee investigations that are not time sensitive. Long term investigations requiring extensive research and/or detailed forensic work.

7.2.15. Factors that assist in determining the severity of an incident include:

- Whether the incident affects a single agency or multiple agencies;
- Functional impact of the incident (availability);
- Information impact of the incident (confidentiality, integrity);
- Recoverability from the incident;
- Whether a breach of personally identifiable information (PII) held by the agency has occurred;
- Reputational risk to the agency;
- Impact on any MOUs, MOAs and similar formal agreements.

References

7.2.16. Additional information relating to information security incidents can be found at:

Title	Publisher	Source
The Incident Object Description Exchange Format, RFC 5070, December 2007	The Internet Engineering Taskforce (IETF)	http://www.ietf.org/rfc/rfc5070.txt

Expert Review for Incident Object Description Exchange Format (IODEF) Extensions in IANA XML Registry, ISSN: 2070-1721, RFC 6685, July 2012	IETF	http://tools.ietf.org/html/rfc6685
Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERTs, October 2013	ENISA	http://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs
Computer Security Incident Handling Guide, Special Publication 800-61: Revision 2, August 2012	NIST	http://dx.doi.org/10.6028/NIST.SP.800-61r2
NIST Special Publication 800-60 Volume I Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories	NIST	http://www.csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
NIST Special Publication 800-60 Volume II Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II: Appendices	NIST	http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf
The National Cyber Security Centre Voluntary Cyber Security Standards for Industrial Control Systems v1.0	GCSB NCSC	http://www.gcsb.govt.nz/assets/GCSB-Documents/NCSC-voluntary-cyber-security-standards-for-ICD-v.1.0.pdf http://www.ncsc.govt.nz/resources/
The New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CIRSTs)	NCSC	https://www.ncsc.govt.nz/resources/
Information Sharing Specifications for Cybersecurity	DHS	https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

Rationale & Controls

7.2.17. Reporting information security incidents

7.2.17.R.01. Rationale

Reporting information security incidents provides management with a means to assess and minimise damage to a system and to take remedial actions. Incidents should be reported to an ITSM, as soon as possible. The ITSM may seek advice from NCSC as required.

7.2.17.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1203]

Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.

7.2.17.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1205]

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 system, software or other malfunctions;
- put mechanisms in place to enable the types, volumes and costs of information security incidents and malfunctions to be quantified and monitored; and
- deal with the violation of agency information security policies and procedures by personnel through training and, where warranted, a formal disciplinary process.

7.2.18. Responsibilities when reporting an information security incident

7.2.18.R.01. Rationale

The ITSM actively manages information security incidents and MUST ensure the CISO has sufficient awareness of and information on any information security incidents within an agency.

The CISO is required to keep the CSO and/or Agency Head informed of information security incidents within their agency.

7.2.18.R.02. Rationale

Reporting on **Critical** and **Serious** incidents requires immediate action.

Reporting on incidents categorised as **Low** can usually be adequately managed through periodic (weekly or monthly) reports.

7.2.18.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1211]

The ITSM MUST keep the CISO fully informed of information security incidents within an agency.

7.2.19. Reporting significant information security incidents to National Cyber Security Centre (NCSC)

7.2.19.R.01. Rationale

The NCSC uses significant information security incident reports as the basis for identifying and responding to information security events across

government. Reports are also used to develop new policy, procedures, techniques and training measures to prevent the recurrence of similar information security incidents across government.

7.2.19.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:1216]

The Agency ITSM, MUST report information security incidents categorised as:

- **Critical**;
- **Serious**; or
- incidents related to multi-agency or government systems;

to the NCSC (see also below) as soon as possible.

7.2.20. Reporting non-critical information security incidents to National Cyber Security Centre (NCSC)

7.2.20.R.01. Rationale

The NCSC uses information compiled from security incident reports as the basis for identifying and responding to information security events across government. Reports are also used to develop new policy, procedures, techniques and training measures to prevent the recurrence of similar information security incidents across government. This includes incidents categorised as **Low.**

7.2.20.C.01. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:1220]

Agencies SHOULD report information security incidents categorised as **Low** to the NCSC.

7.2.21. How to report information security incidents to National Cyber Security Centre (NCSC)

7.2.21.R.01. Rationale

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

7.2.21.R.02. Rationale

To simplify the reporting of information security incidents to the NCSC, a Cyber Security Incident – Report Form is provided on the NCSC website under Reporting an Incident at https://www.ncsc.govt.nz/

7.2.21.C.01. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:1223]

Agencies SHOULD formally report information security incidents using the NCSC on-line reporting form.

7.2.22. Outsourcing and information security incidents

7.2.22.R.01. Rationale

In the case of outsourcing of information technology services and functions, the agency remains responsible for the reporting of all information security incidents. This includes any outsourced cloud services used by the agency. As such, the agency MUST ensure that the service provider informs them of all information security incidents to enable them to assess the incident and provide formal reporting.

7.2.22.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:1226]

Agencies that outsource their information technology services and functions MUST ensure that the service provider advises and consults with the agency when an information security incident occurs.

7.2.23. Cryptographic keying material

7.2.23.R.01. Rationale

Reporting any information security incident involving the loss or misuse of cryptographic keying material is particularly important. Systems users in this situation are those that rely on the use of cryptographic keying material for the confidentiality and integrity of their secure communications.

7.2.23.R.02. Rationale

It is important to note that a loss or compromise of keying material is a **Critical** or **Serious** information security incident and strict procedures must be followed to minimise the impact of the incident.

7.2.23.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:1233]

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

7.2.24. Replacement of Cryptographic Key (HACE) keying material

7.2.24.R.01. Rationale

If an encryption key is compromised, there is no need to attack the algorithm itself and it is a trivial matter to decrypt any encrypted data. This is why strong key management is vital in order to protect the encryption keying materials. If a compromise of keying materials is known or even suspected, the cryptographic key must be replaced as a matter of urgency and measures taken to reduce the impact of the key compromise. See also Section 17.9 – Key Management.

7.2.24.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:6592]

Agencies MUST replace compromised cryptographic keys as a matter of urgency and record the replacement in the incident reporting.

7.2.25. High Assurance Cryptographic Equipment (HACE) keying material

7.2.25.R.01. Rationale

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

7.2.25.C.01.   Control

     Agencies MUST urgently notify GCSB of **any** suspected loss or compromise of keying material associated with HACE.

7.3. Managing Information Security Incidents

Objective

7.3.1.   To identify and implement processes for incident identification, management and analysis of information security incidents, including selection of appropriate remedies which will assist in preventing or reducing the impact of future information security incidents.

Context

Scope

7.3.2.   This section covers information relating primarily to managing information security incidents. The management of physical and personnel security incidents is considered to be out of scope unless it directly impacts on the protection of systems (e.g. the breaching of physical protection for a server room).

7.3.3.   It is important to note that, in most cases, information systems are likely to be affected.

References

7.3.4.   Additional information relating to the management of ICT evidence is contained in:

Reference	Title	Source
ISO/IEC_27037	Information Technology – Security Techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.	http://www.iso27001security.com/html/27037.html http://www.standards.co.nz/
HB 171:2003	Guidelines for the Management of Information Technology Evidence	https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF
	The New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CIRSTs)	http://www.ncsc.govt.nz/resources/

Rationale & Controls

7.3.5.   Information security incident management documentation

7.3.5.R.01.   Rationale

     Ensuring responsibilities and procedures for information security incidents are documented in relevant Information Security Documentation will ensure that when an information security incident does occur, agency personnel can respond in an appropriate manner. In addition, ensuring that system users are aware of reporting procedures will assist in identifying any information security incidents that an ITSM, or system owner fail to notice.

7.3.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1260]

     Agencies MUST detail information security incident responsibilities and procedures for each system in the relevant Information Security Documents.

7.3.6.   Recording information security incidents

7.3.6.R.01.   Rationale

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

7.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1264]

     Agencies SHOULD ensure that **all** information security incidents are recorded in a register.

7.3.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1266]

     Agencies SHOULD use their incidents register as a reference for future security risk assessments.

7.3.7.   Handling data spills

7.3.7.R.01.   Rationale

     A data spill is defined as the unauthorised or unintentional release, transmission or transfer of data. If there is a possibility that classified information may be compromised as a result of an information security incident, agencies MUST be able to respond in a timely fashion to limit damage and contain the incident.

7.3.7.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1271]

     Agencies MUST implement procedures and processes to detect data spills.

7.3.7.C.02.   Control

     When a data spill occurs agencies MUST assume that data at the highest classification held on or processed by the system, has been compromised.

7.3.7.C.03.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1274]

Agency SOPs MUST include procedure for:

- all personnel with access to systems;
- notification to the ITSM of any data spillage; and
- notification to the ITSM of access to any data which they are not authorised to access.

7.3.7.C.04. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1275]

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

7.3.7.C.05. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1276]

Agencies MUST treat any data spill as an information security incident and follow the IRP to deal with it.

7.3.7.C.06. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1277]

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

7.3.8.   Containing data spills

7.3.8.R.01. Rationale

The spillage of classified information onto a system not accredited to handle the information is considered a serious information security incident. It may be a critical information security incident if PII or particularly sensitive information is spilled. Refer to Section 7.2 – Reporting Information Security Incidents.

7.3.8.R.02. Rationale

Isolation may include disconnection from other systems and any external connections. In some cases system isolation may not be possible for architectural or operational reasons.

7.3.8.R.03. Rationale

Segregation may be achieved by isolation, enforcing separation of key elements of a virtual system, removing network connectivity to the relevant device or applying access controls to prevent or limit access.

7.3.8.R.04. Rationale

It is important to note that powering off a system can destroy information that may be useful in forensics analysis or other investigative work. In large, inter-connected systems, powering off a system may not be feasible.

7.3.8.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1283]

When classified information is introduced onto a system not accredited to handle the information, the following actions MUST be followed:

1. Immediately seek the advice of an ITSM;
2. Segregate or isolate the affected system and/or data spill;
3. Personnel MUST NOT delete the higher classified information unless specifically authorised by an ITSM.

7.3.8.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:1284]

When classified information is introduced onto a system not accredited to handle the information, personnel MUST NOT copy, view, print or email the information.

7.3.8.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1285]

When a data spill involving classified information or contaminating classified systems occurs and systems cannot be segregated or isolated agencies SHOULD **immediately** contact the NCSC for further advice.

7.3.9.   Handling malicious code infection

7.3.9.R.01. Rationale

The guidance for handling malicious code infections is provided to assist in preventing the spread of the infection and to prevent reinfection. Important details include:

- the infection date/time of the machine;
- any observed effects and source details;
- the possibility that system records and logs could be compromised; and
- the period of infection.

7.3.9.R.02. Rationale

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

7.3.9.R.03. Rationale

Agencies SHOULD be aware that some malicious code infections may be categorised as Advanced Persistent Threats (APTs) which may have been present for some time before detection. Specialist assistance may be required to deal with APTs.

7.3.9.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1290]

Agencies SHOULD follow the steps described below when malicious code is detected:

- isolate the infected system;
- decide whether to request assistance from NCSC;

- if such assistance is requested and agreed to, delay any further action until advised by NCSC;
- scan all previously connected systems and any media used within a set period leading up to the information 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, including any websites with password controlled access;
- advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems;
- use up-to-date anti-malware software to remove the malware from the systems or media;
- monitor network traffic for malicious activity;
- report the information security incident and perform any other activities specified in the IRP; and
- in the worst case scenario, rebuild and reinitialise the system.

7.3.10. Allowing continued attacks

7.3.10.R.01.   Rationale

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 advisor(s) whether the actions are breaching the Telecommunications (Interception Capability and Security) Act 2013.

7.3.10.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1294]

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.

7.3.11. Integrity of evidence

7.3.11.R.01.   Rationale

While gathering evidence it is important to maintain the integrity of the information and the chain of evidence. Even though in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected. This may also include a record of activities taken by the agency to contain the incident.

7.3.11.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1297]

Agencies SHOULD:

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

7.3.12. Seeking assistance

7.3.12.R.01.   Rationale

If the integrity of evidence relating to an information security incident is contaminated or compromised, it reduces NCSC's ability to assist agencies. As such, NCSC requests that no actions which could affect the integrity of the evidence are carried out prior to NCSC's involvement.

7.3.12.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1300]

Agencies SHOULD ensure that any requests for NCSC assistance are made as soon as possible after the information security incident is detected and that no actions which could affect the integrity of the evidence are carried out prior to NCSC's involvement.

8. Physical Security

8.1. Facilities

Objective

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

Context

Scope

8.1.2.   This section covers information on the physical security of facilities. Information on physical security controls for servers and network devices, network infrastructure and IT equipment can be found in the following sections of this chapter.

Physical security requirements for storing classified information

8.1.3.   Many of the physical controls in this manual are derived from the management protocol for physical security within the Protective Security Requirements (PSR). In particular from the minimum standard for security containers, secure rooms or lockable commercial cabinets needed for storing classified information.

Secure and unsecure areas

8.1.4.   In the context of this manual a secure area may be a single room or a facility that has security measures in place for the processing of classified information, or may encompass an entire building.

Physical security certification authorities

8.1.5.   The certification of an agency's physical security measures is an essential part of the certification and accreditation process. The authority and responsibility are listed in the table below:

Classification	Authority	Responsibility
SECRET	CSO	Physical
TOP SECRET	NZSIS	Physical
TOP SECRET SCIF	GCSB	Network Infrastructure Technical Security Surveillance Counter Measures

8.1.6.   Top Secret (TS) physical certification should be completed before any Technical inspections and certifications occur.

Facilities located outside of New Zealand

8.1.7.   Agencies operating sites located outside of New Zealand can contact GCSB to determine any additional requirements which may exist such as technical surveillance and oversight counter-measures and testing.

References

8.1.8.   High-level information relating to physical security is also contained in:

Title	Publisher	Source
ISO/IEC 27002:2013, Section 11 - Physical and Environmental Security	ISO /IEC Standards NZ	http://www.iso27001security.com/html/27002.html http://www.standards.co.nz/

PSR references

8.1.9.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV6, GOV7, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1, PHYSEC2, PHYSEC3 and PHYSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Creating a security culture Understand the physical security lifecycle	https://www.protectivesecurity.govt.nz/physical-security/creating-a-security-culture/ https://www.protectivesecurity.govt.nz/physical-security/understand-the-physical-security-lifecycle/
Managing specific scenarios	Secure your ICT facilities Physical Security for ICT systems Mobile and remote working	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/

Rationale & Controls

8.1.10.   Facility physical security

8.1.10.R.01.   Rationale

The application of defence-in-depth to the protection of systems and infrastructure is enhanced through the use of successive layers of physical security.

Typically the layers of security are:

- site;
- building;
- room;
- racks;
- approved containers;
- operational hours; and
- manning levels.

8.1.10.R.02.   Rationale

All layers are designed to control and limit access to those with the appropriate authorisation for the site, infrastructure and system. Deployable

platforms need to meet physical security certification requirements as with any other system. Physical security certification authorities dealing with deployable platforms may 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.

8.1.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1323]

Agencies MUST ensure that any facility containing a system or its associated infrastructure, including deployable systems, are certified and accredited in accordance with the PSR.

8.1.11. Preventing observation by unauthorised people

8.1.11.R.01. Rationale

Agency facilities without sufficient perimeter security are often exposed to the potential for observation through windows or open doors. This is sometimes described as the risk of oversight. Ensuring classified information on desks and computer screens is not visible will assist in reducing this security risk.

8.1.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1326]

Agencies SHOULD prevent unauthorised people from observing systems, in particular desks, screens and keyboards.

8.1.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1327]

Agencies SHOULD position desks, screens and keyboards away from windows and doorways so that they cannot be overseen by unauthorised persons. If required, blinds or drapes SHOULD be fixed to the inside of windows, and doors kept closed to avoid oversight.

8.1.12. Bringing non-agency owned devices into secure areas

8.1.12.R.01. Rationale

No non-agency owned devices are to be brought into TOP SECRET areas without their prior approval of the Accreditation Authority.

8.1.12.C.01. Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:1330]

Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.

8.1.13. Technical Inspection and surveillance counter-measure testing

8.1.13.R.01. Rationale

Technical surveillance counter-measure testing is conducted as part of the physical security certification to ensure that facilities do not have any unauthorised listening devices or other surveillance devices installed and that physical security measures are compatible with technical controls. This testing and inspection will normally occur AFTER the physical site accreditation has been completed (in accordance with the PSR). Further testing may also be necessary after uncleared access to the secure facility, such as contractors or visitors.

8.1.13.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1333]

Agencies MUST ensure that technical surveillance counter-measure tests are conducted as a part of the physical security certification.

8.1.13.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1334]

Agencies MUST determine if further technical surveillance counter-measure testing is required, particularly if visitors or contractors have entered secure areas.

8.2. Servers And Network Devices

Objective

8.2.1. Secured server and communications rooms provide appropriate physical security for servers and network devices.

Context

Scope

8.2.2. This section covers the physical security of servers and network devices. Information relating to network infrastructure and IT equipment can be found in other sections of this chapter.

Secured server and communications rooms

8.2.3. In order to reduce physical security requirements for information systems infrastructure, other network devices and servers, agencies may choose to certify and accredit the physical security of the site or IT equipment room to the standard specified in the PSR. This has the effect of providing an additional layer of physical security. See PSR - Physical Security, Protective Security Requirements - Physical security planning; Protective Security Requirements – Physical Security for ICT Systems; Protective Security Requirements – Secure your ICT facilities; Storage requirements for electronic information in ICT facilities (PDF)

8.2.4. Agencies choosing NOT to certify and accredit the physical security of the site or IT equipment room, must continue to meet the full storage requirements specified in the PSR. See PSR - Physical Security, Protective Security Requirements - Physical security planning; Protective Security Requirements – Physical Security for ICT Systems; Protective Security Requirements – Secure your ICT facilities; Storage requirements for electronic information in ICT facilities (PDF)

Rationale & Controls

8.2.5. Securing servers and network devices

8.2.5.R.01. Rationale

Security containers for IT infrastructure, network devices or servers situated in an unsecure area must be compliant with the requirements of the PSR. Installing IT infrastructure, network devices or servers in a secure facility can lower the storage requirements, provided multiple layers of physical security have been implemented, certified and accredited.

8.2.5.R.02.   Rationale

The establishment of a secure communications room to house IT infrastructure, network devices, and other related equipment will provide a further physical security layer.

8.2.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1349]

Agencies MUST ensure that servers and network devices are secured within cabinets as outlined in PSR Management protocol for physical security, with supporting document – Storage requirements for electronic information in ICT facilities.

8.2.6.   Securing server rooms, communications rooms and security containers

8.2.6.R.01.   Rationale

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 in the first place. Such activities will compromise the security efforts of the agencies and should not be permitted by the agency.

8.2.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1353]

Agencies MUST ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

8.2.6.C.02.   Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:1354]

Agencies MUST NOT leave server rooms, communications rooms or security containers in an unsecured state unless the server room is occupied by authorised personnel.

8.2.7.   Administrative measures

8.2.7.R.01.   Rationale

Site security plans (SitePlan), the physical security equivalent of the SecPlan 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.

8.2.7.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1357]

Agencies MUST develop a Site Security Plan (SitePlan) for each server and communications room. Information to be covered includes, but is not limited to:

- a summary of the security risk review for the facility the server or communications room is located in;
- 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 removal of system users and issuing of personal identification number codes and passwords;
- personnel security clearances, security awareness training and regular briefings;
- regular inspection of the generated audit trails and logs;
- end of day checks and lockup;
- reporting of information security incidents; and
- what activities to undertake in response to security alarms.

8.2.8.   No-lone-zones

8.2.8.R.01.   Rationale

Areas containing particularly sensitive materials or IT 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.

8.2.8.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1360]

Agencies operating no-lone-zones MUST suitably signpost the area and have all entry and exit points appropriately secured.

8.3. Network Infrastructure

Objective

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

Context

Scope

8.3.2.   This section covers information relating to the physical security of network infrastructure. Information relating to servers, network devices and IT equipment can be found in other sections of this chapter. Additionally, information on using encryption for infrastructure in unsecure areas can be found in Section 17.1 - Cryptographic Fundamentals.

Rationale & Controls

8.3.3.   Network infrastructure in secure areas

8.3.3.R.01.   Rationale

Network infrastructure is considered to process information being communicated across it and as such needs to meet the minimum physical security requirements for processing classified information as specified in the PSR Management protocol for physical security, with supporting document – Storage requirements for electronic information in ICT facilities.

8.3.3.R.02.   Rationale

The physical security requirements for network infrastructure can be lowered if encryption is being applied to classified information communicated over the infrastructure (i.e. data in transit encryption). Note this does NOT change the classification of the data itself, only the physical protection requirements.

8.3.3.R.03. Rationale

It is important to note that physical controls do not provide any protection against malicious software or other malicious entities that may be residing on or have access to the system.

8.3.3.R.04. Rationale

If classified information being communicated over the infrastructure is not encrypted the malicious entry can capture, corrupt or modify the traffic to assist in furthering any attempts to exploit the network and the information being communicated across it.

8.3.3.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1373]

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

8.3.3.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1374]

Agencies communicating classified information over infrastructure in secure areas SHOULD encrypt their information with at least an Approved Cryptographic Protocol. See Section 17.3 – Approved Cryptographic Protocols

8.3.4. Protecting network infrastructure

8.3.4.R.01. Rationale

In order to prevent tampering with patch panels, fibre distribution panels and structured wiring, any such enclosures need to be placed within at least lockable commercial cabinets. Furthermore, keys for such cabinets should not be remain in locks as this defeats the purpose of using lockable commercial cabinets in the first place.

8.3.4.C.01. Control System Classification(s): Top Secret; Compliance: MUST [CID:1377]

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

8.3.4.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1378]

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

8.3.5. Network infrastructure in unsecure areas

8.3.5.R.01. Rationale

As agencies lose control over classified information when it is communicated over unsecure public network infrastructure or over infrastructure in unsecure areas they MUST ensure that it is encrypted to a sufficient level that if it was captured that it would be sufficiently difficult to determine the original information from the encrypted information.

8.3.5.R.02. Rationale

Encryption does not change the class level of the information itself but allows reduced handling requirements to be applied.

8.3.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1382]

Agencies communicating classified information over public network infrastructure or over infrastructure in unsecure areas MUST use encryption to lower the handling instructions to be equivalent to those for unclassified networks.

8.4. IT Equipment

Objective

8.4.1. IT equipment is secured outside of normal working hours, is non-operational or when work areas are unoccupied.

Context

Scope

8.4.2. This section covers information relating to the physical security of IT equipment containing media. This includes but is not limited to workstations, printers, photocopiers, scanners and multi-function devices (MFDs).

8.4.3. Additional information relating to IT equipment and media can be found in the following chapters and sections of this manual:

- Section 11.2 - Fax Machines, Multifunction Devices and Network Printers;
- Chapter 12 - Product Security; and
- Chapter 13 – Decommissioning and Disposal.

Handling IT equipment containing media

8.4.4. During non-operational hours agencies need to store media containing classified information that resides within IT equipment in accordance with the requirements of the PSR. Agencies can comply with this requirement by undertaking one of the following processes:

- ensuring IT equipment always reside in an appropriate class of secure room;
- storing IT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet;
- using IT 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 IT 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; or

- configuring IT 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.

8.4.5. The intent of using cryptography or preventing the storage of classified information on non-volatile media is to enable agencies to treat the media within IT equipment in accordance with the storage requirements of a lower classification, as specified in the PSR, during non-operational hours. Temporary data should be deleted at log off or shut down and volatile media secured.

8.4.6. As the process of using cryptography and preventing the storage of classified information on non-volatile media does not constitute the sanitisation and reclassification of the media, the media retains its classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal requirements as specified in this manual.

IT equipment using hybrid hard drives or solid state drives

8.4.7. The process of preventing the storage of classified information on non-volatile media, and enforcing deletion of temporary data at logoff or shutdown, is NOT approved as a method of lowering the storage requirements, when hybrid hard drives or solid state drives are used.

Rationale & Controls

8.4.8.   Accounting for IT equipment

8.4.8.R.01.   Rationale

Ensuring that IT equipment containing media is accounted for by using asset registers, equipment registers, operational & configuration records and regular audits will assist in preventing loss or theft, or in the cases of loss or theft, alerting appropriate authorities to its loss or theft.

8.4.8.R.02.   Rationale

Asset registers may not provide a complete record as financial limits may result in smaller value items not being recorded. In such cases other registers and operational information can be utilised to assist in building a more complete record.

8.4.8.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1400]

Agencies MUST account for all IT equipment containing media.

8.4.9.   Processing requirements

8.4.9.R.01.   Rationale

As the media within IT equipment takes on the classification of the information it is processing, the area that it is used within needs to be certified to a level that is appropriate for the classification of that information.

8.4.9.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1407]

Agencies MUST certify the physical security of facilities containing IT equipment to the highest classification of information being processed, stored or communicated by the equipment within the facilities.

8.4.10.   Storage requirements

8.4.10.R.01.   Rationale

The PSR states that either Class C, B or A secure rooms or Class C, B or A security containers or lockable commercial cabinets can be used to meet physical security requirements for the storage of IT equipment containing media. The class of secure room or security container will depend on the physical security certification of the surrounding area and the classification of the information.

8.4.10.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1403]

Agencies MUST ensure that when secure areas are non-operational or when work areas are unoccupied IT equipment with media is secured in accordance with the minimum physical security requirements for storing classified information as specified in the PSR Management protocol for physical security – Physical Security of your ICT assets and facilities, with supporting document – Storage requirements for electronic information in ICT facilities.

8.4.11.   Securing non-volatile media for storage

8.4.11.R.01.   Rationale

The use of techniques to prevent the storage of classified information on non-volatile media and processes to delete temporary data at logoff or shutdown may sound secure but there is no guarantee that they will always work effectively or will not be bypassed in unexpected circumstances such as a loss of power. As such, agencies need to consider these risks when implementing such a solution.

8.4.11.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1409]

Agencies choosing to prevent the storage of classified information on non-volatile media and enforcing scrubbing of temporary data at logoff or shutdown SHOULD:

- assess the security risks associated with such a decision; and
- specify the processes and conditions for their application within the system's SecPlan.

8.4.12.   Securing volatile media for storage

8.4.12.R.01.   Rationale

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

- an attacker gaining access to the IT equipment immediately after power is removed and accessing the contents of volatile media to recover encryption keys or parts thereof. This is sometimes described as a data remanence attack;
- extreme environmental conditions causing data to remain in volatile media for extended periods after the removal of power; and
- the physical security of the locations in which the IT equipment will reside.

8.4.12.C.01.   Control

Agencies securing volatile media for IT equipment during non-operational hours SHOULD:

- disconnect power from the equipment the media resides within;
- assess the security risks if not sanitising the media; and
- specify any additional processes and controls that will be applied within the system's SecPlan.

8.4.13.   Encrypting media within IT equipment

8.4.13.R.01.   Rationale

Current industry good practice is to encrypt all media within IT equipment. Newer operating systems provide this functionality and older operating systems can be supported with the use of open source or proprietary applications.

8.4.13.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1415]

Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.

8.5. Tamper Evident Seals

Objective

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

Context

Scope

8.5.2.   This section covers information on tamper evident seals that can be applied to assets.

Rationale & Controls

8.5.3.   Recording seal usage

8.5.3.R.01.   Rationale

Recording information about seals in a register and on which asset they are used assists in reducing the security risk that seals could be substituted without security personnel being aware of the change.

8.5.3.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1425]

Agencies MUST record the usage of seals in a register that is appropriately secured.

8.5.3.C.02.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1426]

Agencies MUST record in a register, information on:

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

8.5.3.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1427]

Agencies SHOULD record the usage of seals in a register that is appropriately secured.

8.5.3.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1428]

Agencies SHOULD record in a register information on:

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

8.5.4.   Purchasing seals

8.5.4.R.01.   Rationale

Using uniquely numbered seals ensures that a seal can be uniquely mapped to an asset. This assists security personnel in reducing the security risk that seals could be replaced without anyone being aware of the change.

8.5.4.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1431]

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.

8.5.4.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1432]

Seals and any seal application tools SHOULD be secured when not in use.

8.5.4.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1433]

Agencies SHOULD NOT allow contractors to independently purchase seals and associated tools on behalf of the government.

8.5.5.   Reviewing seal usage

8.5.5.R.01.   Rationale

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 at least annual reviews will allow for detection of any tampering to an asset and ensure that the correct seal is located

on the correct asset.

8.5.5.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1436]

Agencies SHOULD review seals for differences with a register at least annually. At the same time seals SHOULD be examined for any evidence of tampering.

9. Personnel Security

9.1. Information Security Awareness and Training

Objective

9.1.1. A security culture is fostered through induction training and ongoing security education tailored to roles, responsibilities, changing threat environment and sensitivity of information, systems and operations.

Context

Scope

9.1.2. This section covers information relating specifically to information security awareness and training.

PSR references

9.1.3. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV4, INFOSEC2, PERSEC1 and PERSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/
PSR content protocols	Management protocol for information security Management protocol for personnel security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/
PSR requirements sections	Creating a security culture Build security awareness	https://www.protectivesecurity.govt.nz/personnel-security/creating-a-security-culture/ https://www.protectivesecurity.govt.nz/governance/build-security-awareness/

Rationale & Controls

9.1.4. Information security awareness and training responsibility

9.1.4.R.01. Rationale

Agency management is <u>responsible</u> for ensuring that an appropriate information security awareness and a training program is provided for all personnel. Without management support, security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

9.1.4.R.02. Rationale

Awareness and knowledge degrades over time without ongoing refresher training and updates. Providing ongoing information security awareness and training will assist in keeping personnel aware of issues and their responsibilities.

9.1.4.R.03. Rationale

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

9.1.4.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1449]

Agency management MUST ensure that all personnel who have access to a system have sufficient training and ongoing information security awareness.

9.1.5. Information security awareness and training

9.1.5.R.01. Rationale

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

- become familiar with their roles and responsibilities;
- understand any legislative or regulatory mandates and requirements;
- understand any national or agency policy mandates and requirements;
- understand and support security requirements;
- assist in maintaining security; and
- learn how to fulfil their security responsibilities.

9.1.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1452]

Agencies MUST provide ongoing information security awareness and a training programme for personnel on topics such as responsibilities,

legislation and regulation, consequences of non-compliance with information security policies and procedures, and potential security risks and counter-measures.

9.1.5.C.02.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1453]

Agencies MUST provide information security awareness training as part of their employee induction programmes.

9.1.6.   Degree and content of information security awareness and training

9.1.6.R.01.   Rationale

The detail, content and coverage of information security awareness and training will depend on the objectives of the organisation. Personnel with responsibilities beyond that of a general user should have tailored training to meet their needs.

9.1.6.R.02.   Rationale

As part of the guidance provided to system users, there should be sufficient emphasis placed on the activities that are NOT allowed on systems. The minimum list of content will also ensure that personnel are sufficiently exposed to issues that could cause an information security incident through lack of awareness or through lack of knowledge.

9.1.6.C.01.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1457]

Agencies SHOULD align the detail, content and coverage of information security awareness and training programmes to system user responsibilities.

9.1.6.C.02.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1458]

Agencies SHOULD ensure that information security awareness and training includes information on:

- the purpose of the training or awareness program;
- any legislative or regulatory mandates and requirements;
- any national or agency policy mandates and requirements;
- agency security appointments and contacts;
- the legitimate use of system accounts, software and classified 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 information 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; and
- supporting documentation such as SOPs and user guides.

9.1.6.C.03.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1459]

Agencies SHOULD ensure that information security awareness and training includes advice to system users not to attempt to:

- tamper with the system;
- bypass, strain or test information security mechanisms;
- introduce or use unauthorised IT equipment or software on a system;
- replace items such as keyboards, pointing devices and other peripherals with personal equipment;
- assume the roles and privileges of others;
- attempt to gain access to classified information for which they have no authorisation; or
- relocate equipment without proper authorisation.

9.1.7.   System familiarisation training

9.1.7.R.01.   Rationale

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, will provide them with specific knowledge relating to these types of systems.

9.1.7.C.01.   ControlSystem Classification(s): Top Secret; Compliance: MUST [CID:1462]

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.

9.1.8.   Disclosure of information while on courses

9.1.8.R.01.   Rationale

Government personnel attending courses with non-government personnel may not be aware of the consequences of disclosing information relating to the security of their agency's systems. Raising awareness of such consequences in personnel will assist in preventing disclosures that could lead to a targeted attack being launched against an agency's systems.

9.1.8.C.01.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1465]

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

9.2. Authorisations, Security Clearances And Briefings

Objective

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

Context

Scope

9.2.2.   This section covers information relating to 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 Section 16.2 - System Access.

Security clearances – New Zealand and foreign

9.2.3.   Where this manual refers to security clearances, the reference applies to a national security clearance granted by a New Zealand government agency. Foreign nationals may be granted a national security clearance if risks can be mitigated. Refer to PSR Personnel Security for more information.

PSR References

9.2.4.   Additional policy and information on granting and maintaining security clearances can be found in:

Reference	Title	Source
PSR Mandatory Requirements	GOV4, INFOSEC1, PERSEC1, PERSEC2, PERSEC3, PERSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for personnel security Management Protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://protectivesecurity.govt.nz/personnel-security/clearances/recruiting-and-managing-clearance-holders/ https://protectivesecurity.govt.nz/personnel-security/clearances/recruiting-and-managing-clearance-holders/
PSR requirements sections	Creating a security culture Build security awareness Security zones Recruiting and managing national security clearance holders	https://www.protectivesecurity.govt.nz/personnel-security/creating-a-security-culture/ https://www.protectivesecurity.govt.nz/governance/build-security-awareness/ https://www.protectivesecurity.govt.nz/security-zones/ https://protectivesecurity.govt.nz/personnel-security/clearances/recruiting-and-managing-clearance-holders/

Rationale & Controls

9.2.5.   Documenting authorisations, security clearance and briefing requirements

9.2.5.R.01.   Rationale

Ensuring that the requirements for access to a system are documented and agreed upon will assist in determining if system users have appropriate authorisations, security clearances and need-to-know to access the system.

9.2.5.R.02.   Rationale

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

9.2.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1480]

Agencies MUST specify in the System Security Plan (SecPlan) any authorisations, security clearances and briefings necessary for system access.

9.2.6.   Authorisation and system access

9.2.6.R.01.   Rationale

Personnel seeking access to a system will 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 be given only the privileges that they need to undertake their duties. Providing all system users with privileged access when there is no such requirement can cause significant security vulnerabilities in a system.

9.2.6.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1483]

Agencies MUST:

- limit system access on a need-to-know/need-to-access basis;
- provide system users with the least amount of privileges needed to undertake their duties; and
- have any requests for access to a system authorised by the supervisor or manager of the system user.

9.2.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1484]

Agencies SHOULD:

- limit system access on a need-to-know/need-to-access basis;
- provide system users with the least amount of privileges needed to undertake their duties; and
- have any requests for access to a system authorised by the supervisor or manager of the system user.

9.2.7. Recording authorisation for personnel to access systems

9.2.7.R.01.   Rationale

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.

9.2.7.C.01.   Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:1487]

Agencies SHOULD:

- maintain a secure record of:
    - all authorised system users;
    - their user identification;
    - why access is required;
    - role and privilege level,
    - who provided the authorisation to access the system;
    - when the authorisation was granted; and
- maintain the record, for the life of the system or the length of employment whichever is the longer, to which access is granted.

9.2.8. Security clearance for system access

9.2.8.R.01.   Rationale

Information classified as CONFIDENTIAL and above requires personnel to have been granted a formal security clearance before access is granted. Refer to the PSR Personnel Security Mandatory Requirements.

9.2.8.C.01.   Control **System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT** [CID:1490]

System users MUST NOT be granted access to systems or information classified CONFIDENTIAL or above unless vetting procedures have been completed and formal security clearance granted.

9.2.8.C.02.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:1491]

All system users MUST:

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

9.2.9. System access briefings

9.2.9.R.01.   Rationale

Some systems process endorsed or compartmented information. As such, unique briefings may exist that system users need to receive before being granted access to the system. All system users will require a briefing on their responsibilities on access to and use of the system to which they have been granted access to avoid inadvertent errors and security breaches. Specialised system training may also be required.

9.2.9.C.01.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:1494]

All system users MUST have received any necessary briefings before being granted access to compartmented or endorsed information or systems.

9.2.10. Access by foreign nationals to NZEO systems

9.2.10.R.01.   Rationale

NZEO information is restricted to New Zealand nationals.

9.2.10.C.01.   Control **System Classification(s): All Classifications; Compliance: MUST NOT** [CID:1497]

Where systems process, store or communicate unprotected NZEO information, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.

9.2.10.C.02.   Control **System Classification(s): All Classifications; Compliance: MUST NOT** [CID:1498]

Where agencies protect NZEO information on a system by implementing controls to ensure that NZEO information is not passed to, or made accessible to, foreign nationals, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.

9.2.11. Access by foreign nationals to New Zealand systems

9.2.11.R.01.   Rationale

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

9.2.11.C.01.   Control **System Classification(s): All Classifications; Compliance: MUST NOT** [CID:1501]

Where systems process, store or communicate classified 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.

9.2.12. Granting limited higher access

9.2.12.R.01. Rationale

Under exceptional circumstances, temporary access to systems classified RESTRICTED and below may be granted.

9.2.12.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:1504]

Agencies MUST NOT permit limited higher access for systems and information classified CONFIDENTIAL or above.

9.2.12.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1505]

Agencies granting limited higher access to information or systems MUST ensure that:

- the requirement to grant limited higher access is temporary in nature and is an exception rather than the norm;
- an ITSM has recommended 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 an occasional NOT non-ongoing basis;
- the system user is not granted privileged access to the system;
- the system user's access is formally documented; and
- the system user's access is approved by the CISO.

9.2.13. Controlling limited higher access

9.2.13.R.01. Rationale

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 have access only to that information they require to undertake their duties.

9.2.13.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1508]

Agencies granting limited higher access to a system MUST ensure that:

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

9.2.14. Granting emergency access

9.2.14.R.01. Rationale

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 be formally documented.

9.2.14.R.02. Rationale

It is important that appropriate debriefs take place at the conclusion of any emergency in order to manage the ongoing security of information and systems and to identify "lessons learned".

9.2.14.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:1512]

Emergency access MUST NOT be granted unless personnel have a security clearance to at least CONFIDENTIAL level.

9.2.14.C.02. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:1513]

Emergency access MUST NOT be used on reassignment of duties while awaiting completion of full security clearance procedures.

9.2.14.C.03. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1514]

Agencies granting emergency access to a system MUST ensure that:

- the requirements to grant emergency access is due to an immediate and critical need to access classified information and there is insufficient time to complete clearance procedures;
- 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;
- appropriate briefs and debriefs for the information and system are conducted;
- access is limited to information and systems necessary to deal with the particular emergency and is governed by strict application of the "need to know" principle;
- emergency access is limited to ONE security clearance level higher than the clearance currently held; and
- the security clearance process is completed as soon as possible.

9.2.14.C.04. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1515]

Personnel granted emergency access MUST be debriefed at the conclusion of the emergency.

9.2.15. Accessing endorsed or compartmented information

9.2.15.R.01. Rationale

Limited higher access to systems processing, storing or communicating endorsed or compartmented information is not permitted.

9.2.15.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:1518]

Agencies MUST NOT grant limited higher access to systems that process, store or communicate endorsed or compartmented information.

9.3. Using The Internet

Objective

9.3.1.   Personnel use Internet services in a responsible and security conscious manner, consistent with agency policies.

Context

Scope

9.3.2.   This section covers information relating to personnel using Internet services such as the Web, Web-based email, news feeds, subscriptions and other services. Whilst this section does not address Internet services such as IM, IRC, IPT and video conferencing, agencies need to remain aware that unless applications using these communications methods are evaluated and approved by GCSB they are NOT approved for communicating classified information over the Internet.

9.3.3.   Additional information on using applications that can be used with the Internet can be found in Section 14.3 - Web Applications and Section 15.1 - Email Applications.

Rationale & Controls

9.3.4.   Using the Internet

9.3.4.R.01.   Rationale

Agencies will need to determine what constitutes suspicious activity, questioning or contact in relation to their own work environment. Suspicious activity, questioning or contact may relate to the work duties of personnel or the specifics of projects being undertaken by personnel within the agency.

9.3.4.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1529]

Agencies MUST ensure personnel are instructed to report any suspicious activity, questioning or contact when using the Internet, to an ITSM.

9.3.5.   Awareness of Web usage policies

9.3.5.R.01.   Rationale

Users MUST be familiar with and formally acknowledge agency Web usage policies for system users in order to follow the policy and guidance.

9.3.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1532]

Agencies MUST make their system users aware of the agency's Web usage policies.

9.3.5.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1533]

Personnel MUST formally acknowledge and accept agency Web usage policies.

9.3.6.   Monitoring Web usage

9.3.6.R.01.   Rationale

Agencies may choose to monitor compliance with aspects of Web usage policies, such as access attempts to blocked websites, pornographic and gambling websites, as well as compiling a list of system users that excessively download and/or upload data without an obvious or known legitimate business requirement.

9.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1536]

Agencies SHOULD implement measures to monitor their personnel, visitor and contractor compliance with their Web usage policies.

9.3.7.   Posting information on the Web

9.3.7.R.01.   Rationale

Personnel need to take special care not to accidentally post information on the Web, especially in forums and blogs. Even Official Information or UNCLASSIFIED information that appears to be benign in isolation could, in aggregate, have a considerable security impact on the agency, government sector or wider government.

9.3.7.R.02.   Rationale

To ensure that personal opinions of agency personnel are not interpreted as official policy or associated with an agency, personnel will need to maintain separate professional and personal accounts when using websites, especially when using online social networks.

9.3.7.R.03.   Rationale

Accessing personal accounts from an agency's systems is discouraged.

9.3.7.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1541]

Agencies MUST ensure personnel are instructed to take special care when posting information on the Web.

9.3.7.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1542]

Agencies MUST ensure personnel posting information on the Web maintain separate professional accounts from any personal accounts they have for websites.

9.3.7.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1543]

Agencies SHOULD monitor websites where personnel post information and if necessary remove or request the removal of any inappropriate information.

9.3.7.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1544]

Accessing personal accounts from agency systems SHOULD be discouraged.

9.3.8.   Posting personal information on the Web

9.3.8.R.01.   Rationale

Personnel need to be aware that any personal interest or other information they post on websites can be used to develop a detailed profile of their families, lifestyle, interest 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 information from them or implant malicious software on systems by inducing them to, for instance, open emails or visit websites with malicious content.

9.3.8.R.02.   Rationale

Profiling is a common marketing and targeting technique facilitated by the internet.

9.3.8.R.03.   Rationale

Individuals who work for high-interest agencies, who hold security clearances or who are involved in high-profile projects are of particular interest to profilers, cyber criminals and other users of this information.

9.3.8.R.04.   Rationale

The following is of particular interest to profilers:

- photographs;
- past and present employment details;
- personal details, including DOB, family members, birthdays, address and contact details;
- schools and institutions;
- clubs, hobbies and interests;
- educational qualifications;
- current work duties;
- details of work colleagues and associates; and
- work contact details.

9.3.8.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1550]

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.

9.3.8.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1551]

Personnel SHOULD be encouraged to use privacy settings for websites to restrict access to personal information they post to only those they authorise to view it.

9.3.8.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1552]

Personnel SHOULD be encouraged to undertake a Web search of themselves to determine 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.

9.3.9.   Peer-to-peer applications

9.3.9.R.01.   Rationale

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 sharing or public consumption. Examples of peer-to-peer file sharing applications include Shareaza, KaZaA, Ares, Limewire, eMule and uTorrent.

9.3.9.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1555]

Agencies SHOULD NOT allow personnel to use peer-to-peer applications over the Internet.

9.3.10.   Receiving files via the Internet

9.3.10.R.01.   Rationale

When personnel receive files via peer-to-peer file sharing, IM or IRC applications they are often bypassing security mechanisms put in place by the agency 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.

9.3.10.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1558]

Agencies SHOULD NOT allow personnel to receive files via peer-to-peer, IM or IRC applications.

9.4. Escorting Uncleared Personnel

Objective

9.4.1.   Uncleared personnel are escorted within secure areas.

Context

Scope

9.4.2.   This section covers information relating to the escorting of uncleared personnel without security clearances in secure areas.

PSR references

9.4.3.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV4, INFOSEC1, PERSEC1, PERSEC2, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for personnel security Management Protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Creating a security culture Build security awareness Security zones Visitor control	https://www.protectivesecurity.govt.nz/personnel-security/creating-a-security-culture/ https://www.protectivesecurity.govt.nz/governance/build-security-awareness/ https://www.protectivesecurity.govt.nz/security-zones/ https://www.protectivesecurity.govt.nz/physical-security/understand-the-physical-security-lifecycle/design/specific-security-measures/visitor-control/

Rationale & Controls

9.4.4.   Unescorted access

9.4.4.R.01.   Rationale

Ensuring that personnel have correct security clearances to access sensitive areas and that access by escorted personnel is recorded for auditing purposes is widely considered a standard security practice.

9.4.4.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1569]

Agencies MUST ensure that all personnel with unescorted access to TOP SECRET areas have appropriate security clearances and briefings.

9.4.5.   Maintaining an unescorted access list

9.4.5.R.01.   Rationale

Maintaining an unescorted access list reduces the administrative overhead of determining if personnel can enter a TOP SECRET area without an escort. Personnel with approval for unescorted access must be able to verify their identity at all times while within the secure area.

9.4.5.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1572]

Agencies MUST maintain an up to date list of personnel entitled to enter a TOP SECRET area without an escort.

9.4.5.C.02.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1573]

Personnel MUST display identity cards at all times while within the secure area.

9.4.6.   Displaying the unescorted access list

9.4.6.R.01.   Rationale

Displaying an unescorted access list allows staff to quickly verify if personnel are entitled to be in a TOP SECRET area without an escort. Care should be taken not to reveal the contents of the access list to non-cleared personnel.

9.4.6.C.01.   Control System Classification(s): Top Secret; Compliance: SHOULD [CID:1576]

Agencies SHOULD display within a TOP SECRET area, an up to date list of personnel entitled to enter the area without an escort.

9.4.6.C.02.   Control System Classification(s): Top Secret; Compliance: SHOULD NOT [CID:1577]

The unescorted access list SHOULD NOT be visible from outside of the secure area.

9.4.7.   Visitors

9.4.7.R.01.   Rationale

Visitors to secure areas should be carefully supervised to ensure the need-to-know principle is strictly adhered to.

9.4.7.C.01.   Control System Classification(s): Top Secret; Compliance: SHOULD [CID:1580]

Visitors SHOULD be carefully supervised to ensure they do not gain access to or have oversight of information above the level of their clearance or outside of their need-to-know.

9.4.8.   Recording visits in a visitor log

9.4.8.R.01.   Rationale

Recording visitors to a TOP SECRET area ensures that the agency has a record of visitors should an investigation into an incident need to take place in the future.

9.4.8.C.01.   Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:1583]

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.

9.4.9. Content of the visitor log

9.4.9.R.01.   Rationale

The contents of the visitor log ensure that security personnel have sufficient details to conduct an investigation into an incident if required.

9.4.9.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1586]

Agencies MUST, at minimum, record the following information in a visitor log for each entry:

- name;
- organisation;
- person visiting;
- contact details for person visiting; and
- date and time in and out.

9.4.10. Separate visitor logs

9.4.10.R.01.   Rationale

Maintaining a separate visitor log for TOP SECRET areas assists in enforcing the need-to-know principle. General visitors do not need-to-know of personnel that have visited TOP SECRET areas.

9.4.10.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1589]

Agencies with a TOP SECRET area within a larger facility MUST maintain a separate log from any general visitor log.

10. Infrastructure

10.1. Cable Management Fundamentals

Objective

10.1.1. Cable management systems are designed to support the integration of systems across government facilities, assist maintenance and engineering changes, as well as minimise the opportunity for tampering or unauthorised changes to cable systems.

Context

Scope

10.1.2. This section covers information relating to cable distribution systems used in facilities within New Zealand. When designing cable management systems, Section 10.5 - Cable Labelling and Registration and Section 10.6 - Cable Patching of this chapter also apply.

Applicability of controls within this section

10.1.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Common implementation scenarios

10.1.4. This section provides common requirements for non-shared facilities. Specific requirements for facilities shared between agencies and facilities shared with non-government entities can be found in subsequent sections of this chapter.

Red/Black Concept and Cable Separation

10.1.5. The **RED/BLACK** concept is the separation of electrical and electronic circuits, devices, equipment cables, connectors, components and systems that transmit store or process national security information from non-national security information. The **RED/BLACK** concept is sometimes described as **RED/BLACK** architecture or **RED/BLACK** engineering.

10.1.6. The **RED/BLACK** concept should not be confused with the generic description HIGH/LOW or HIGH SIDE/LOW SIDE. In this context, HIGH refers to systems **classified** CONFIDENTIAL and above and LOW refers to systems **classified** RESTRICTED and below. While these concepts are similar and often used interchangeably, it is important to recognise that information does not usually change classification. The signal or transmission, however, may transit both **RED** and **BLACK** systems in order to reach its intended destination. It is important to note that systems carrying a particular classification may also carry information at **ALL** lower classifications **BUT NOT** any higher classifications.

10.1.7. An example is the use of radio transmissions or Wi-Fi where the information may hold a HIGH classification and originate in **RED** equipment but once transmission occurs the **signal** is **BLACK** as radio and Wi-Fi signals can be detected by anyone within range.

10.1.8. This also leads to the situation where some equipment may have both **RED** and **BLACK** elements. Examples include Wi-Fi Access Points and encryption devices. **RED** Information in a **BLACK** environment is invariably protected by encryption and a variety of technical countermeasures.
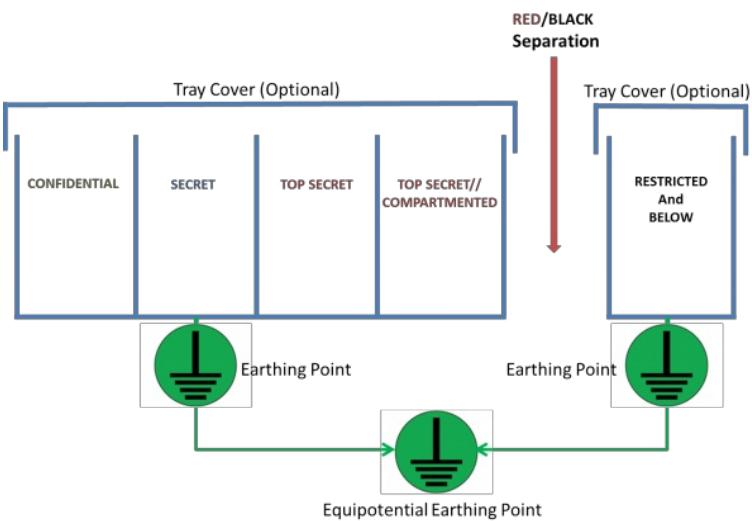
10.1.9. All cables with metal conductors (the signal carrier, the grounding element, the strengthening member or an armoured outer covering) can act as fortuitous signal conductors allowing signals to escape or to cross-contaminate other cables and signals. This provides a path for the exploitation of signals, data and information.

10.1.10. A fundamental control is the separation of cables and related equipment with sufficient distance between them to prevent cross-contamination.

Cable trays

10.1.11. Where copper or a combination of copper and fibre cables are used, cable trays will provide separation, assist cable management and enhance cable protection. While preferable to separate **RED** cables of different systems for cable management purposes, the most important element is to maintain **RED/BLACK** separation.

10.1.12. It is preferable that cable trays contain dividers. Some cable trays provide only a single receptacle for cables (no dividers). If dividers are not available, multi-core fibre cables should be used. Cables of similar classifications should be bundled. A typical cable tray layout with dividers is depicted below:

Catenary

10.1.13. The use of catenary (wire, rope, nylon cord or similar cable support mechanisms) is becoming more widespread in place of cable trays. Care MUST be taken to maintain **RED/BLACK** separation if this method of cable support is used.

Earthing

10.1.14. It is important that any metal trays or metal catenary are earthed for both safety and to avoid creating any fortuitous conductors. All earthing points MUST be equipotentially bonded.

Fibre optic cabling

10.1.15. Fibre optic cabling does not produce, and is not influenced by, electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects.

10.1.16. Many more fibres can be run per cable diameter than wired cables thereby reducing cable infrastructure costs. Fibre Optic cable is usually constructed with a glass core, cladding on the core and a further, colour coded coating. Multiple cores can be bundled into a single cable and multiple cables can be bundled into a high capacity cable. This is illustrated in Figures 1 below. Cables also have a central strength member of mylar or some similar high strength, non-conductive material
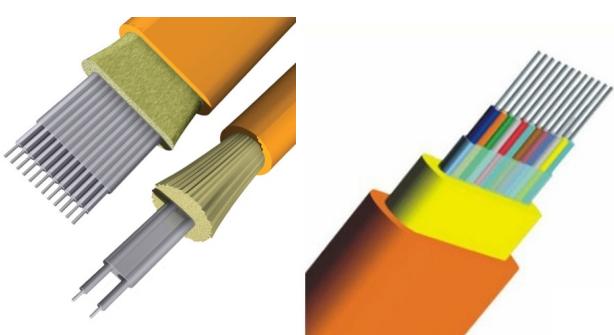
10.1.17. Fibre cable is considered the best method to future proof against unforeseen threats.

10.1.18. Cable trays for **fibre only cable** may be of any suitable material. If metal trays are used they MUST be earthed.

Ribbon Fibre Optic Cable

10.1.19. In the context of this discussion, traditional and ribbon fibre optic cables are subject to identical controls, restrictions in installation and use and any operational caveats.

10.1.20. Unlike traditional beam optical cable, ribbon fibre optic cable is arranged into a strip. Because the ribbon contains only coated optical fibres, this type of cable takes up much less space and is generally lighter (weight) than individually buffered optical fibres. As a result, ribbon cables are denser than any other fibre cable design. They are ideal for applications where space is limited, such as in an existing conduit that has very little room left for an additional cable. Ribbon fibre optic cable is a convenient solution for space and weight challenges.


Figure 2: Typical Ribbon Cable

10.1.21. Ribbon cables enable the migration to high fibre count systems required to support high bandwidth applications including 10, 40 and 100Gb/s. Ribbon cables are rarely used in long distance fibre optic trunk cable but are typically used in data centres, campus, commercial buildings and large industrial sites. Fibre counts can range from 2 to over 1700.
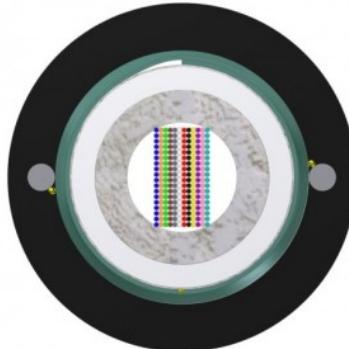
10.1.22. The cable ribbons are coated optical fibres placed side by side, encapsulated in Mylar tape, similar to a miniature version of wire ribbons used in computer wiring. A single ribbon many contain 4, 8, 12 or 24 optical fibres with ribbons stacked up to 22 high. At present 12-fiber ribbons are readily accessible and identifiable with ribbon identification numbers, TIA-598 compliant fibre colour coding and are available with non-flame-retardant or formulated flame-retardant outer jacket. They are also available in several configurations including all-dielectric, armoured and aerial self-supporting cables.

10.1.23. Because the cable profile is different to older round cable type, new cable strippers, cleavers, and fusion splicers are required for installation and
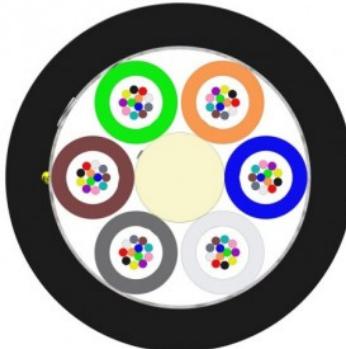
maintenance.

10.1.24. Fibre optic ribbon cable comes in two basic configurations: loose tube ribbon cable and jacket ribbon. Loose tube cables are where fibre ribbons are stacked on top of one another inside a loose-buffered tube. This arrangement can hold several hundred fibres in close quarters. The buffer, strength members, and cable jacket carry any strain while the fibre ribbons move freely inside the buffer tube.

10.1.25. Jacket ribbon cable is similar to a regular tight-buffered cable, but it is elongated to contain a fibre ribbon. This type of cable typically features a small amount of strength member and a ripcord to tear through the jacket.
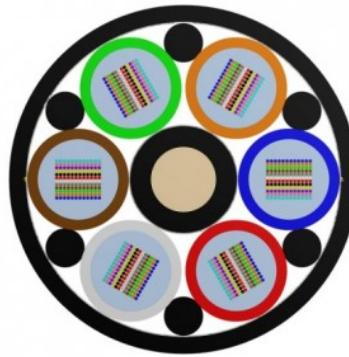

Figure 3: Jacket Cable   **Figure 4: Loose Tube Cable**
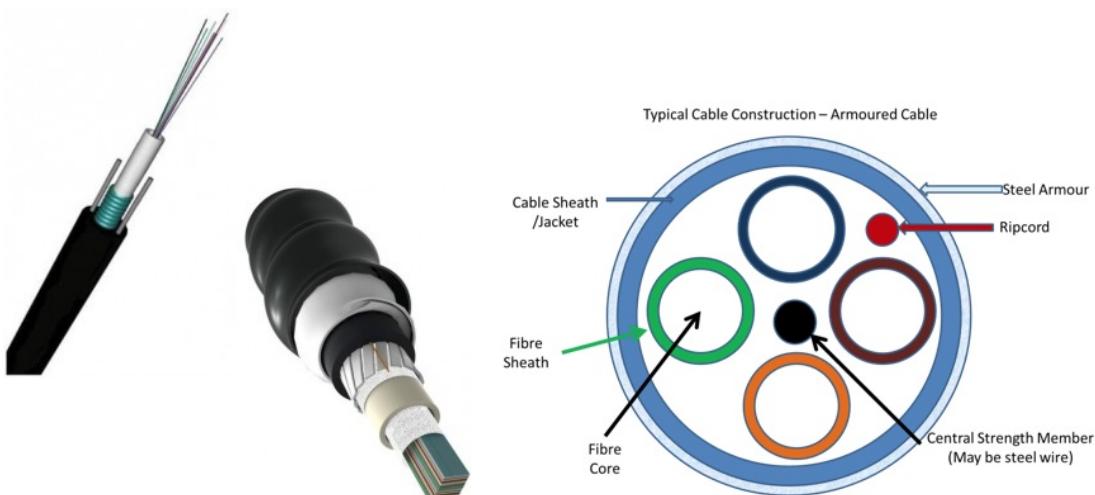
10.1.26. Infrastructure cables contain multiple fibre ribbon units inside a central tube with dielectric strength members for tensile strength and colour coded fibres with individual ribbon unit ID numbers for clear identification. Ribbon fibre optic cables are available in configurations supporting high-speed, applications such as Gigabit Ethernet, 10 Gigabit Ethernet, Gigabit ATM and Fibre Channel.


Figure 5: Infrastructure (High Cable Count) Ribbon Cable

Armoured Fibre optic cabling

10.1.27. Some fibre optic cable also includes conductive metal cable strengtheners and conductive metal armoured sheaths which may be wire-wound or stainless steel mesh for external cable protection and steel wire cores as core strength members. This strengthening and armouring is conductive and specialist advice may be needed to avoid earth loops, cross-coupling, inductive coupling or the introduction of other compromising signals and currents. Fibre optic cable with metal cable strengtheners or conductive armoured sheaths is considered *unsuitable* for secure installations.


Figure 6 - Armoured Ribbon Fibre Cable
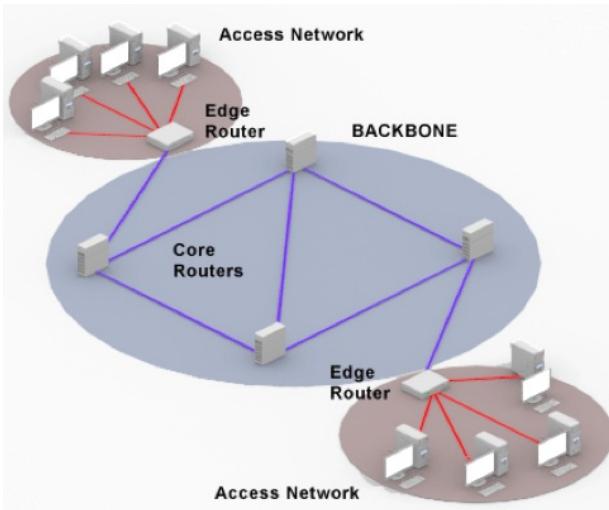
Backbone

10.1.28. A backbone or core is the central cabling that connects the infrastructure (servers, databases, gateways, equipment and telecommunication rooms etc.) to local areas networks, workstations and other devices, such as MFD's. Smaller networks may also be connected to the backbone.

10.1.29. A backbone can span a geographic area of any size including an office, a single building, multi-story buildings, campus, national and international infrastructure. In the context of the NZISM the term backbone generally refers to the central cabling within a building or a campus.

10.1.30. Backbones can be defined in terms of six criteria:

- transmission media;
- topology;
- security required;
- access control;
- transmission technique;
- transmission speed and capability.

TOP SECRET cabling

10.1.31. For TOP SECRET cabling the cable's non-conductive protective sheath IS NOT considered to be a conduit. For TOP SECRET fibre optic cables with sub-units, the cable's outer protective sheath IS considered to be a conduit.

Power Filters

10.1.32. A power filter is a device placed between an external power source and electronic devices. It is used in order to attenuate external transients, conducted radio frequencies (RF) or electromagnetic interference (EMI) between the AC or DC power line and the equipment. Filters can also reduce radiated interference to assist in managing emissions or susceptibility to interference.

10.1.33. The power lines entering an electronic device can act both as an antenna and as a low impedance conduction path for signals that exist inside the device. These signals may couple into the power line, either through inductance or capacitance, from internal circuitry, other internal wiring or from other components such as transformers, coils or adjacently routed wires. To a lesser degree, but still problematic, the power lines can also pickup induced current signals from magnetic fields inside the enclosure.

10.1.34. The purpose of power supply filters is to smooth the power supply and provide a degree of isolation from the external power supply for connected electronic devices. RF/EMI filters are designed to reduce line - to - ground (common mode) interference, EMI and anomalous RF. Best practice is to solve or suppress EMI and RF emissions at source, rather than after emission.

10.1.35. There are international and national regulations on frequencies and signal levels that a device is permitted to produce in order to minimise or prevent interference with other equipment. Practically no modern equipment, with fast digital circuits and switch-mode power supply regulators can meet electromagnetic compatibility (EMC) requirements without efficient filtering, particularly when operating in close proximity. While most devices are designed by manufacturers to meet regulation, not all devices filter EMI or RF to levels acceptable for secure environments. It may be necessary to use a power line filter to keep signals inside the enclosure as much as possible and keep any generated signals to less than the legal or required limits for conducted emissions.

10.1.36. Power filters have a variety of capabilities depending on their specification. It is important the filters are selected correctly for the power supply, expected load and required attenuation capacity. It is important to note that an Uninterruptible Power Supply (UPS) is NOT considered an RF/EMI filter.

10.1.37. Common usage of filters is for computer systems, laboratory and testing equipment, medical devices, consumer electronics, and to protect any equipment where good quality power supply and protection of the electronic devices and data is required. Devices can be within buildings, vehicle, ships, aircraft or portable.

10.1.38. Power filters often include EMC/ RFI filters which channel emissions to earth to prevent them from being conducted back down the supply cables. This can be detected as an earth leakage current which may cause Residual Current Devices (RCDs) to trip. This problem can be corrected by using the correct specification of power filter or installing low leakage current devices. Agencies should consult the GCSB if such problems occur.

References

10.1.39.

Title	Publisher	Source

NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB	GCSB CONFIDENTIAL document available on application to authorised personnel
AS/NZS 3000:2007/Amdt 2:2012 - Electrical Installations (Known as the Australia/New Zealand Wiring Rules,	Standards NZ	Standards New Zealand http://www.standards.co.nz/
ANSI/TIA-568-C.3 – Optical Fiber Cabling Components	American National Standards Institute (ANSI)	http://www.ansi.org/
IEEE 802 – Local and Metropolitan Area Networks: Overview and Architecture	Institute of Electrical and Electronics Engineers (IEEE)	http://ieeexplore.ieee.org/document/6847097/

References - Fibre Standards

10.1.40. Fibre Standards.

Title	Description	Source
AS/NZS 2967:2014	**Optical fibre communication cabling systems safety.** Provides rules for safe practices in the handling, installation, testing, use and disposal of optical fibre cabling and associated materials and equipment.	https://shop.standards.govt.nz/catalog
IEC/ISO 11801	**Information technology - Generic cabling for customer premises.** Specifies general-purpose telecommunication cabling systems (structured cabling), including several classes of optical fibre interconnections.	https://webstore.iec.ch/home
IEC 60793 Series	**Optical fibres.** A list of all parts in the IEC 60793 series, published under the general title Optical fibres, can be found on the IEC website.	https://webstore.iec.ch/home
IEC 60794 Series	**Optical fibre cables.** A list of all parts in the IEC 60794 series, published under the general title Optical fibre cables, can be found on the IEC website.	https://webstore.iec.ch/home
ANSI/TIA-568-C.3	**Optical Fibre Cabling Components**	https://webstore.ansi.org
ANSI/TIA-598-D (Revision of TIA-598-C) July 2014	**Optical Fibre Cable Colour Coding** This standard defines the recommended identification scheme or system for individual fibres, fibre units, and groups of fibre units within a cable structure.	https://webstore.ansi.org
ITU-T G.657 – 659 series	**Optical Fibre Cables** Characteristics and recommendations for selection, use and installation.	https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

PSR references

10.1.41. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Security zones	https://www.protectivesecurity.govt.nz/security-zones/

Managing specific scenarios	Secure your ICT facilities Physical Security for ICT systems	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/

Rationale & Controls

10.1.42. Backbone

10.1.42.R.01. Rationale

The design of a backbone requires consideration of a number of criteria including the capacity of the cable to carry the predicted volume of data at acceptable speeds. An element of "future proofing" is also required as re-cabling to manage capacity issues can be costly. Fibre optic cable provides a convenient means of securing and "future proofing" backbones.

10.1.42.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2216]

Agencies MUST use fibre optic cable for backbone infrastructures and installations.

10.1.42.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2217]

Agencies SHOULD use fibre optic cable for backbone infrastructures and installations.

10.1.43. Use of Fibre Optic Cable

10.1.43.R.01. Rationale

Fibre optic cable is considered more secure than copper cables and provides electrical isolation of signals. Fibre will also provide higher bandwidth and speed to allow a degree of future-proofing in network design.

10.1.43.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2220]

Agencies SHOULD use fibre optic cabling.

10.1.43.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2221]

Agencies SHOULD consult with the GCSB where fibre optic cable incorporating conductive metal strengtheners or sheaths is specified.

10.1.43.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2222]

Agencies SHOULD consult with the GCSB where copper cables are specified.

10.1.43.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:2223]

Agencies SHOULD NOT use fibre optic cable incorporating conductive metal strengtheners or sheaths except where essential for cable integrity.

10.1.44. Cabling Standards

10.1.44.R.01. Rationale

Unauthorised personnel could inadvertently or deliberately access system cabling. This could result in loss or compromise of classified information. Non-detection of covert tampering or access to system cabling may result in long term unauthorised access to classified information by a hostile entity.

10.1.44.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2226]

Agencies MUST install all cabling in accordance with the relevant New Zealand standards as directed by AS/NZS 3000:2007 and NZCSS400.

10.1.45. Cable colours

10.1.45.R.01. Rationale

To facilitate cable management, maintenance and security cables and conduit should be colour-coded to indicate the classification of the data carried and/or classification of the compartmented data.

10.1.45.R.02. Rationale

Cables and conduit may be the distinguishing colour for their entire length or display a distinguishing label marking and colour at each end and at a maximum of two metre intervals along the cable.

10.1.45.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2230]

Agencies MUST comply with the cable and conduit colours specified in the following table.

Classification	Cable colour
Compartmented Information (SCI)	Orange/Yellow/Teal or other colour
TOP SECRET	Red
SECRET	Blue
CONFIDENTIAL	Green
RESTRICTED and all lower classifications	Black

10.1.45.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:2231]

Additional colours may be used to delineate special networks and compartmented information of the same classification. These networks MUST

be labelled and covered in the agency's SOPs.

10.1.46. Cable colours for foreign systems in New Zealand facilities

10.1.46.R.01. Rationale

Foreign systems should be segregated and separated from other agency systems for security purposes. Colour-coding will facilitate installation, maintenance, certification and accreditation.

10.1.46.C.01. Control System Classification(s): Top Secret; Compliance: MUST [CID:2234]

The cable colour to be used for foreign systems MUST be agreed between the host agency, the foreign system owner and the Accreditation Authority.

10.1.46.C.02. Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:2235]

Agencies MUST NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.

10.1.46.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2236]

The cable colour to be used for foreign systems SHOULD be agreed between the host agency, the foreign system owner and the Accreditation Authority.

10.1.46.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:2237]

Agencies SHOULD NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.

10.1.47. Cable groupings

10.1.47.R.01. Rationale

Grouping cables provides a method of sharing conduits and cable reticulation systems in the most efficient manner. These conduits and reticulation system must be inspectable and cable separations must be obvious.

10.1.47.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2240]

Agencies MUST contact GCSB for advice when combining the cabling of special networks.

10.1.47.C.02. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:2241]

Agencies MUST NOT deviate from the approved fibre cable combinations for shared conduits and reticulation systems as indicated below.

Group	Approved combination
1	UNCLASSIFIED
	RESTRICTED
2	CONFIDENTIAL
	SECRET
3	TOP SECRET
	Other Special Networks
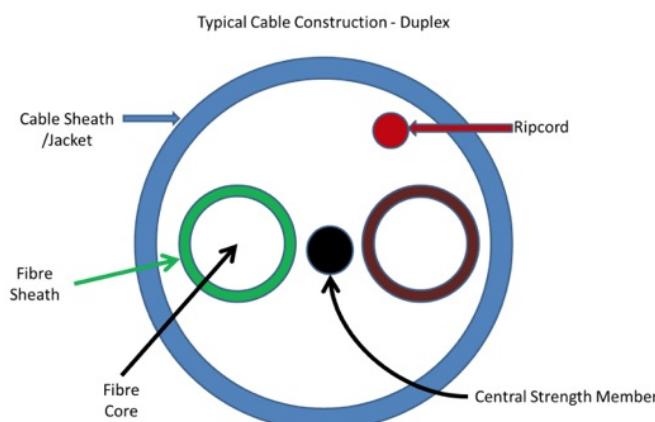
10.1.48. Fibre optic cables sharing a common conduit

10.1.48.R.01. Rationale
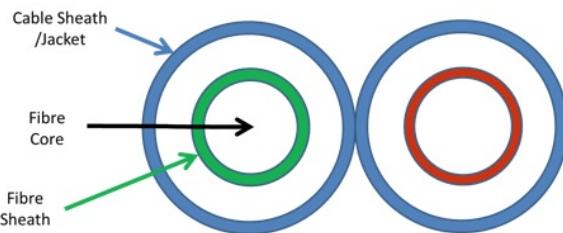
The use of multi-core fibre optic cables can reduce installation costs. The principles of separation and containment of cross-talk and leakage must be adhered to.

10.1.48.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2244]
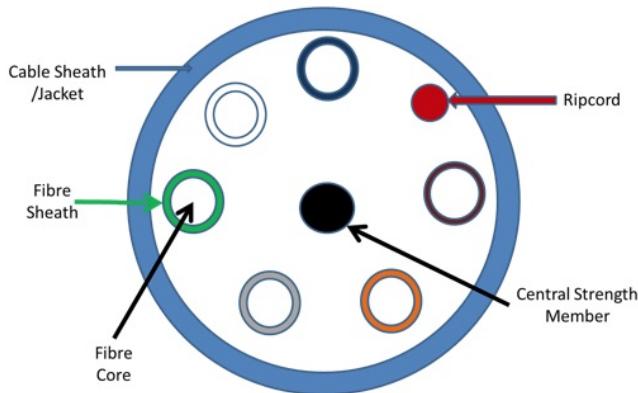
With fibre optic cables the arrangements of fibres within the cable sheath, as illustrated in Figure 3, MUST carry a single classification only.

Typical Cable Construction - Duplex

Typical Cable Construction - TwinFlex
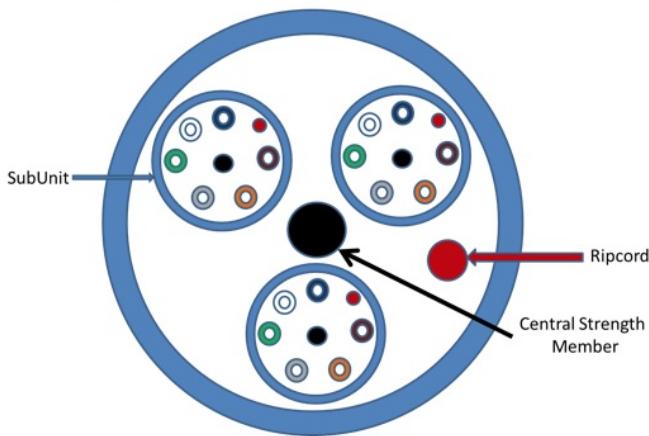
Typical Cable Construction – Multi-Core Cable

10.1.48.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:2245]

If a fibre optic cable contains subunits, as shown in Figure 4, each subunit MUST carry only a single classification.

Typical Cable Construction – Multi-Core with Subunits

10.1.48.C.03. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:2246]

Agencies MUST NOT mix classifications up to RESTRICTED with classifications of CONFIDENTIAL and above in a single cable.

10.1.49. Audio secure areas

10.1.49.R.01. Rationale

Audio secure areas are designed to prevent audio conversation from being heard outside the walls. Penetrating an audio secure area for cables in an unapproved manner can degrade this. Consultation with GCSB needs to be undertaken before any modifications are made to audio secure areas.

10.1.49.C.01. Control System Classification(s): Top Secret; Compliance: MUST [CID:2249]

When penetrating an audio secure area for cables, agencies MUST comply with all directions provided by GCSB.

10.1.50. Wall outlet terminations

10.1.50.R.01. Rationale

Wall outlet boxes are the preferred method of connecting cable infrastructure to workstations and other equipment. They allow the management of cabling and can utilise a variety of connector types for allocation to different classifications.

10.1.50.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2253]

Cable groups sharing a wall outlet MUST use different connectors for systems of different classifications.

10.1.50.C.02. Control

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.

10.1.50.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2255]

Cable outlets MUST be labelled with the system classification and connector type.

10.1.50.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2256]

Cable outlets SHOULD be labelled with the system classification and connector type.

10.1.51. Power Filters

10.1.51.R.01. Rationale

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks. See also 10.1.32.

10.1.51.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:5899]

Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.

10.2. Cable Management for Non-Shared Government Facilities

Objective

10.2.1. Cable management systems in non-shared government facilities are implemented in a secure and easily inspectable and maintainable way.

Context

Scope

10.2.2. This section provides specific requirements for cabling installed in **non-shared** Government facilities.

- A **non-shared** facility is a facility occupied **solely** by a single agency.
- A **shared** facility is a facility occupied by **more than one** agency. A shared facility should have stricter physical and technical security controls than a non-shared facility.

This section is to be applied in addition to common requirements for cabling as outlined in the Section 10.1 - Cable Management Fundamentals.

Applicability of controls within this section

10.2.3. The controls within this section are only applicable to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual will need to be consulted.

References

10.2.4. Further references can be found at:

Title	Publisher	Source
NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB	GCSB CONFIDENTIAL document available on application to authorised personnel
AS/NZS 3000:2007/Amdt 2:2012 - Electrical Installations (Known as the Australia/New Zealand Wiring Rules,	Standards NZ	http://www.standards.co.nz/

Rationale & Controls

10.2.5. Cabling Inspection

10.2.5.R.01. Rationale

Regular inspections of cable installations are necessary to detect any unauthorised or malicious tampering or cable degradation.

10.2.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2270]

In TOP SECRET areas or zones, all cabling MUST be inspectable at a minimum of five-metre intervals.

10.2.5.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2271]

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

10.2.6. Cables sharing a common reticulation system

10.2.6.R.01. Rationale

Laying cabling in a neat and controlled manner, observing separation requirements, allows for inspections and reduces the need for individual cable trays for each classification.

10.2.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2274]

Approved cable groups may share a common reticulation system but SHOULD have either a dividing partition or a visible gap between the differing cable groups or bundles.

10.2.7. Cabling in walls

10.2.7.R.01.   Rationale

Cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements.

10.2.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2277]

Flexible or plastic conduit SHOULD be used in walls to run cabling from cable trays to wall outlets.

10.2.8. Cabinet separation

10.2.8.R.01.   Rationale

Having a definite gap between cabinets allows for ease of inspections for any unauthorised or malicious cabling or cross patching.

10.2.8.C.01.   Control System Classification(s): Top Secret; Compliance: SHOULD [CID:2280]

TOP SECRET cabinets SHOULD have a visible inspectable gap between themselves and lower classified cabinets.

10.2.9. Power Filters

10.2.9.R.01.   Rationale

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks. See also 10.1.32.

10.2.9.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:5902]

Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.

10.3. Cable Management for Shared Government Facilities

Objective

10.3.1. Cable management systems in shared government facilities are implemented in a secure and easily inspectable and maintainable way.

Context

Scope

10.3.2. This section provides specific requirements for cabling installed in **shared** Government facilities.

- A **shared** facility is a facility occupied by **more than one** agency. A shared facility should have stricter physical and technical security controls than a non-shared facility.
- A **non-shared** facility is a facility occupied **solely** by a single agency.

This section is to be applied in addition to common requirements for cabling as outlined in Section 10.1 - Cable Management Fundamentals.

Applicability of controls within this section

10.3.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual will need to be consulted.

Rationale & Controls

10.3.4. Use of fibre optic cabling

10.3.4.R.01.   Rationale

Fibre optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared facility where you do not have total control over other areas of the facility.

10.3.4.R.02.   Rationale

It is more difficult to tap than copper cabling.

10.3.4.R.03.   Rationale

Many more fibres can be run per cable diameter than wired cables thereby reducing cable infrastructure costs.

10.3.4.R.04.   Rationale

Fibre cable is the best method to future proof against unforseen threats.

10.3.4.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2295]

Agencies SHOULD use fibre optic cabling.

10.3.5. Cabling inspection

10.3.5.R.01.   Rationale

In a shared facility it is important that cabling systems are inspected for illicit tampering and damage on a regular basis and have stricter controls than a non-shared facility.

10.3.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:2299]

In TOP SECRET areas, cables MUST be fully inspectable for their entire length.

10.3.5.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2298]

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

10.3.6. Cables sharing a common reticulation system

10.3.6.R.01. Rationale

In a shared facility with another government agency, tighter controls may be required for sharing reticulation systems. Note also the red/black separation requirements in paragraph 10.1.5.

10.3.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2302]

Approved cable groups SHOULD have either a dividing partition or a visible gap between the individual cable groups. If the partition or gap exists, cable groups may share a common reticulation system.

10.3.7. Enclosed cable reticulation systems

10.3.7.R.01. Rationale

In a shared facility with another government agency, TOP SECRET cabling is enclosed in a sealed reticulation system to restrict access and control cable management.

10.3.7.C.01. Control System Classification(s): Top Secret; Compliance: SHOULD [CID:2305]

The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings that contain TOP SECRET cabling, SHOULD be clear plastic.

10.3.8. Cabling in walls

10.3.8.R.01. Rationale

In a shared facility with another government agency, 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 facility.

10.3.8.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2308]

Cabling from cable trays to wall outlets SHOULD run in flexible or plastic conduit.

10.3.9. Wall penetrations

10.3.9.R.01. Rationale

Wall penetrations by cabling, requires the integrity of the classified area 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 area.

10.3.9.C.01. Control System Classification(s): Top Secret; Compliance: SHOULD [CID:2311]

For wall penetrations that exit into a lower classified area, cabling SHOULD be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

10.3.10. Power reticulation

10.3.10.R.01. Rationale

In a shared 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.

10.3.10.C.01. Control System Classification(s): Top Secret; Compliance: SHOULD [CID:2314]

TOP SECRET facilities SHOULD have a power distribution board, separately reticulated, located within the TOP SECRET area and supply UPS power to all equipment.

10.3.11. Power Filters

10.3.11.R.01. Rationale

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks. See also 10.1.32.

10.3.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2317]

Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.

10.3.12. Cabinet separation

10.3.12.R.01. Rationale

Having a visible gap between cabinets facilitates inspection for any unauthorised, malicious or cross patch cabling.

10.3.12.C.01. Control System Classification(s): Top Secret; Compliance: SHOULD [CID:2320]

TOP SECRET cabinets SHOULD have a visible gap to separate them from lower classified cabinets.

10.4. Cable Management for Shared Non-Government Facilities

Objective

10.4.1. Cable management systems are implemented in shared non-government facilities to minimise risks to data and information.

Context

Scope

10.4.2. This section provides specific requirements for 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 Section 10.1 - Cable Management Fundamentals section.

Applicability of controls within this section

10.4.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms

or facilities outside New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Rationale & Controls

10.4.4. Use of fibre optic cabling

10.4.4.R.01.   Rationale

Fibre optic cabling is essential in a shared non-government facility. Fibre optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared non-government facility where an agency's controls may have a limited effect outside the agency controlled area.

10.4.4.R.02.   Rationale

Fibre optic cable is more difficult to tap than copper cabling and anti-tampering monitoring can be employed to detect tampering.

10.4.4.R.03.   Rationale

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

10.4.4.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2335]

In TOP SECRET areas, agencies MUST use fibre optic cabling.

10.4.4.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2336]

Agencies SHOULD use fibre optic cabling.

10.4.5. Cabling inspection

10.4.5.R.01.   Rationale

In a shared non-government facility, it is imperative that cabling systems be inspectable for tampering and damage on a regular basis particularly where higher threat levels exist or where threats are unknown.

10.4.5.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2340]

In TOP SECRET areas, cables MUST be fully inspectable for their entire length.

10.4.5.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2341]

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

10.4.6. Cables sharing a common reticulation system

10.4.6.R.01.   Rationale

In a shared non-government facility, tighter controls are placed on sharing reticulation systems as the threats attributable to tampering and damage are increased.

10.4.6.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2344]

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.

10.4.6.C.02.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2345]

TOP SECRET cabling MUST run in a non-shared, enclosed reticulation system.

10.4.6.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2346]

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.

10.4.7. Enclosed cable reticulation systems

10.4.7.R.01.   Rationale

In a shared non-government facility, TOP SECRET cabling is enclosed in a sealed reticulation system to prevent access and control cable management.

10.4.7.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2349]

In TOP SECRET areas, the front covers for conduits and cable trays in floors, ceilings and of associated fittings MUST be clear plastic or be inspectable and have tamper proof seals fitted.

10.4.7.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2350]

The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings SHOULD be clear plastic or be inspectable and have tamper proof seals fitted.

10.4.8. Cabling in walls or party walls

10.4.8.R.01.   Rationale

In a shared non-government facility, cabling run correctly in walls allows for neater installations facilitating separation and inspectability. Controls are more stringent than in a non-shared facility or a shared government facility.

10.4.8.R.02.   Rationale

A party wall is a wall shared with an unclassified area where there is no control over access. In a shared non-government facility, cabling is not allowed in a party wall. An inner wall can be used to run cabling where the area is sufficient for inspection of the cabling.

10.4.8.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:2354]

Cabling MUST NOT run in a party wall.

10.4.9. Sealing reticulation systems

10.4.9.R.01.   Rationale

In a shared non-government facility, where the threats of access to cable reticulation systems is increased, GCSB endorsed anti-tamper seals are required to provide evidence of any tampering or illicit access.

10.4.9.R.02.   Rationale

In a shared non-government facility, all conduit joints and wall penetrations are sealed with a visible smear of glue or sealant to prevent access to cabling.

10.4.9.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2358]

Agencies MUST use GCSB endorsed tamper evident seals to seal all removable covers on reticulation systems, including:

- conduit inspection boxes;
- outlet and junction boxes; and
- T-pieces.

10.4.9.C.02.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2359]

Tamper evident seals MUST be uniquely identifiable and a register kept of their unique number and location.

10.4.9.C.03.   Control System Classification(s): Top Secret; Compliance: MUST [CID:2360]

Conduit joints MUST be sealed with glue or sealant.

10.4.9.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2361]

Conduit joints SHOULD be sealed with glue or sealant.

10.4.10. Wall penetrations

10.4.10.R.01.   Rationale

A cable wall penetration into a lesser-classified area requires the integrity of the classified area 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 area.

10.4.10.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2365]

Wall penetrations that exit into a lower classified area, cabling MUST be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

10.4.11. Power reticulation

10.4.11.R.01.   Rationale

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.

10.4.11.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2368]

Secure facilities MUST have a power distribution board located within the secure area and supply UPS power all equipment.

10.4.12. Power Filters

10.4.12.R.01.   Rationale

Power filters are used to provide filtered (clean) power and reduce opportunity for technical attacks. Refer to 10.1.32 or consult the GCSB for technical advice.

10.4.12.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2371]

Power filters MUST be used to provide filtered (clean) power and reduce opportunity for technical attacks.

10.4.13. Equipment Cabinet separation

10.4.13.R.01.   Rationale

A visible gap between equipment cabinets will make any cross-cabling obvious and will simplify inspections for unauthorised or compromising changes.

10.4.13.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2374]

Equipment cabinets MUST have a visible gap or non-conductive isolator between cabinets of different classifications.

10.4.13.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2375]

There SHOULD be a visible inspectable gap or non-conductive isolator between equipment cabinets of different classifications.

10.5. Cable Labelling and Registration

Objective

10.5.1.   To facilitate cable management, and identify unauthorised additions or tampering.

Context

Scope

10.5.2. This section covers information relating to the labelling of cabling infrastructure installed in secure areas.

Applicability of controls within this section

10.5.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Rationale & Controls

10.5.4. Conduit label specifications

10.5.4.R.01. Rationale

Conduit labelling of a specific size and colour will facilitate identifying secure conduits.

10.5.4.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2387]

Agencies MUST comply with the conduit label colours specified in the following table.

Classification	Cable colour
Compartmented Information (SCI)	Orange/Yellow/Teal or other colour
TOP SECRET	Red
SECRET	Blue
CONFIDENTIAL	Green
RESTRICTED and all lower classifications	Black

10.5.5. Installing conduit labelling

10.5.5.R.01. Rationale

Conduit labelling in public or reception areas should not draw undue attention to the level of classified processing or any other agency capability.

10.5.5.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:2390]

Conduit labels installed in public or visitor areas SHOULD NOT be labelled in such a way as to draw attention to or reveal classification of data processed or other agency capability.

10.5.6. Labelling wall outlet boxes

10.5.6.R.01. Rationale

Clear labelling of wall outlet boxes reduces the possibility of incorrectly attaching IT equipment of a lesser classification to the wrong outlet.

10.5.6.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2393]

Wall outlet boxes MUST denote the classification, cable and outlet numbers.

10.5.6.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2394]

Wall outlet boxes SHOULD denote the classification, cable and outlet numbers.

10.5.7. Standard operating procedures

10.5.7.R.01. Rationale

Recording labelling conventions in SOPs facilitates maintenance and fault finding.

10.5.7.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2397]

The SOPs SHOULD record the site conventions for labelling and registration.

10.5.8. Labelling cables

10.5.8.R.01. Rationale

Labelling cables with the correct socket number, equipment type, source or destination minimises the likelihood of improperly cross connecting equipment and can assist in fault finding and configuration management.

10.5.8.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2400]

Agencies MUST label cables at each end, with sufficient information to enable the physical identification and inspection of the cable.

10.5.8.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2401]

Agencies SHOULD label cables at each end, with sufficient information to enable the physical identification and inspection of the cable.

10.5.9. Cable register

10.5.9.R.01. Rationale

Cable registers provide a source of information that assessors can view to verify compliance.

10.5.9.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2404]

Agencies MUST maintain a register of cables.

10.5.9.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2405]

Agencies SHOULD maintain a register of cables.

10.5.10. Cable register contents

10.5.10.R.01.   Rationale

Cable registers allow installers and assessors to trace cabling for inspection, tampering or accidental damage. It tracks all cable management changes through the life of the system.

10.5.10.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2408]

The cable register MUST record at least the following information:

- cable identification number;
- classification;
- socket number, equipment type, source or destination site/floor plan diagram; and
- seal numbers if applicable.

10.5.10.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2409]

The cable register SHOULD record at least the following information:

- cable identification number;
- classification;
- socket number, equipment type, source or destination site/floor plan diagram; and
- seal numbers if applicable.

10.5.11. Cable inspections

10.5.11.R.01.   Rationale

Regular cable inspections, are a method of checking the cable management system against the cable register as well as detecting tampering, damage, breakages or other anomalies.

10.5.11.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2412]

Agencies SHOULD inspect cables for inconsistencies with the cable register in accordance with the frequency defined in the SecPlan.

10.6. Patch Panels, Patch Cables and Racks

Objective

10.6.1. Cable termination, patch panels, patch cables and racks are designed to prevent emanations, cross-connecting or cross-patching systems of differing classifications as well as following good engineering practice.

Context

Scope

10.6.2. This section covers information relating to the configuration and installation of patch panels, patch cables and fly leads associated with communications systems.

10.6.3. Reference should also be made to:

- Section 8.5 – Tamper-evident seals;
- Section 10.1 – Cable management fundamentals;
- Section 10.7 – Emanation Security Threat Assessments.

Applicability of controls within this section

10.6.4. The controls within this section are applicable to all communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside New Zealand the Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Exception for patch cable and fly lead connectors

10.6.5. For patch cables, the same connectors can be used for different classifications **if** 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.

Fibre optic patch panels

10.6.6. For Fibre optic patch panels are sometimes also described as fibre distribution panels. Their principal function is to safety terminate the fibre optic cable and provide connection access to the cable's individual fibres.

10.6.7. Fibre patch panels are termination units, providing a secure, organised chamber for housing connectors and splice units while organising, managing and protecting fibre optic cable, splices and connectors.

10.6.8. Fibre patch panels can be either rack mounted or wall mounted and are usually placed near terminating equipment and connected with patch cables. Free standing patch panel racks are also available. Patch panels may also be mounted within standard equipment racks.

10.6.9. Rack mount panels may have flat or angled faces to assist in organising the cables themselves. Angled panels are intended to direct patch cables into vertical cable managers on either side of the rack. This facilitates maintenance and reduces the requirement for horizontal cable management.

10.6.10. Fibre patch panels can accommodate fibre adapter panels (also called connector panels), associated trunk cables, connectors, patch cords, and usually integrate cable management.

10.6.11. There are several components in a fibre patch panel which may include:

- Chassis or frame;
- Drawer to facilitate access for installation and maintenance;
- Cassette;
- Coupler panels (adapter panels) – to hold the connector couplers;
- The connector couplers (connector adapters);
- Splice tray – organises and secures splice modules;
- Patch cable management trays.

10.6.12. While well over 80 different fibre optic cable connector types have been manufactured, there are between 15 and 20 types in common use.

Multimedia Patch Panels

10.6.13. A multimedia modular panel allows copper and fibre cables to be terminated in the same rack mount space. It accommodates several different adapters, suited for Cat6a/6/5e/5 Ethernet cables and fibre patch cables.

Rack Layout and Cable Management

10.6.14. Standardised rack layouts and cable management are important for engineering support, security, equipment cooling and to minimise accidental or unnecessary outages. Many data centres will dictate a hotside (hot air out) and coldside (cold air in). The hotside is generally the rear of equipment and the rack. The coldside is generally the front panel of equipment and rack. The ducting of hot/cold air is often also standardised.

10.6.15. Standardising rack layout and cable management minimises problems caused by:

- Accidently not being able to locate end points of network and patch cables without tracing the cable end to end.
- Physically impeding access to equipment.
- Positioning of equipment and cables such that airflow (cooling) is impeded. As the density of equipment in racks increases, cooling becomes an increasingly important factor. Poor rack design combined with dense rack utilization can contribute to internal rack temperatures significantly higher than ambient room temperatures.

10.6.16. Standardising rack layout and cable management also assists in the maintenance of separation and segregation between **RED/BLACK** systems.

Standardised Rack Configuration

10.6.17. Separate **RED/BLACK** racks are easier to manage, build and maintain and reduce the opportunity for accidental or deliberate cross-connection of **RED/BLACK** systems. Ideally separate **RED/BLACK** racks should be used.

10.6.18. In small installations (typically single workstation) shared racks are unavoidable. In such cases a shared rack configuration is permissible **provided** separation elements and controls are properly implemented. Extra care must be taken to avoid accidental cross-connection of systems. The following illustrates a standardised shared rack configuration where **RED/BLACK** and power systems are separated:
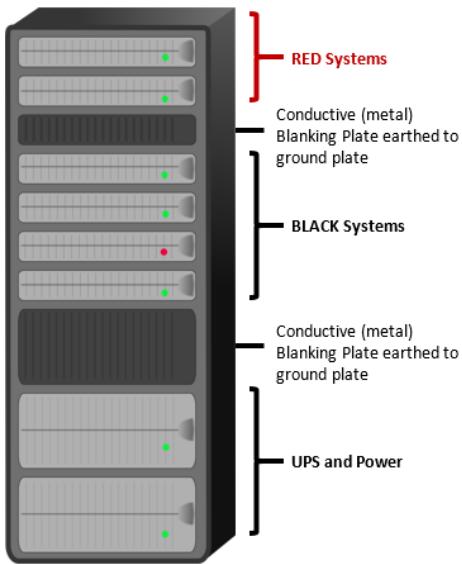
Figure 11: Separation of RED/BLACK

Separation of Cable Runs

10.6.19. In order to maintain the integrity of **RED**/**BLACK** separation, cables for power and data should be separately bundled as power **RED** or **BLACK** and data **RED** or **BLACK**. Cables should be run with as much distance between the bundles as can be practically managed, within the constraints of cable feeds and rack configuration. Ideally **RED** and **BLACK** should be on opposite sides of the rack. Cables should be no longer than required to avoid overlength cables compromising separation.

Access to BLACK equipment and components by uncleared staff and contractors

10.6.20. In some instances there may be a requirement for external technical or other uncleared personnel to access **BLACK** equipment and components for servicing, repair or replacement. Care must be taken to maintain the integrity of **RED** equipment and components. This can be especially problematic in shared rack configurations as described above.

This requirement should be identified before installation takes place and segregation measures implemented. Ideally physical separation of **BLACK** from **RED** is the best solution, recognising however, this may not always be possible or practical. Other solutions may include, for example, a shared

rack that has two doors with the **RED** door locked and alarmed so that **BLACK** equipment can be accessed without compromising the security of **RED** equipment. Discussion with the GCSB may identify other practical solutions.

References

10.6.21. Further References avaliable below:

Title	Publisher	Source
ISO/IEC 11801-5:2017 - Data centres	ISO/IEC	https://www.iso.org/standards.html
ISO/IEC TR 14763-2-1 - Information technology -- Implementation and operation of customer premises cabling -- Part 2-1: Planning and installation - Identifiers within administration systems	ISO/IEC	https://www.iso.org/standards.html
TIA-606-B- Administration Standard for the Telecommunications Infrastructure of Commercial Buildings	ANSI	https://www.ansi.org
ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers	ANSI	https://www.ansi.org
PD IEC/TR 62691:2016-Optical fibre cables. Guidelines to the installation of optical fibre cables	International Electrotechnical Commission (IEC) Available through Standards New Zealand	https://www.standards.govt.nz
PD IEC/TR 62362:2010 - Selection of optical fibre cable specifications relative to mechanical, ingress, climatic or electromagnetic characteristics. Guidance	International Electrotechnical Commission (IEC) Available through Standards New Zealand	https://www.standards.govt.nz
IEC 60794-2-31 Ed. 2.0 b(2012) - Optical fibre cables - Part 2-31: Indoor cables - Detailed specification for optical fibre ribbon cables for use in premises cabling	International Electrotechnical Commission (IEC) Available through Standards New Zealand	https://www.standards.govt.nz
IEC 60794-2-11 Ed. 2.0 b(2012)-Optical fibre cables - Part 2-11: Indoor optical fibre cables - Detailed specification for simplex and duplex cables for use in premises cabling	International Electrotechnical Commission (IEC) Available through Standards New Zealand	https://www.standards.govt.nz
AS/NZS 2967:2014 Optical fibre communication cabling systems safety	Standards New Zealand	https://www.standards.govt.nz
AS/NZS 14763.3:2017 Information technology - Implementation and operation of customer premises cabling - Part 3: Testing of optical fibre cabling	Standards New Zealand	https://www.standards.govt.nz
AS/NZS IEC 60825.2:2011 Safety of laser products - Part 2: Safety of optical fibre communication systems (OFCS)	Standards New Zealand	https://www.standards.govt.nz
AS/NZS ISO/IEC 24764:2012 - Generic cabling systems for data centres	Standards New Zealand	https://www.standards.govt.nz
AS/NZS 61386.1:2015 - Conduit systems for cable management - Part 1: General requirements	Standards New Zealand	https://www.standards.govt.nz
AS/NZS 61386.21:2015 - Conduit systems for cable management - Part 21: Particular requirements - Rigid conduit systems	Standards New Zealand	https://www.standards.govt.nz
AS/NZS 61386.22:2015 - Conduit systems for cable management - Part 22: Particular requirements - Pliable conduit systems	Standards New Zealand	https://www.standards.govt.nz
AS/NZS 61386.23:2015 - Conduit systems for cable management - Part 23: Particular requirements - Flexible conduit systems	Standards New Zealand	https://www.standards.govt.nz
AS/NZS ISO/IEC 29125:2012 - Telecommunications cabling requirements for remote powering of data terminal equipment	Standards New Zealand	https://www.standards.govt.nz

BS EN 61300-2-37:2016 - Fibre optic interconnecting devices and passive components. Basic test and measurement procedures. Tests. Cable bending for fibre optic closures	British Standards Institution (BSI) Available through Standards New Zealand	https://www.standards.govt.nz
BS EN 60794-2-31:2013 - Optical fibre cables. Indoor cables. Detailed specification for optical fibre ribbon cables for use in premises cabling	British Standards Institution (BSI) Available through Standards New Zealand	https://www.standards.govt.nz
BS EN 50411-2:2008 - Fibre organisers and closures to be used in optical fibre communication systems. Product specifications. General and guidance for optical fibre cable joint closures, protected microduct closures, and microduct connectors	British Standards Institution (BSI) Available through Standards New Zealand	https://www.standards.govt.nz
BS EN 60794-2-30:2008 - Optical fibre cables. Indoor cables. Family specification for ribbon cables	British Standards Institution (BSI) Available through Standards New Zealand	https://www.standards.govt.nz
BS EN 60794-2-21:2012 - Optical fibre cables. Indoor optical fibre cables. Detailed specification for multi-fibre optical distribution cables for use in premises cabling	British Standards Institution (BSI) Available through Standards New Zealand	https://www.standards.govt.nz

Rationale & Controls

10.6.22. Terminations to patch panels

10.6.22.R.01. Rationale

Cross-connecting a system to another system of a lesser classification through a patch panel may result in a data spill. A data spill could result in the following issues:

- inadvertent or deliberate access to information and systems by non-cleared personnel; and/or
- information spilling to a system of another classification.

10.6.22.R.02. Rationale

Cross-connecting Cables run to patch panels are best managed by bundling similar classifications or groups together. **RED**/**BLACK** separations should be maintained at all times. A simple approach to this is to bundle and run **RED** cables up vertical rails of the cabinet and **BLACK** cables up the opposite side. Where multiple cabinets are installed sides may be alternated to ensure **RED/RED** and **BLACK/BLACK** groupings are maintained by running cables groups up/down/across separate rails in the cabinet or in separate conduits.

10.6.22.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2425]

Agencies MUST ensure that only approved cable groups terminate on a patch panel.

10.6.22.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:5607]

RED and **BLACK** cables must be separated and bundled.

10.6.23. Patch cable and fly lead connectors

10.6.23.R.01. Rationale

Cables equipped with connectors specific to a classification will prevent inadvertent cross-connection. These connectors can be keyed or have specific profiles to prevent connection to other systems.

10.6.23.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2428]

In areas containing cabling for multiple classifications, agencies MUST ensure that the connectors for each classification are distinct and different to those of the other classifications.

10.6.23.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2429]

In areas containing cabling for multiple classifications, agencies MUST document the selection of connector types for each classification.

10.6.23.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2430]

In areas containing cabling for systems of different classifications, agencies SHOULD ensure that the connectors for each system are different to those of the other systems.

10.6.23.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2431]

In areas containing cabling for systems of different classifications, agencies SHOULD document the selection of connector types.

10.6.24. Physical separation of patch panels

10.6.24.R.01. Rationale

Appropriate physical separation between systems classified **CONFIDENTIAL** or above and a system of a lesser

classification (**RESTRICTED** and below) will:

- reduce or eliminate the chances of cross patching between the systems; and
- reduce or eliminate the possibility of unauthorised personnel or personnel gaining access to classified system elements.

Refer also to 10.1 – Cable Management Fundamentals for the discussion on **RED/BLACK** concept and cable separation.

10.6.24.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:2434]

Agencies SHOULD physically separate patch panels of different classifications by installing them in separate cabinets.

10.6.24.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2435]

Where spatial constraints demand patch panels of different classification are located in the same cabinet, agencies MUST:

- provide a physical barrier within the cabinet to separate patch panels;
- ensure that only personnel cleared to the highest classification of the circuits in the panel have access to the cabinet; and
- obtain approval from the relevant Accreditation Authority prior to installation.

10.6.25. Cabinet Arrangement

10.6.25.R.01. Rationale

Standardised layout of rack and cabinets facilitates maintenance and reduces risk of accidental cross-connects. Cabinets may also include UPS or other power supply equipment which is most appropriately housed at the bottom of the cabinet. RED/BLACK separations of equipment and cables should be maintained. Refer to 10.6.16 in the Context above.

10.6.25.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:5610]

Agencies SHOULD arrange the installation of cabinets as follows:

- **RED** equipment at the top;
- **BLACK** equipment in the centre;
- Power equipment at the bottom.

10.6.26. Rack Diagrams

10.6.26.R.01. Rationale

A rack diagram is a two-dimensional elevation drawing showing the layout or arrangement of equipment on a rack. It may show the front and the rear elevation of the rack layout. It does not have to be drawn to scale.   This provides essential information when maintenance or development is undertaken or new equipment installed.

10.6.26.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:5613]

Agencies SHOULD record equipment layouts and other relevant information on rack diagrams.

10.6.27. Fly lead installation

10.6.27.R.01. Rationale

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 then agencies will need to treat the cabling as infrastructure and run it in conduit or fixed infrastructure such as desk partitioning. Secure patch cords properly to keep them off the floor or the base of racks, where they can be stepped on.

10.6.27.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:2438]

Agencies SHOULD ensure that the fibre optic fly leads used to connect wall outlets to IT equipment either:

- do not exceed 5m in length; or
- 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; and
  - are approved by the Accreditation Authority.

10.6.28. Earthing and Bonding

10.6.28.R.01. Rationale

It is important that any metal trays or metal catenary are earthed for both safety and to avoid creating any fortuitous conductors. Effective earthing also depends on properly bonding all conductive elements of a cabinet, rack or case housing any equipment. Bonding requires good mechanical and electrical connection between conductive elements through bolts and nuts and/or earth straps or jump leads. Specialist bonding hardware is widely available.

10.6.28.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:5621]

All earthing points MUST be equipotentially bonded.

10.6.28.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:5623]

All conductive elements of a cabinet, rack or case housing any equipment MUST be earth bonded.

10.6.29. Cable Management

10.6.29.R.01. Rationale

Good cable management facilitates maintenance, promotes air flow and cooling, reduces risk of accidental cross-connects or disconnects and supports safe operation.

10.6.29.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:5626]

Cabinet rails MUST be installed to

- provide adequate room for patch cables and wire managers;
- provide adequate space for cable management at front, sides, and rear; and
- arrange switches and patch panels to minimize patching between cabinets & racks.

10.6.30. Labelling Cables

10.6.30.R.01. Rationale

The labelling principles include the following:

- Labelling is logical and consistent, across all locations, matching the project drawings;
- The labelling scheme identifies any associated physical locations (building, room, cabinet, rack, port, etc.);
- Labelling is easily read, durable, and capable of surviving for the life of the component that was labelled;
- The labelling system, and the identifiers used, are agreed upon by all stakeholders; and
- Labelling is all-encompassing and include cables, connecting hardware, conduits, firestops, grounding and bonding locations, racks, cabinets, ports, and telecommunications spaces.

10.6.30.R.02. Rationale

Specific labelling requirements include:

- All labels use a permanent identifier;
- The labelling/numbering scheme is logical in its organisation, using alphanumeric characters for ease of reference;
- Each cable and each pathway is labelled on each end, and each label identifies the termination points of both ends of the cable;
- All labels are legible, defacement resistance, and have high adhesion characteristics and durability;
- Labels are placed so they can be read without disconnecting a cable;
- Labels for station connections may appear on the face plate;
- All jack, connector, and block hardware are be labelled on either the outlet or panel; and
- All labels match with the any installation and maintenance records.

10.6.30.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:5627]

Agencies SHOULD implement the principles and specific cable labelling requirements described above.

10.6.31. Power Cords

10.6.31.R.01. Rationale

It is important to separate copper data cables and power cables as all power feeds, line and connectors have the potential to emanate, create magnetic fields and cause interference with copper data cables if laid in close proximity to each other. Good practice is to:

- Label power cords at both ends to minimise the risk inadvertently disconnecting the wrong power cord;
- Colour code power cords and power strips;
- Use locking power cords, receptacles, or retention clips.

10.6.31.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:5619]

Agencies SHOULD follow best practice described above for the installation of power cables.

10.7. Emanation Security Threat Assessments

Objective

10.7.1. In order to minimise compromising emanations or the opportunity for a technical attack, a threat assessment is used to determine appropriate countermeasures.

Context

Scope

10.7.2. This section relates to emanation security threat assessment advice and identification of appropriate countermeasures to minimise the loss of classified information through compromising emanations or a technical attack.

10.7.3. This section is applicable to:

- agencies located outside New Zealand;
- secure facilities within New Zealand; and
- mobile platforms and deployable assets that process classified information.

References

10.7.4. Information on conducting an emanation security threat assessment and additional information on cabling and separation standards, as well as the potential dangers of operating RF transmitters in proximity to classified systems, is documented in:

Title	Publisher	Source

NZCSS400 Installation Engineering	GCSB	CONFIDENTIAL document available on application to authorised personnel
NZCSI 403B TEMPEST Threat and Countermeasures Assessment	GCSB	CONFIDENTIAL document available on application to authorised personnel
NZCSI 420 Laboratory Tempest Test Standard for Equipment in Controlled Environments	GCSB	CONFIDENTIAL document available on application to authorised personnel

PSR references

10.7.5. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Security zones Validate your security measures Use multiple layers of security - 'defence in depth'	https://www.protectivesecurity.govt.nz/security-zones/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/validate-your-security-measures/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/design/defence-in-depth/
Managing specific scenarios	Secure your ICT facilities Physical Security for ICT systems	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/
Resource centre	Email fraud: an INFOSEC case study	

Rationale & Controls

10.7.6.   Emanation security threat assessments within New Zealand

10.7.6.R.01.   Rationale

Obtaining the current threat advice from GCSB on potential adversaries and threats and applying the appropriate countermeasures is vital in maintaining the confidentiality of classified systems from an emanation security attack.

10.7.6.R.02.   Rationale

Failing to implement recommended countermeasures 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 is very expensive and time consuming to retro-fit.

10.7.6.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2454]

Agencies designing and installing systems with RF transmitters within or co-located with their facility MUST:

- contact GCSB for guidance on conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.6.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:2455]

Agencies designing and installing systems with RF transmitters that co-locate with systems of a classification CONFIDENTIAL and above MUST:

- contact GCSB for guidance on conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.7.   Emanation security threat assessment outside New Zealand

10.7.7.R.01.   Rationale

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 countermeasures 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.

10.7.7.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2458]

Agencies deploying systems overseas in temporary, mobile or fixed locations MUST:

- contact GCSB for assistance with conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.7.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2459]

Agencies deploying systems overseas SHOULD:

- contact GCSB for assistance with conducting an emanation security threat advice; and
- install cabling and equipment in accordance with this document plus any specific installation criteria derived from the emanation security threat assessment.

10.7.8. Early identification of emanation security issues

10.7.8.R.01. Rationale

The identification of emanation security controls that need to be implemented for a system at an early stage in the project lifecycle. This can significantly affect project costs. Costs are invariably greater where changes are necessary once the system had been designed or has been implemented.

10.7.8.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2463]

Agencies SHOULD conduct an emanation security threat assessment as early as possible in project lifecycles.

10.7.9. IT equipment in SECURE areas

10.7.9.R.01. Rationale

All equipment must conform to applicable industry and government standards, including NZCSI 420; Laboratory Tempest Test Standard for Equipment in Controlled Environments. Not all equipment within a secure facility in New Zealand requires testing against TEMPEST standards.

10.7.9.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2465]

Agencies MUST ensure that IT equipment within secure areas meet industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

10.8. Network Design, Architecture and IP Address Management

Objective

10.8.1. IP Address architecture, allocation and addressing schemes enable and support system security and data protection.

Context

Scope

10.8.2. This section includes discussion of the principles of separation and segregation as network design and network architecture characteristics. It also discusses how IP addresses can be used to support these principles for improved security of larger or multi-classification agency systems.

Background

10.8.3. The larger the network, the more difficult it is to protect. A large, unsegmented network presents a large attack surface with greater susceptibility to the rapid spread and dissemination of system faults, weaknesses, vulnerabilities and attacks. In a non-segmented network, traffic and applications generally have access to the entire network. If a fault occurs or an attacker gains entry, the fault or attacker can move laterally through the network causing disruption, network outages and enabling access to critical operational or classified data.

10.8.4. A large network is also more difficult to monitor and control. Segmenting the network limits an attacker's ability to move through the network by preventing lateral movement between zones. Segmentation also enhances the ability to detect, monitor, control, isolate and correct faults.

10.8.5. A fundamental construct in the management of risk in networks is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular Trust Zone. Refer also to Section 22.1 – Cloud Computing and Section 22.2 – Virtualisation.

Separation and Segregation

10.8.6. Separation and Segregation are determined by system function and the sensitivity of the data the system stores, processes and transmits. One common example is placing systems that require a connection to the Internet into a demilitarized zone (DMZ) that is separated and segregated (isolated) from more sensitive systems. Another example is the use of compartments.

10.8.7. Separation and Segregation limits the ability of an intruder to exploit a vulnerability with the intent of elevating privileges to gain access to more sensitive systems on the internal network. VLANs may be used to further separate systems by controlling access and providing segregation thus giving additional protection.

10.8.8. Network segmentation is an effective strategy for protecting access to key data assets, and impeding the lateral movement of system faults, threats and malicious activity. Segregation has the following benefits:

- Enhanced performance: with fewer hosts per subnet, there is a reduced signalling and traffic overhead allowing more bandwidth for data communication.
- Improved security: with less signalling traffic going through all network segments, it is more difficult for an attacker to analyse the addressing scheme and network structure. Failures in one segment are less likely to propagate and more robust access control can be established and enforced.

10.8.9. Effective segregation also requires:

- Specialised knowledge: networks may support many devices with complex policies and rule sets. Support staff must be properly educated and trained to ensure the network segmentation is maintained.

- Administrative effort: changes in infrastructure, such as new applications and new technologies, can extend the time required to make changes and ensure the integrity of network segments.
- Infrastructure Investment: segregation may require more equipment, new equipment with advanced functionalities, or specific software to deal with multiple segments. These requirements should be considered during budget planning.

ISO 27001 and ISO 27002 implementation recommendations for network segregation

10.8.10. These ISO Standards require the implementation of network segregation. In particular they recommend that groups of information services, users, and information systems are segregated on networks. Specific recommendations are summarised below:

- Divide large networks into separate network domains (segments);
- Consider physical and logical segregation;
- Define domain perimeters;
- Define traffic rules between domains;
- Use authentication, encryption, and user-level network access control technologies;
- Consider integration of the organisation's network and segments with those of business partners.

10.8.11. The following structures and techniques should be considered:

- **Criteria-based segmentation**: Pre-define rules to establish perimeters and create new segments in order to reduce unnecessary redesign and future administrative overheads. Examples of criteria are trust level (e.g., external public segment, staff segment, server segment, database segment, suppliers segment, etc.), organisational unit (e.g., Operations, Service Desk, Outreach, etc.), and combinations (e.g., external public access).
- **Use of physical and logical segmentation:** Depending upon the risk level identified in the risk assessment, it may be necessary to use physically separated infrastructures to protect the organisation's information and assets (e.g., classified data flowing through a dedicated fibre), or you may use solutions based on logical segmentation like Virtual Private Network (VPN).
- **Access rules for traffic flowing**: Traffic between segments, including those of permitted external parties, should be controlled according to the need to access information. Gateways should be configured based on information classification and risk assessment. A specific case of access control applies to wireless networks, since they have poor perimeter definition. The recommendation is to treat wireless communication as an external connection until the traffic can reach a proper wired gateway before granting access to internal network segments. Refer also to Chapter 19 – Gateway Security.

Network Design

10.8.12. A poorly designed network has increased support costs, reduced availability, security risks, and limited support for new applications and solutions. Less-than-optimal performance affects end users and access to central resources. Some of the issues that stem from a poorly designed network may include the following:

- **Failure domains**: One of the most important reasons to implement an effective network design is to minimise the spread and extent of faults. When Layer 2 and Layer 3 boundaries are not clearly defined, failure in one network area can have a far-reaching effect.
- **Broadcast domains**: Broadcasts exist in every network. Many applications and network operations require broadcasts to function correctly; therefore, it is not possible to eliminate them completely. In the same way that avoiding failure domains involves clearly defining boundaries, broadcast domains should have clear boundaries and include an optimal number of devices to minimise the negative impact of broadcasts.
- **MAC unicast flooding**: Some switches limit unicast frame forwarding to ports that are associated with the specific unicast address. However, when frames arrive at a destination MAC address that is not recorded in the MAC table, they are flooded out of the switch ports in the same VLAN except for the port that received the frame. This behaviour is called unknown MAC unicast flooding.
- Because this type of flooding causes excessive traffic on all the switch ports, network interface cards (NIC) must contend with a larger number of frames on the wire. When data is propagated on a connection or network segment for which it was not intended, security can be compromised.
- **Multicast traffic on ports where it is not intended**: IP multicast is a technique that allows IP traffic to be propagated from one source to a multicast group that is identified by a single IP and MAC destination-group address pair. Similar to unicast flooding and broadcasting, multicast frames are flooded out all the switch ports. A robust design allows for the containment of multicast frames while allowing them to be functional.
- **Difficulty in management and support**: Traffic flows can be difficult to identify in a poorly designed network. This can make support, maintenance, and problem resolution time-consuming and difficult as well as creating security risks.
- **Possible security vulnerabilities**: A switched network that has been designed with little attention to security requirements at the access layer can compromise the integrity of the entire network.
- **Criteria-based segmentation**: Pre-define rules to establish perimeters and create new segments in order to reduce unnecessary redesign and future administrative overheads. Examples of criteria are trust level (e.g., external public segment, staff segment, server segment, database segment, suppliers segment, etc.), organisational unit (e.g., Operations, Service Desk, Outreach, etc.), and combinations (e.g., external public access).

Design Implementation

10.8.13. To assist in the implementation of separation and segregation as network design and architectural principles, the following aspects should be considered:

- Classification;
- Security Zones;
- IP Address Management;
- Central Information Repository;
- Private Use of Reserved Addresses;
- Devices with Default IP Addresses; and
- Connector types and cable colours.

Classification

10.8.14. Classified systems should, by definition, be segregated. This is particularly important where network elements have access to compartments and compartmented data.

10.8.15. Ideally compartmented elements of systems should be segregated and separated from the main network. This may include the use of a reserved address space, monitored to detect violations or unauthorised attempts to connect to compartments or to access compartmented data.

Security Zones

10.8.16. A security zone is a group of one or more physical or virtual firewall interfaces and the network segments connected to the zone's interfaces. Protection for each zone is individually specified and controlled so that each zone receives the specific protections it requires according to classification, endorsement, compartment and sensitivity of data.

IP Address Management

10.8.17. The fundamental goal of an IP addressing scheme is to ensure network devices are uniquely addressed. IP Address Schemes are a fundamental part of any network's security architecture and should support network separation and segregation. There are a number of techniques to assist in separating and segregating network elements. It is also useful to consider how to segregate and control network traffic through:

- Defined network perimeters and boundaries; and
- Defined network traffic rules.

10.8.18. A well-structured IP addressing scheme promotes the ability to quickly identify node properties from an IP address which assist in network management and fault finding and rectification.

Address Block Allocation

10.8.19. There are two main difficulties when assigning address blocks for types of devices. First is that over time there is insufficient provision for additional devices and network growth. When the allocated address block is exhausted, the addressing scheme is compromised (broken). The second is that you have a small number of devices in an address block, but are running out of addresses in other parts of the network. If you "borrow" from a pre-assigned address range, the addressing scheme is also compromised.

10.8.20. Internal IP address ranges are defined by the IETF. Commonly known as RFC 1918 addresses, the most recent RFC is 6761. These RFC's define private IP address ranges which cannot be used for external (Internet) IP addressing. Three address ranges (blocks) are defined:

IPv4 Address Range	Network IPv4 address Block	Directed Broadcast IPv4 address	IPv4 Addresses
10.0.0.0 to 10.255.255.255	10.0.0.0/8	10.255.255.255	16,777,216
172.16.0.0 to 172.31.255.255	172.16.0.0/12	172.31.255.255	1,048,576
192.168.0.0 to 192.168.255.255	192.168.0.0/16	192.168.255.255	65,536

10.8.21. IPv4 addresses are 32-bit binary addresses, divided into 4-Octets and normally represented in a decimal format. An example of IPv4 address is 192.168.100.10. IPv6 addresses are so much larger than IPv4 addresses and impractical to clearly represent in decimals. IPv6 addresses are usually represented in hexadecimal numbers, separated by a colon. An example of an IPv6 address is 2001:0DB8:0000:0002:0022:2217:FF3B:118C. Private IPv6 addresses are specified in RFC 4193

10.8.22. Private addressing is a means of distinguishing networks, assisting in separation and segregation.

Private use of reserved addresses

10.8.23. Some IP addresses have been reserved in IETF standards. Despite official warnings, some organisations use parts of the reserved IP address space for their internal networks where address space is exhausted or poorly designed. This creates conflicts with devices and signalling traffic protocols which can create network faults, anomalies and network outages. This practice is strongly discouraged.

Devices which have default IP addresses

10.8.24. Some devices are supplied with default IP addresses. If using the IETF RFC 1918 addressing protocol (e.g. 10.0.x.x) some devices may have been allocated the same (duplicate) IP address.

10.8.25. It is important to change default addresses to new addresses that conform with the addressing scheme selected for the agency.

DHCP

10.8.26. In theory, there is only one network device that absolutely needs a true static address, the DHCP server. In practice, it is preferable to assign address blocks to major groups of devices for control, fault isolation and security purposes. Traditionally static devices are provided with a reserved address. These devices may include:

- DCHP Server;
- Gateway devices;
- Firewalls;
- Routers; and
- Switches.

10.8.27. The majority of other devices can be allocated a DHCP address.

10.8.28. It is important to identify the essential device groups using a risk assessment, operational characteristics, level of security, system classification and other relevant architectural features, business requirements and operational constraints.

Connector Types and Cable Colours

10.8.29. Cable management is discussed in detail earlier in this chapter. In particular note the discussion (10.1.4) of Red/Black concepts which includes separation of electrical and electronic circuits, devices, equipment cables, connectors and systems that transmit store or process national security

information (Red) from non-national security information (Black)

10.8.30. Wherever practical and possible, connectors for systems of different classifications should be distinct and be selected to avoid accidental cross-connection of systems of different classifications. This can be achieved through the use of colour and keyed connectors where the colour and keying is different for each classification level or compartment (refer also to 10.1.30 and 10.6.6).

Central Information Repository

10.8.31. Creating a central repository of all the information on networks, IP addresses and devices, is critical to maintaining control of the network. The challenge with traditional tools is that there are often specific tools for each category of devices: one system to track virtual machines, one system to track wireless users, one system to track Windows servers, one system to track Linux machines, etc.

10.8.32. A single repository where all the data relevant to networks, hosts, servers, dynamic clients, and virtual environments can be tracked and synchronised is essential for larger networks. The ability to search across all this information will enable network teams to quickly track changing network landscapes and rapidly troubleshoot issues as they arise. In addition, business data related to a network resource helps bind together the logical network construct and the reality of IT resources.

References

10.8.33. Further references can be found at:

Title	Publisher	Source
Network Segmentation and Segregation	ASD	https://www.asd.gov.au/publications/protect/network_segmentation_segregation.htm
Cisco on Cisco Best Practices – Cisco IP Addressing Policy	Cisco	https://www.cisco.com/c/dam/en_us/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_IP_Addressing_Best_Practices.pdf
IP Addressing and Subnetting for New Users, Document ID: 13788	Cisco	https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.pdf
IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS Release 15S	Cisco	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_ipv4/configuration/15-s/ipv4-15-s-book.html
Introduction to Server and Domain Isolation	Microsoft	https://technet.microsoft.com/en-us/library/cc725770(v=WS.10).aspx
ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements	ISO	https://www.iso.org
ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls	ISO	https://www.iso.org
RFC-1518 - An Architecture for IP Address Allocation with CIDR	IETF	https://tools.ietf.org/html/rfc1518
RFC-1918 – Address Allocation for Private Internets	IETF	https://tools.ietf.org/html/rfc1918
RFC 2036 – Observations on the use of Components of the Class A Address Space within the Internet	IETF	https://tools.ietf.org/html/rfc2036
RFC 2050 – Internet Registry IP Allocation Guidelines	IETF	https://tools.ietf.org/html/rfc2050
RFC 2101 – IPv4 Address Behaviour Today	IETF	https://tools.ietf.org/html/rfc2101
RFC 2401 - Security Architecture for the Internet Protocol	IETF	https://tools.ietf.org/html/rfc4301
RFC 2663 – IP Network Address Translator (NAT) Terminology and Considerations	IETF	https://tools.ietf.org/html/rfc2663

RFC 2894 - Router Renumbering for IPv6	IETF	https://tools.ietf.org/html/rfc2894
RFC 3022 – Traditional IP Network Address Translator (Traditional NAT)	IETF	https://tools.ietf.org/html/rfc3022
RFC 3053 - IPv6 Tunnel Broker	IETF	https://tools.ietf.org/html/rfc3053
RFC 3056 - Connection of IPv6 Domains via IPv4 Clouds	IETF	https://tools.ietf.org/html/rfc3056
RFC 3232 - Assigned Numbers	IETF	https://tools.ietf.org/html/rfc3232
RFC 3260 – New Terminology and Clarifications for Diffserv	IETF	https://tools.ietf.org/html/rfc3260
RFC 3330 – Special-Use IPv4 Addresses" (superseded)	IETF	https://tools.ietf.org/html/rfc3330
FC 3879 – Deprecating Site Local Addresses	IETF	https://tools.ietf.org/html/rfc3879
RFC 3927 – Dynamic Configuration of IPv4 Link-Local Addresses	IETF	https://tools.ietf.org/html/rfc3927
RFC 3956 - Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address	IETF	https://tools.ietf.org/html/rfc3956
RFC 4193 – Unique Local IPv6 Unicast Addresses	IETF	https://tools.ietf.org/html/rfc4193
RFC-4632 - Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan	IETF	https://tools.ietf.org/html/rfc4632
RFC 5214 - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	IETF	https://tools.ietf.org/html/rfc5214
RFC 5737 - IPv4 Address Blocks Reserved for Documentation	IETF	https://tools.ietf.org/html/rfc5737
RFC 6040 - Tunnelling of Explicit Congestion Notification	IETF	https://tools.ietf.org/html/rfc6040
RFC 6052 - IPv6 Addressing of IPv4/IPv6 Translators	IETF	https://tools.ietf.org/html/rfc6052
RFC 6081 - Teredo Extensions	IETF	https://tools.ietf.org/html/rfc6081
RFC 6434 - IPv6 Node Requirements	IETF	https://tools.ietf.org/html/rfc6434
RFC 6598 – Reserved IPv4 Prefix for Shared Address Space	IETF	https://tools.ietf.org/html/rfc6598
RFC 6761 - Special-Use Domain Names	IETF	https://tools.ietf.org/html/rfc6761
RFC 6890 – Special-Purpose IP Address Registries	IETF	https://tools.ietf.org/html/rfc6890
RFC 7371 - Updates to the IPv6 Multicast Addressing Architecture	IETF	https://tools.ietf.org/html/rfc7371

| RFC 7619 - The NULL Authentication Method

in the Internet Key Exchange Protocol Version 2 (IKEv2)	IETF	https://tools.ietf.org/html/rfc7619
RFC 8012 - Label Switched Path (LSP) and Pseudowire (PW) Ping/Trace over MPLS Networks Using Entropy Labels (ELs)	IETF	https://tools.ietf.org/html/rfc8012
RFC 8190 - Updates to the Special-Purpose IP Address Registries	IETF	https://tools.ietf.org/html/rfc8190

Rationale & Controls

10.8.34. Risk Assessment

10.8.34.R.01. Rationale

A risk assessment is a fundamental tool in the architecture and design of a network.

10.8.34.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:5815]

Agencies MUST conduct and document a risk assessment before creating an architecture, and designing an agency network.

10.8.34.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:5816]

The principles of separation and segregation as well as the system classification MUST be incorporated into the risk assessment.

10.8.35. Security Architecture

10.8.35.R.01. Rationale

It is important that the principles of separation and segregation as well as the system classification are incorporated into the overall security architecture to maximise design and operational efficiency and to provide and support essential security to the network design.

10.8.35.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:5820]

Security architectures MUST apply the principles of separation and segregation.

10.8.36. Identification of major classifications/categories of network segments

10.8.36.R.01. Rationale

Identified in the risk assessment, it is essential that the classification of systems is clearly identified and is apparent in all architecture and design elements and systems documentation.

10.8.36.R.02. Rationale

Clear distinction of networks of different classifications is reinforced through the use of different IP addressing schemes as well as the application of Red/Black, separation and segregation concepts and principles. Refer also to section 10.1.

10.8.36.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:5825]

The classification and other restrictions on the security and control of information MUST be clearly identified for each part of the Agency network.

10.8.37. Visibility

10.8.37.R.01. Rationale

Clear identification and visibility of the classifications or category of a network segment is essential in minimising accidental cross-connections, incident management and in limiting the propagation of errors form one segment to others. This also assists in network maintenance and management.

10.8.37.R.02. Rationale

Clear visual identification is supported by the use of IP addressing and cable colour schemes as well as the use of different types of cable connectors for different network segments.

10.8.37.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:5843]

Systems of different classifications MUST be visually distinct.

10.8.38. Information Repository

10.8.38.R.01. Rationale

Clear documentation and records of changes to the architecture and construct of a network are essential in change management, planning, design of network modifications, incident management and maintenance of a strong security posture.

10.8.38.R.02. Rationale

A single repository where all the data relevant to networks, hosts, servers, dynamic clients, and virtual environments can be tracked and synchronised is essential for larger networks. The ability to search across all this information will enable network teams to quickly track changing network landscapes and rapidly troubleshoot issues as they arise.

10.8.38.R.03. Rationale

The repository should also contain business data related to a network resource which helps manage necessary changes and upgrades to a network in a fashion that appropriately allocates IT resources and recognises business needs.

10.8.38.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:5831]

An information repository, containing essential network information, change records and business requirements SHOULD be established and maintained.

11. Communications Systems and Devices

11.1. Radio Frequency and Infrared Devices

Objective

11.1.1. To maintain the integrity of secure areas, only approved radio frequency (RF) and infrared devices (IR) are brought into secure areas.

Context

Scope

11.1.2. This section covers information relating to the use of RF and infrared devices in secure areas. Information on the use of RF devices outside secure areas can be found in Chapter 21 - Working Off-Site.

11.1.3. RF devices include any transmitter on any frequency, including mobile phones, cordless phones, Bluetooth, Wi-Fi, RFID and other similar devices.

Exemptions for the use of infrared and laser devices

11.1.4. An infrared device and laser device can be used in a secure area provided it does not have the potential to communicate classified information.

Exemptions for the use of RF devices

11.1.5. 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;
- access control sensors; and
- laser pointers.

References

11.1.6.

Title	Publisher	Source
NIST 800-121 Guide to Bluetooth Security	NIST	http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf

PSR references

11.1.7. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Security zones	https://www.protectivesecurity.govt.nz/security-zones/
Managing specific scenarios	Secure your ICT facilities Mobile and remote working Physical Security for ICT systems Communication security	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/communications-security/

11.1.8.   Pointing devices

11.1.8.R.01.   Rationale

Wireless RF pointing devices can pose an emanation security risk. They are not to be used in secure areas unless within a RF screened building.

11.1.8.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:2483]

Wireless RF pointing devices MUST NOT be used in secure areas unless used within a RF screened building or RF mitigations are implemented.

11.1.9.   Infrared keyboards

11.1.9.R.01.   Rationale

When using infrared keyboards with CONFIDENTIAL or SECRET systems, drawn opaque curtains are an acceptable method of protecting windows and managing line of sight and reflected transmissions.

11.1.9.R.02.   Rationale

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. While infrared transmissions are generally designed for short range (5 to 10 metres) manufacturing and design variations and some environmental conditions can amplify and reflect infrared over much greater distances.

11.1.9.C.01.   Control System Classification(s): Confidential, Secret; Compliance: MUST NOT [CID:2487]

Agencies using infrared keyboards MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- 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; and
- infrared keyboards to be operated in areas with unprotected windows.

11.1.9.C.02.   Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:2488]

Agencies using infrared keyboards MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- multiple infrared keyboards at different classifications in the same area;
- other infrared devices within the same area; and
- infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.

11.1.9.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2489]

Agencies using infrared keyboards SHOULD ensure that infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecure area.

11.1.10. Bluetooth and wireless keyboards

11.1.10.R.01. Rationale

As the Bluetooth protocol provides little security and wireless keyboards often provide no security, they cannot be relied upon for the protection of classified information. As with infrared transmissions Bluetooth transmissions can reach considerable distances.

11.1.10.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2492]

Agencies MUST complete a technical evaluation of the secure area before the use of Bluetooth keyboards or other Bluetooth devices are permitted.

11.1.10.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:2494]

Agencies using Bluetooth keyboards or other Bluetooth devices MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- multiple keyboards or other devices at different classifications in the same area;
- other Bluetooth or infrared devices to be brought into range of the keyboard or its receiving device/port; and
- Bluetooth keyboards or other devices to be operated in areas with unprotected (non-shielded/curtained) windows.

11.1.10.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:2495]

Agencies MUST NOT use Bluetooth or wireless keyboards unless within a RF screened building.

11.1.11. RF devices in secure areas

11.1.11.R.01. Rationale

RF devices pose security threat as they are capable of picking up and transmitting classified background conversations. Furthermore, many RF devices can connect to IT equipment and act as unauthorised data storage devices or bridge "air gaps".

11.1.11.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2497]

Agencies MUST prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.

11.1.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2498]

Agencies SHOULD prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.

11.1.12. Detecting RF devices in secure areas

11.1.12.R.01. Rationale

As RF devices are prohibited in secure areas, agencies should deploy technical measures to detect and respond to the unauthorised use of such devices.

11.1.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:2501]

Agencies SHOULD deploy measures to detect and respond to active RF devices within secure areas.

11.1.13. RF controls

11.1.13.R.01. Rationale

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.

11.1.13.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2504]

Agencies SHOULD limit the effective range of communications outside the agency's area of control by:

- minimising the output power level of wireless devices;
- RF shielding; and
- Physical layout and separation.

11.2. Fax Machines, Multifunction Devices and Network Printers

Objective

11.2.1. Fax machines, multifunction devices (MFD's) and network printers are used in a secure manner.

Context

Scope

11.2.2. This section covers information relating to fax machines, MFDs and network printers connected to either the ISDN, PSTN, HGCE or other networks. Further information on MFDs communicating via network gateways can be found in Section 20.2 - Data Import and Export

Rationale & Controls

11.2.3. Fax machine, MFD and network printer usage policy

11.2.3.R.01. Rationale

Fax machines, MFDs and network printers are capable of communicating classified information, and are a potential source of information security incidents. It is therefore essential that agencies develop a policy governing their use.

11.2.3.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2537]

Agencies MUST develop a policy governing the use of fax machines, MFDs, and network printers.

11.2.4. Sending fax messages

11.2.4.R.01. Rationale

Once a fax machine or MFD has been connected to cryptographic equipment and used to send a classified fax message it can pose risks if subsequently connected directly to unsecured telecommunications infrastructure or the public switched telephone network (PSTN). 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 an information security incident.

11.2.4.R.02. Rationale

Non-encrypted communications may be exposed in transmission and, if incorrectly addressed or an incorrect recipient number is entered, may cause a data breach.

11.2.4.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2543]

Agencies sending classified fax messages MUST ensure that the fax message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the public switched telephone network.

11.2.4.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2545]

Agencies MUST have separate fax machines or MFDs for sending classified fax messages and messages classified RESTRICTED and below.

11.2.5. Sending fax messages using HGCE

11.2.5.R.01. Rationale

The establishment and use of appropriate procedures for sending a classified fax message will ensure that it is sent securely to the correct recipient.

11.2.5.R.02. Rationale

Using the correct memory erase procedure will prevent a classified fax message being communicated in the clear.

11.2.5.R.03. Rationale

Implementing the correct procedure for establishing a secure call will prevent sending a classified fax message in the clear.

11.2.5.R.04. Rationale

Overseeing the receipt and transmission of fax messages, clearing equipment memory after use and then powering off the equipment will prevent unauthorised access to this information.

11.2.5.R.05.   Rationale

Ensuring fax machines and MFDs are not connected to unsecured phone lines will prevent accidentally sending classified messages stored in memory

11.2.5.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2557]

Agencies intending to use fax machines or MFDs to send classified information MUST comply with additional requirements. Contact the GCSB for further details.

11.2.6.   Receiving fax messages

11.2.6.R.01.   Rationale

Whilst the communications path between fax machines and MFDs may be appropriately protected, personnel need to remain cognisant of the need-to-know of the information that is being communicated. As such it is important that 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.

11.2.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2562]

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; and
- notify the sender immediately if the fax message does not arrive when expected.

11.2.7.   Connecting MFDs to telephone networks

11.2.7.R.01.   Rationale

When a MFD is connected to a computer network and a telephone network the device can act as a bridge between the networks. As such the telephone network needs to be accredited to the same classification as the computer network the MFD is connected to.

11.2.7.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:2568]

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.

11.2.7.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:2570]

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.

11.2.8.   Connecting MFDs to computer networks

11.2.8.R.01.   Rationale

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.

11.2.8.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:2575]

Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies MUST ensure that:

- each MFD applies user identification, authentication and audit functions for all classified information communicated by that device;
- these mechanisms are of similar strength to those specified for workstations on that network; and
- each gateway can identify and filter the classified information in accordance with the requirements for the export of data through a gateway.

11.2.9.   Copying documents on MFDs

11.2.9.R.01.   Rationale

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.

11.2.9.C.01.   Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:2578]

Agencies MUST NOT permit MFDs connected to computer networks to be used to copy classified documents above the classification of the connected network.

11.2.10. Observing fax machine and MFD use

11.2.10.R.01.   Rationale

Placing fax machines and MFDs in public areas can assist in reducing the likelihood that any suspicious use of fax machines and MFDs by personnel will go unnoticed.

11.2.10.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2581]

Agencies SHOULD ensure that fax machines and MFDs are located in an area where their use can be observed.

11.2.11. Servicing and Maintenance

11.2.11.R.01.   Rationale

Network and MFD printers invariably use hard disk drives, flash drives or other reusable storage which can contain copies of classified

information. Any maintenance or servicing should be conducted under supervision or by cleared personnel.

11.2.11.R.02. Rationale

Copiers and laser printers may use electrostatic drums as part of the reproduction and printing process. These drums can retain a "memory" of recent documents which can be recovered. Any storage devices or drums replaced during maintenance should follow the prescribed media disposal and destruction processes (See Chapter 13 – Decommissioning and Disposal).

11.2.11.R.03. Rationale

Toner cartridges and other components may incorporate a memory chip, often used to track pages numbers and estimate print capacity. These chips have read/write capability and may pose a risk to classified systems. Once chips have been removed, the toner cartridges themselves may be disposed of through supplier recycling or other approved disposal channels.

11.2.11.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2589]

Any maintenance or servicing MUST be conducted under supervision or by cleared personnel.

11.2.11.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2590]

Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing MUST be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.11.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2591]

Toner cartridges MUST have the memory chip removed before the cartridge is recycled or otherwise disposed of. The memory chip MUST be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.11.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2592]

Any maintenance or servicing SHOULD be conducted under supervision or by cleared personnel.

11.2.11.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2593]

Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing SHOULD be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.12. USB Devices

11.2.12.R.01. Rationale

MFDs may also be equipped with USB ports for maintenance and software updates. It is possible to copy data from installed storage devices to USB devices. Any use of USB capabilities must be carefully managed.

11.2.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2596]

The use of any USB capability MUST be conducted under supervision or by cleared personnel.

11.2.12.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2597]

The use of any USB capability SHOULD be conducted under supervision or by cleared personnel.

11.2.13. Decommissioning and Disposal

11.2.13.R.01. Rationale

The use of storage media and the characteristics of electrostatic drums allow the recovery of information from such devices and components. To protect the information, prescribed disposal procedures should be followed.

11.2.13.R.02. Rationale

The use of storage media and the characteristics of electrostatic drums allow the recovery of information from such devices and components. To protect the information, prescribed disposal procedures should be followed.

11.2.13.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2604]

Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents MUST be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.13.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2606]

Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents SHOULD be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.3. Telephones and Telephone Systems

Objective

11.3.1.   Telephone systems are prevented from communicating unauthorised classified information.

Context

Scope

11.3.2.   This section covers information relating to the secure use of fixed, including cordless, telephones, as well as the systems they use to communicate information.

11.3.3.   Information regarding Voice over Internet Protocol (VoIP) and encryption of data in transit is covered in Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony and Section 17.1 - Cryptographic Fundamentals.

11.3.4.   It MUST be noted that VOIP and cellular phones have some of the same vulnerabilities as wired and cordless phones.

11.3.5. Telephones and telephone systems usage policy

11.3.5.R.01.   Rationale

All unsecure telephone networks are subject to interception. The level of expertise needed to do this varies greatly. Accidentally or maliciously revealing classified information over a public telephone networks can lead to interception.

11.3.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:2627]

Agencies MUST develop a policy governing the use of telephones and telephone systems.

11.3.6. Personnel awareness

11.3.6.R.01.   Rationale

There is a high risk of unintended disclosure of classified information when using telephones. It is important that personnel are made aware of what levels of classified information they discuss on particular telephone systems as well as the audio security risk associated with the use of telephones.

11.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:2630]

Agencies MUST advise personnel of the maximum permitted classification for conversations using both internal and external telephone connections.

11.3.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2631]

Agencies SHOULD advise personnel of the audio security risk posed by using telephones in areas where classified conversations can occur.

11.3.7. Visual indication

11.3.7.R.01.   Rationale

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.

11.3.7.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2637]

Agencies permitting different levels of conversation for different types of connections MUST use telephones that give a visual indication of the classification of the connection made.

11.3.8. Use of telephone systems

11.3.8.R.01.   Rationale

When classified conversations are to be held using telephone systems, the conversation needs to be appropriately protected through the use of encryption measures.

11.3.8.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2643]

Agencies intending to use telephone systems for the transmission of classified information MUST ensure that:

- the system has been accredited for the purpose; and
- all classified traffic that passes over external systems is appropriately encrypted.

11.3.9. Cordless telephones

11.3.9.R.01.   Rationale

Cordless telephones have little or no effective transmission security, therefore should not be used for classified or sensitive communications. They also operate in an unlicensed part of the radio spectrum used for a wide range of other devices.

11.3.9.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:2648]

Agencies MUST NOT use cordless telephones for classified conversations.

11.3.9.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2649]

Agencies SHOULD NOT use cordless telephones for classified or sensitive conversations.

11.3.10. Cordless telephones with secure telephony devices

11.3.10.R.01.   Rationale

As the data between cordless handsets and base stations is not secure, cordless telephones MUST NOT be used for classified communications even if the device is connected to a secure telephony device.

11.3.10.C.01.   Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:2652]

Agencies MUST NOT use cordless telephones in conjunction with secure telephony devices.

11.3.11. Speakerphones

11.3.11.R.01.   Rationale

Speakerphones are designed to pick up and transmit conversations in the vicinity of the device they should not be used in secure areas as the audio security risk is extremely high.

11.3.11.R.02.   Rationale

If the agency is able to reduce the audio security risk through the use of appropriate countermeasures then an exception may be approved by the Accreditation Authority.

11.3.11.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2656]

If a speakerphone is to be used on a secure telephone system within a secure area, agencies MUST apply the following controls:

- it is located in a room rated as audio secure;
- the room is audio secure during any conversations;
- only cleared personnel involved in discussions are present in the room; and
- ensure approval for this exception is granted by the Accreditation Authority.

11.3.12. Off-hook audio protection

11.3.12.R.01. Rationale

Providing off-hook security minimises the chance of accidental classified conversation being coupled into handsets and speakerphones. Limiting the time an active microphone is open limits this threat. This is normally achieved with push-to-talk (PTT) mechanisms.

11.3.12.R.02. Rationale

Simply providing an off-hook audio protection feature is not, in itself, sufficient. To ensure that the protection feature is used appropriately personnel will need to be made aware of the protection feature and trained in its proper use. Where PTT or some other similar functionality is installed, the activation mechanism (such as a button or switch) must be clearly labelled.

11.3.12.R.03. Rationale

Many new digital desk phones control these functions through software, rather than a mechanical switch.

11.3.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2661]

Agencies MUST ensure that 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.

11.3.12.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2662]

Agencies MUST use push-to-talk mechanisms to meet the requirement for off-hook audio protection. PTT activation MUST be clearly labelled.

11.3.12.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2663]

Agencies SHOULD ensure that 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.

11.3.13. Electronic Records Retention and Voicemail

11.3.13.R.01. Rationale

Voicemail and other messages and communications may fall within the legal definition of electronic records. If so retention and archive requirements are prescribed.

11.3.13.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2666]

Agencies MUST remove unused voice mailboxes.

11.3.13.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:2667]

Agencies MUST expire and archive or delete voicemail messages after the retention period determined by the agency's electronic records retention policy.

11.3.13.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2669]

Agencies SHOULD develop and implement a policy to manage the retention and disposal of such electronic records, including voicemail, email and other electronic records.

11.4. Mobile Telephony

Objective

11.4.1. Mobile telephone systems and devices are prevented from communicating unauthorised classified information.

Context

Scope

11.4.2. This section covers information relating to the secure use of mobile telephones, tablets and other mobile, voice communication capable devices, as well as the systems they use to communicate information.

11.4.3. Mobile devices use RF in various parts of the spectrum to communicate including Wi-Fi, cellular, satellite, RFID, and NFC frequencies. All such mobile devices are considered to be transmitters.

11.4.4. Mobile devices with cellular capability will regularly "poll" for the strongest signal and base or relay station. Monitoring such activity can be used for later interception of transmissions.

11.4.5. Information regarding Voice over Internet Protocol (VoIP) and encryption of data in transit is covered in Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony and Section 17.1 - Cryptographic Fundamentals.

11.4.6. It is important to note that VoIP phones have some of the same vulnerabilities as the mobile devices discussed in this section.

11.4.7. Mobile devices can be equipped with a variety of capabilities including internet connectivity, cameras, speakerphones, recording and remote control. Such devices are also susceptible to Internet malware and exploits. All risks related to the use of the Internet will apply to mobile devices with 3g/4g/5g capability.

PSR references

11.4.8.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Security zones	https://www.protectivesecurity.govt.nz/security-zones/
Managing specific scenarios	Secure your ICT facilities Mobile and remote working Physical Security for ICT systems Communication security	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/communications-security/

Rationale & Controls

11.4.9.   Mobile device usage policy

11.4.9.R.01.   Rationale

All mobile devices are subject to interception. The required level of expertise needed varies greatly. Accidentally or maliciously revealing classified information over mobile devices can be intercepted leading to a security breach.

11.4.9.C.01.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:2691]

Agencies MUST develop a policy governing the use of mobile devices.

11.4.10. Personnel awareness

11.4.10.R.01. Rationale

There is a high risk of unintended disclosure of classified information when using mobile devices. It is important that personnel are aware of what levels of classified information they discuss as well as the wide range of security risks associated with the use of mobile devices.

11.4.10.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:2694]

Agencies MUST advise personnel of the maximum permitted classification for conversations using both internal and external mobile devices.

11.4.10.C.02. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2695]

Agencies SHOULD advise personnel of all known security risks posed by using mobile devices in areas where classified conversations can occur.

11.4.11. Use of mobile devices

11.4.11.R.01. Rationale

When classified conversations are to be held using mobile devices the conversation needs to be appropriately protected through the use of encryption measures and a secure network.

11.4.11.C.01. Control **System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST** [CID:2698]

Agencies intending to use mobile devices for the transmission of classified information MUST ensure that:

- the network has been certified and accredited for the purpose;
- all classified traffic that passes over mobile devices is appropriately encrypted; and
- users are aware of the area, surroundings, potential for overhearing and potential for oversight when using the device.

11.4.12. Mobile Device Physical Security

11.4.12.R.01. Rationale

Mobile devices are invariably software controlled and are subject to malware or other means of compromise. No "off-hook" or "power off" security can be effectively provided, creating vulnerabilities for secure areas. Secure areas are defined in Chapter 1 at 1.1.35.

11.4.12.C.01. Control **System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST** [CID:2701]

Mobile devices MUST be prevented from entering secure areas.

11.4.12.C.02. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2702]

Agencies SHOULD provide a storage area or lockers where mobile devices can be stored before personnel enter secure or protected areas.

11.5. Personal Wearable Devices

Objective

11.5.1. Wearable devices are prevented from unauthorised communication or from compromising secure areas.

Context

Scope

11.5.2. This section covers information relating to the use of personal wearable devices, fitness devices, smart watches, devices embedding in clothing and similar wearable devices.

11.5.3. These devices can use RF in various parts of the spectrum to communicate including Wi-Fi, cellular, satellite, RFID, NFC and Bluetooth frequencies as well as providing data storage capability, audio and video recording and USB connectivity. All such wearable or mobile devices are considered to be transmitters.

11.5.4. Personal wearable devices can be equipped with a variety of capabilities including smart phone pairing, internet connectivity, cameras, speakerphones, audio and video recording and remote control. Some devices (for example Narrative and Autographer) will automatically take snapshots at intervals during the day. In some cases the snapshots are geotagged.

11.5.5. Such devices are also susceptible to Internet malware and exploits. All risks related to the use of the Internet will apply to these devices.

11.5.6. Merely disabling the capabilities described above is not a sufficient mitigation and is not acceptable, posing a high risk of compromise, whether intentional or accidental. The device MUST NOT have such capabilities installed if the device is to enter a secure area.

11.5.7. There is a wide variety of devices now available with upgrades and new models appearing frequently. There are many hundreds of models with a variety of custom operating systems and programmes and other applications. Some industry surveys and predications are forecasting explosive growth in the use of wearable devices, reaching over 100 million devices by 2020. Checking the capabilities and vulnerabilities of each device and subsequent security testing or validation will be an onerous task for agencies and may be infeasible.

Key Risk Areas

11.5.8. Personal wearable devices are not only about the technological aspects, the human factor is equally important. Users often forget about personal information security and their own safety, which enables social engineering attacks on the devices. The main protective measure for users is awareness, but even the *trust-but-verify* rule is not completely reliable in this situation. Accordingly, the information gathered by wearable devices should be appropriately secured to maintain privacy and personal security.

11.5.9. There are four important risk groups to be considered when managing personal wearable devices:

1. Data leaks and breaches;
2. Network security compromises;
3. Personally Identifiable Information (PII) leaks; and
4. Privacy violations.

Personally Identifiable Information (PII)

11.5.10. In most cases, the protection of PII will be the responsibility of the individual. In cases where the use of devices is permitted under a medical exemption, agencies MAY be required to ensure that devices that collect and store data comply with relevant regulation and guidance, such as the Privacy Act and the HIPAA.

PSR references

11.5.11. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Security zones	https://www.protectivesecurity.govt.nz/security-zones/
Managing specific scenarios	Secure your ICT facilities Mobile and remote working Physical Security for ICT systems Communication security	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/communications-security/

References

11.5.12. Further references can be found at:

References	Publisher	Source
ITL bulletin for April 2010 - Guide to protecting personally identifiable information	NIST	http://csrc.nist.gov/publications/nistbul/april-2010_guide-protecting-pii.pdf
NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) - Recommendations of the National Institute of Standards and Technology	NIST	http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
Privacy Act 1993 (the Privacy Act)		Office of The Privacy Commissioner http://www.privacy.org.nz/ http://www.legislation.govt.nz/
The Health Insurance Portability and Accountability Act of 1996 (USA)	US Congress	https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm http://www.hhs.gov/hipaa
Health Information Technology for Economic and Clinical Health Act (HITECH Act) (USA)	US Congress	https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html
Technology, Media and Telecommunications Predictions, 2014	Deloitte	http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-predictions-2014-interactive.pdf
Technology, Media and Telecommunications Predictions, 2015	Deloitte	http://www2.deloitte.com/au/en/pages/technology-media-and-telecommunications/articles/tmt-predictions.html
Study: Wearable Technology & Preventative Healthcare	Technology Advice Research	http://technologyadvice.com/
Security Analysis of Wearable Fitness Devices (Fitbit)	Massachusetts Institute of Technology	https://courses.csail.mit.edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf
Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device	School of Computing and Information Sciences, Florida International University	https://arxiv.org/pdf/1304.5672.pdf
Survey of Security and Privacy Issues of Internet of Things		http://arxiv.org/ftp/arxiv/papers/1501/1501.02211.pdf

Rationale & Controls

11.5.13. Personal Wearable Device usage policy

11.5.13.R.01. Rationale

Any device that uses part of the RF spectrum to communicate is subject to interception. The required level of expertise to conduct intercepts needed varies greatly. Other capabilities of Personal Wearable Devices can be used for malicious purposes, including the theft of classified information and revealing the identities of personnel. Accidentally or maliciously revealing classified information through Personal Wearable Devices can lead to a security breach.

11.5.13.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2736]

Agencies MUST develop a policy governing the use of personal wearable devices, including fitness devices.

11.5.14. Personnel awareness

11.5.14.R.01. Rationale

There is a high risk of unintended disclosure of classified information when using personal wearable devices. It is important that personnel are aware of the level of classified information they discuss, the environment in which they are operating as well as the wide range of security risks associated with the use of mobile and personal wearable devices.

11.5.14.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2750]

Agencies MUST advise personnel of the maximum permitted classification for conversations where any personal wearable or mobile device may be present.

11.5.14.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2752]

Agencies SHOULD advise personnel of all known security risks posed by using personal wearable devices in secure areas or other areas where classified conversations can occur.

11.5.15. Mobile Device Physical Security

11.5.15.R.01. Rationale

Personal wearable devices are invariably software controlled and can be infected with malware or other means of compromise. No "off-hook" or "power off" security can be effectively provided, creating vulnerabilities for secure areas. Secure areas are defined in Chapter 1 at 1.1.33.

11.5.15.C.01. Control**System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT** [CID:2758]

Personal wearable devices MUST NOT be allowed to enter secure areas.

11.5.15.C.02. Control**System Classification(s): All Classifications; Compliance: SHOULD** [CID:2759]

Agencies SHOULD provide a storage area or lockers where personal wearable devices can be stored before personnel enter secure or protected areas.

11.5.16. Medical Exemptions

11.5.16.R.01. Rationale

In some isolated cases personal wearable devices are necessary for the medical well-being of the individual. In such cases personal wearable devices MAY be permitted with the written authority of the Agency's Accreditation Authority. Such devices MUST NOT have any of the following capabilities:

- Camera;
- Microphone;
- Voice/video/still photograph recording;
- Cellular, Wi-Fi or other RF.

Merely disabling such capabilities is not acceptable. The device MUST NOT have such capabilities installed. Permitted device capabilities are:

- Accelerometer;
- Altimeter;
- Gyroscope;
- Heart Activity monitor;
- Vibration feature for the personal notification purposes.

11.5.16.R.02. Rationale

Personal wearable devices may contain Personally Identifiable Information (PII) of the individual using the device. This may be on the device itself in printed or electronic form, and also in the registers of tested, permitted or rejected devices in use within the agency. It is important that relevant legislation and regulation pertaining to the protection of PII is followed.

11.5.16.C.01. Control**System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT** [CID:2763]

Any personal wearable devices approved on medical grounds MUST NOT have any of the following capabilities:
Camera;
Microphone;
Voice/video/still photograph recording;
Cellular, Wi-Fi or other RF means of transmission.

11.5.16.C.02. Control**System Classification(s): Confidential, Top Secret, Secret; Compliance: MUST** [CID:2765]

Where personal wearable devices are exempted on medical grounds and used in secure areas agencies MUST ensure that:

- the agency networks in secure areas have been certified and accredited for the purpose; and
- users are aware of the area, surroundings, potential for overhearing and potential for oversight.

11.5.16.C.03. Control**System Classification(s): All Classifications; Compliance: MUST** [CID:2767]

Where the use of personal wearable devices is permitted on medical grounds and used within a corporate or agency environment, agencies MUST ensure any relevant legislation and regulation pertaining to the protection of Personally Identifiable Information (PII) is followed.

11.6. Radio Frequency Identification Devices

Objective

11.6.1. To ensure Radio Frequency Identification (RFID) devices are used safely and securely in order to protect privacy, prevent unauthorised access and to prevent the compromise of secure spaces.

Context

Scope

11.6.2. This section provides information relating to the risks, security and secure use of RFID devices. Access Control Systems incorporating RFID or smart cards are discussed in more detail in Section 11.7 - Access Control Systems.

Background
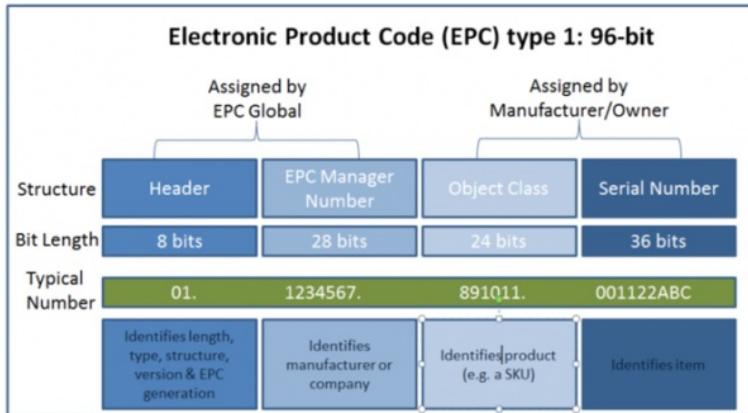
11.6.3. This section contains a short description of the history, formats, operating frequencies, risks, controls and countermeasures related to the use of RFID.

11.6.4. In practical use since the 1970's, RFID is now widely used for product identification, stock control, as anti-theft in manufacturing and retail organisations, payment cards (smart ATM and paywave cards) and access control systems. They are useful tools in improving logistics, profoundly changing cost structures for business, and improving levels of safety and authenticity in a wide range of applications such as access control, passports, payment cards, vehicle immobilisers, toll roads, pharmaceuticals tracking, management of high value items and weapons control. RFID tags are now produced in a wide variety of types and sizes, from the size of a grain of rice or printed on paper to much larger devices incorporating a battery or other power supply.

11.6.5. Unlike bar coding systems, RFID devices can communicate without requiring line of sight and over distances ranging from a few centimetres to kilometres. They can be equipped with sensors to collect data on temperature changes, sudden shocks, humidity or other factors affecting product safety and quality.

11.6.6. RFID devices typically use radio signals to transmit identifying information such as product or serial numbers, manufacture date, origin and batch number. This identifying information is invariably in the form of an Electronic Product Code (EPC) following the standards and conventions published by GS1. GS1 is a global group that also develops standards for other identifiers such as barcodes. The GS1 standards and conventions are now incorporated into ISO standards, see references table at 11.6.55.

Basic Formats

11.6.7. The basic format of an Electronic Product Code (EPC) is illustrated below:

11.6.8. RFID devices are often referred to as "tags". Passive tags are unpowered and harvest power from the RFID reader. Active tags incorporate a power supply, usually a battery. Tags are produced in Classes 0 to 5 and are now generally produced to Generation 2 specifications. The EPCGen2 standard for Class 1 tags focuses on reliability and efficiency but supports only very basic security. Features of the Gen 2 specification include:

- **a 96 bit EPC number** with read/write capability and can be designated used for other data ;
- **a 32/64 bit tag identifier** (TID) – identifies the manufacturer of the tag, also with read/write capabilities;
- **32 bit kill password** to permanently disable the tag;
- **32 bit access password** to lock the read/write characteristics of the tag and also set the tag for disabling ;
- **User memory** – dependant on the manufacturer and can be as little as 0 bits to 2048 bits. Larger user memory is in development.

11.6.9. The distance from which a tag can be read is termed the read range. A read range will depend on a number of factors, including the radio frequency used for reader/tag/reader communication, the size and orientation of the antennae, the power output of the reader, and whether the tags have a battery or other power supply. Battery-powered tags typically have a read range of 100 meters (approximately 300 feet) although this can extend to kilometres under favourable conditions. It is possible that powered RFID tags, typically used on cargo containers, railway wagons, vehicles and other large assets, could be read from a satellite if there is little background "noise" and the broadcast signal is sufficiently powerful.

11.6.10. RFID tags are divided into classes 0 to 5:

Class	Description
0	Read only, passive tags
1	Write once passive tags. 128-bit memory.
2	Read/Write with up to 65Kb read/write memory and authenticated access control. Can monitor temperature, pressure, vibration.
3	Semi-Passive. Own power source but cannot initiate communication. Remains passive until activated by a reader. Up to 65 Kb read/write memory and integrated sensor circuitry.
4	Active tags (own power source) with integrated transmitter. Can communicate with readers and other tags operating in the same RF band. Rewritable memory and ad hoc networking capability. Read range >100 metres (approx. 300').
5	Reader tags, can power class 1 to 3 tags and communicate with all classes. Includes all the capabilities of class 4 tags.

Operating Frequencies

11.6.11. RFID operates in several parts of the Radio Spectrum. Not all frequencies are authorised for use in all countries and will depend on the radio spectrum allocation authority in each country. It is important to note, however, that some RFID tags designed to operate at frequencies not used in the importing country may be attached to imported goods. This can represent a risk from scanning at frequencies not authorised or normally monitored in the importing country.

11.6.12. Depending on the design and intended application, RFID tag can operate at different frequencies. It is important to note that longer range RFID tags operate at frequencies close to or within allocated Wi-Fi frequencies. Allocated frequencies are:

Band	Frequency	Typical Range
LF	125-134.2 kHz and 140-148.5 kHz	Up to 1/2 metre
HF	13.553 - 13.567 MHz and 26.957 - 27.283 MHz	Up to 1 metre
UHF	433 MHz, 858 - 930 MHz, 2.400 - 2.483 GHz, 2.446 - 2.454GHz	1 to 10 metres
SHF	5.725 - 5.875 GHz	> 100 metres

11.6.13. As RFID devices are deployed in more sophisticated applications such as matching hospital patients with laboratory test results or tracking systems for dangerous materials, concerns have been raised about protecting such systems against eavesdropping, unauthorised uses and privacy breaches.

Smart Cards

11.6.14. Smart cards typically comprise an embedded integrated circuit incorporating a microchip with internal memory, a read-only CSN (Card Serial Number) or a UID (User Identification). The card connects to a reader with direct physical contact or a contactless radio frequency (RFID) interface. With an embedded microchip, smart cards can store large amounts of data, carry out on-card functions (such as encryption and authentication) and interact intelligently with a smart card reader. Smart card technology can be found in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in mobile phones, and USB-based tokens. Smart cards are widely used in payment card (debit and credit cards and electronic wallets) and access control systems.

11.6.15. The ISO/IEC 14443 standard for contactless smart card communications defines two types of contactless cards ("A" and "B") and allows for communications at distances up to 10 cm operating at 13.56 MHz. The alternative ISO/IEC 15693 standard allows communications at distances up to 50 cm. The ISO/IEC 7816 standard (in 15 parts) defines the physical, electrical interface and operating characteristics of these cards.

11.6.16. In common with other RFID devices, smart cards incorporate an antenna embedded in the body of the card (or key fob, watch or token). When the card is brought within range of the reader, the chip in the card is powered on. Once powered on, an RF communication protocol is initiated and communication established between the card and the reader for data transfer.

11.6.17. Smart cards typically incorporate protective mechanisms including authentication, secure data storage, encryption, tamper-resistance and secure communication. Support for biometric authentication may also be incorporated.

Threats and Vulnerabilities

11.6.18. Some important characteristics of RFID, inherent in the design and properties of the technology are:

- RFID tags are powered by the field emitted by an RFID reader, so whenever a tag is placed in a reader field it is activated and available. In general terms, class 0 and class 1 tags cannot be powered off, only permanently deactivated;
- RFID tags automatically respond to reader interactions without explicit control of the tag owner, so RFID tags can be operated without their owner's consent;
- It is trivial to establish a communication with an RFID tag and there is no visual confirmation of a tag/reader interaction (i.e., no physical connection or manual operation is required), so it is possible to interact with an RFID tag without being detected.

11.6.19. Specific threats and vulnerabilities in the use of RFID technologies include:

- **Legitimate data-mining**: This risk predates the use of RFID technology, but the volume of data provided by RFID tags, loyalty cards, Near Field Communication (NFC) for bank cards and for electronic wallets increases the risk. Some data collection methods keep to ethical use of data-mining techniques to discover the characteristics and habits of an individual or an organisation. This can pose a business intelligence risk. At times, however, this may challenge the bounds of privacy and data ownership. For example, customer loyalty card data used to discover medical information about an individual or RFID tags to track shipments or deliveries to an organisation by a competitor.
- **Eavesdropping and Data theft**: This risk is similar to the data-mining risk but employs unethical and possibly illegal methods of data collection or obtaining data for nefarious or malicious purposes. RFID tags are designed to broadcast information and data theft by easily concealable RFID scanners is technically trivial. Data theft can pose a risk to business processes.
- **Skimming**: Occurs when an unauthorised reader gains access to data stored on a token. This type of attack is particularly dangerous where contactless access or payment cards are used.
- **Relay Attacks**: Relay attacks use eavesdropping to intercept legitimate tag/reader transmissions and relay these to a device at some distance from the legitimate tag. The device can then behave as the genuine tag. Again this type of attack is particularly dangerous where contactless access or payment cards are used.
- **Insert Attacks**: Insert attacks insert system commands where normal data is expected and relies on a lack of data validation. It is possible that a tag can have legitimate data replaced by a malicious command.
- **Tag Cloning**: Clones replicate the functionality of legitimate tags and can be used to access controlled areas, abuse private data, or make an unauthorised electronic transaction. Tag authentication using a challenge-response protocol is a defence against cloning as the information that attackers can obtain through the air interface (such as by eavesdropping) is insufficient to provide a legitimate response. The design of the tag can also incorporate measures at the circuit manufacturing stage to protect tags from duplication by reverse engineering.
- **Data corruption**: Most RFID tags are rewritable by design. This feature may be locked (turning the tag into a write-once, read-many device) or left active, depending on application and security sensitivity. For example, in libraries, the RFID tags are frequently left unlocked for the convenience of librarians in reusing the tags on different books or to track check-ins and check-outs. If tags are not protected, it creates an opportunity for malicious users to overwrite data, typically in the theft of high-value goods by marking them as low-value items or in the case of weapons monitoring, changing the weapon identification.
- **Shipment or People tracking**: While RFID tags are designed to assist in stock control and supply chain management, unauthorised tracking of shipments or of people is undesirable and may even be dangerous. It is possible to follow individuals carrying tags using several techniques, including placing fake readers at building access points, deploying unauthorised readers near legitimate readers and creating relay points along expected routes.
- **Tag Blocking**: This is a form of denial of service by introducing a blocker tag which is designed to simulate all possible tags in an allocated range. This causes readers to continually perform multiple reads on non-existent and non-responsive tags. Blocker tags are sometimes used where privacy or confidentiality are required.

- **Denial of Service (DOS)**: Also known as flooding attacks where a signal is flooded with more data than it is designed to handle. Similar in many respects to RF Jamming.

Attack Vectors

11.6.20. Attack vectors for RFID devices include:

- interception of legitimate transmissions (man-in-the-middle [MITM] attacks);
- interception of authorised reader data by an unauthorised device;
- unauthorised access to tags and readers;
- rogue/cloned tags;
- rogue and unauthorised RFID readers;
- side-channel attacks (timing measurements, electromagnetic radiations etc.);
- attacks on back-end systems;
- jamming of legitimate signals.

11.6.21. Because RFID devices incorporate antennas, there is a possibility of radiation hazards from high –powered devices, particularly active tags and readers. It is important to note however that these cases are rare, occur in high powered devices only and that the vast majority of RFID devices do not pose radiation hazards. Related hazards include electromagnetic radiation hazards to personnel (HERP), fuel (HERF) and ordnance (HERO).

11.6.22. Threats and Vulnerabilities of RFID systems are summarised in the table below:

Threat/Vulnerability	Tag	RF	Reader	Network	Back-End	People
Eavesdropping	●	●		●	●	
Relay Attack		●				
Unauthorised Tag Reading (skimming)	●	●	●			
People Tracking	●	●				●
Shipment Tracking	●	●				
Tag Cloning	●	●				
Replay Attack	●	●				
Insert Attack	●		●	●	●	
Tag Content Modification	●					
Malware	●		●	●	●	
RFID System Failure			●	●	●	●
Tag Destruction	●					
Tag Blocking	●	●				
Denial of Service (DoS)	●		●	●		
RF Jamming	●	●				●
Back-End Attacks				●	●	
Radiation Hazard	●	●	●			●

11.6.23. It is important to note that attacks are often used in combination creating blended attacks. Blended attacks may be a combination of attack types, use of multiple attack vectors, the targeting of individual sub-systems or combinations of all three elements.

Good Practices and Countermeasures

11.6.24. Good practice for ensuring the security and privacy of RFID systems includes:

- a risk assessment to determine the nature and extent of risk and threat in the proposed use of RFID;
- strong security architecture to protect RFID databases and communication systems;
- authentication of approved users of RFID systems;

- encryption of radio signals when feasible;
- temporarily or permanently disabling tags when not required;
- shielding RFID tags and tag reading areas to prevent unauthorised access or modification;
- incident management, audit procedures, logging and time stamping to help detect and manage security breaches; and
- tag disposal and recycling procedures that permanently disable or destroy sensitive data.

Authentication

11.6.25. By design and usage, RFID technologies are item, product or shipment identification **but** not authentication technologies. Authentication of a reader or tag requires a common secret (key) shared when establishing communication, and before data is exchanged. Currently, only RFID tags with microprocessors have sufficient computation resources to use authentication techniques. These can be found in such applications as e-passports, or payment or ticketing applications (public transport, for example).

11.6.26. With a challenge/response authentication mechanism the reader issues an enquiry to the tag which results in a response. The secret tag information is computed information from internal cryptographic algorithms by both the tag and reader and the results are sent. Correct responses are required for a successful information exchange. The system is essentially the same as encrypting data over a standard radio link.

11.6.27. The ISO/JTC1/SC31 committee is in the process of establishing new standards to support the use of simple RFID authentication and encryption protocols.

Keyed-Hash Message Authentication Code (HMAC)

11.6.28. HMAC is a protocol where both an RFID reader and RFID tag share a common secret key that can be used in combination with a hash algorithm to provide one-way or mutual authentication between tag and reader. When HMAC is applied to messages, it also assures the integrity of data in the messages.

11.6.29. HMAC is not specified in any RFID standard, but the capability is generally available in vendor products. HMAC is often used where the risk of eavesdropping is high and passwords alone are considered to offer an inadequate authentication mechanism. This will be determined by the risk assessment. HMAC is also used where applications require evidence of a tag's authenticity.

Digital Signatures

11.6.30. Digital signatures are compatible with existing RFID tag standards. In authenticated RFID systems, tags can receive, store, and transmit digital signatures with existing read and write commands because the complexity is managed by readers or back-end systems. However, the use of digital signatures to support authentication of readers to tags would require tags to support relatively complex cryptographic functions, beyond the capacity of common tag designs.

11.6.31. In addition, digital signatures that are not generated by the tag itself are subject to replay attacks. An adversary could query a tag to obtain its evidence of authenticity (i.e., the digital signature created by a previous reader) and then replicate that data on a cloned tag. Consequently, password or symmetric key authentication systems likely will support tag access control, as opposed to tag authenticity verification, for the immediate future.

Encryption

11.6.32. Data stored in the memory of an RFID tag is intended to be freely shared with the various tag users (manufacturers, stock controllers, shipping agents, etc.). Only an RFID reader is required to access the data which raises the question of data security. Memory and computational power of an RFID tag is limited, but data elements can be password-protected or reserved for nominated usage. Several levels of authorisation (read-only, read and write, delete, etc.) can be determined. It is also advisable to encrypt the data entered onto the tag, the encryption/decryption taking place at the RFID reader or back-end system.

Cover-Coding

11.6.33. Cover-coding is a method of hiding information from eavesdroppers. In the EPCglobal Class-1 Generation-2 standard, cover-coding is used to obscure passwords and information written to a tag using the write command. Some proprietary technologies also support similar features. Cover-coding is an example of minimalist cryptography because it operates within the challenging power and memory constraints of passive RFID tags.

11.6.34. Cover-coding is a useful mitigation where eavesdropping is a risk, but adversaries are expected to be at a greater distance from the tags than readers. Cover-coding helps prevent the execution of unauthorised commands that could disable a tag or modify the tag's data. Cover-coding mitigates business process, business intelligence, and privacy risks.

Rolling Code

11.6.35. A rolling code approach is a scheme where the identifier given by the RFID tag changes after each read action. It requires the RFID reader and RFID tag to use identical algorithms. If multiple readers are used, they must be linked so that tracking of code changes can be monitored. This scheme reduces the usefulness of any responses that may be observed unless the pattern of change can be detected or deduced.

Other Defensive Measures

11.6.36. Other defensive measures, sometimes described as palliative techniques, include shielding, blocker tags, tag "kill" commands, tamper resistance and temporary deactivation. It is important to note these techniques do not use encryption.

Shielding

11.6.37. RF shielding is designed to limit the propagation of RF signals outside of the shielded area. Shielding helps to prevent unauthorised reading, access to or modification of the RFID tag data or interfering with RFID readers. Shielding can be applied to small, individual items, such as passports and credit cards or to large elements such as shipping containers.

11.6.38. Shielding is also important where interference is present or detected. This may be caused by environmental conditions, such as operating in a port area, or by deliberate attempts to access readers or tags.

11.6.39. Engineering assessments will determine the requirement for shielding from adverse environmental conditions and the risk assessment will determine the likelihood and threat from unauthorised and deliberate attempts to access readers, tags and data.

11.6.40. RFID blocking wallets and **RFID card sleeves** are available to block RFID frequencies. These are typically used for credit and other payment, access and transit cards and e-passports, as a countermeasure for skimming attacks or unauthorised tracking.

Blocker Tags

11.6.41. A special tag, called a "blocker" tag, blocks an RFID reader by simultaneously answering with 0 and 1 to every reader's request during the identification protocol. The reader is then incapable of distinguishing individual tags. The blocker tag may block a reader universally or within ranges.

11.6.42. This furnishes privacy by shielding consumers from the unwanted scanning of RFID tags that they may carry or wear. It also protects against unauthorised readers and eavesdroppers. The blocker tag is an alternative to more simple solutions such as the kill command, shielding and active jamming. It is important to note that active jamming may be illegal (see 11.6.53).

11.6.43. Blocker tags can also implement one or more privacy policies and multiple blocker tags may cover multiple zones. The blocker tag has a very low-cost of implementation and standard tags need no modification and little support for password-protected bit flipping. A threat is that blocker tags can be used to mount DoS attacks in which a malicious blocker tag universally blocks readers.

Tag "Kill" Command

11.6.44. The "kill" command is a password-protected command specified in the EPC Gen-1 and EPC Gen-2 standards intended to make a tag non-operational. A typical application is anti-theft where the kill command is activated at a point-of-sale terminal, after goods have been paid for. Kill commands can be password protected.

11.6.45. Kill commands function by fusing a ROM component or antenna connection by applying a large amount of power to the tag at the point of sale reader/terminal. It is important to note that the antenna deactivation method does not completely kill the tag but rather disable its RF interface. Once in the disabled state, the tag still retains data and can still function.

11.6.46. The kill feature can represent a threat to an RFID system if the password is compromised. This risk is particularly apparent where the same password is used for multiple tags. If a weak (e.g., short or easily guessed) password is assigned to the kill command, tags can be disabled at will. Also important is the longer a tag uses the same password, the more likely it is that the password will be compromised.

11.6.47. Data stored on the tag is still present in the tag's memory after it is disabled (although it can no longer be accessed wirelessly), and, therefore, still may be accessible with physical access to the tag.

Tamper Resistance

11.6.48. Some RFID tags are designed with tamper resistant or tamper-evident features to help prevent unauthorised alteration of removal of tags from the objects to which they are attached. A simple type of tamper resistance is the use of a frangible, or easily broken, antenna. If this tag is removed, the connection with the antenna is severed, rendering the tag inoperable. Other, more complex types of RFID systems monitor the integrity of objects associated with the tags to ensure that the objects have not been compromised, altered, or subjected to extreme conditions.

11.6.49. Simple forms of tamper resistance may leave data intact and subject to the same threats described above. In addition it is possible to circumvent tamper resistance mechanisms by repairing a frangible antenna. It is important to note that tamper-resistance and tamper-evidence technologies do not prevent the theft or destruction of the tag or its associated items.

Temporary Deactivation

11.6.50. Some tags allow the RF interface to be temporarily deactivated. Methods vary amongst manufacturers with some methods requiring physical intervention. Typically tags would be activated inside a designated area and deactivated when shipped, preventing eavesdropping or other unauthorised transactions during shipment. When the tags arrive at their destination, they can be reactivated, for example for inventory management. Conversely, tags can be used for tracking during shipment and may be deactivated on delivery.

RFID Risks and Controls Summary

11.6.51. A summary of RFID Risks and Controls is presented in the Table below:

Risk Control	Business Process	Business Intelligence	Privacy	Electro-Magnetic Radiation	Back-End System Attack
Tag Access Controls	●	●	●		●
Password Authentication	●	●	●		●
HMAC	●	●	●		●
Digital Signature	●	●			●
Cover-Coding		●			●
Encryption – Data in Transit		●	●		
Encryption – Data at Rest		●			●
Encryption – Data on Tag	●	●	●		
Shielding	●	●	●	●	
Blocker Tags		●	●		
Tag Kill Feature		●	●		
Tamper Resistance	●	●			

Temporary Deactivation	●	●	●		
RF Engineering and Frequency Selection	●	●	●	●	

Relevant Legislation

11.6.52. In New Zealand, operation of radio and other equipment in the RF spectrum is controlled Radiocommunications Act 1989, Reprint as at 5 December 2013 and administered by the Ministry of Business Innovation and Employment.

RF Jammers

11.6.53. It is illegal to import, manufacture, sell or use a radio jammer in New Zealand except with a licence issued by the Radio Spectrum Management unit of the Ministry of Business, Innovation and Employment. The use and management of RF jammers is governed by the Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011 under the Regulation 32(1)(i) [a notice in the Gazette] of the Radiocommunications Regulations 2001.

Secure Spaces

11.6.54. The use of RFID technology in secure areas must be carefully considered, recognising that an RFID tag or system incorporates antennae and transmitting capabilities which may compromise the security of such areas. Passive tags (classes 0 and 1) pose little risk in themselves as they require a reader to activate and have little on-board capability. Read/write tags (class 2) pose a higher risk as they have the capability to store data. Other tags (classes 3 to 5) can pose a significant risk to secure spaces.

PSR references

11.6.55. The relevant PSR Mandatory Requirements are:

References	Title	Source
PSR Mandatory Requirements	GOV2, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Security zones	https://www.protectivesecurity.govt.nz/security-zones/
Managing specific scenarios	Secure your ICT facilities Mobile and remote working Physical Security for ICT systems Communication security	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/communications-security/

References - Guidance

11.6.56. Further references on Guidance can be found at:

References	Publisher	Source
Special Publication 800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems	NIST	http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf
FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008	NIST	http://csrc.nist.gov/publications/PubsFIPS.html#198-1
FIPS PUB 180-4 Secure Hash Standard (SHS)	NIST	http://csrc.nist.gov/publications/PubsFIPS.html#180-4
Implementation Guide for the use of GS1 EPCglobal Standards in the Consumer Electronics Supply Chain	GS1/EPCglobal	http://www.gs1.org/epc-rfid
Smart Border Alliance RFID Feasibility Study Final Report Attachment D – RFID Technology Overview	US Department of Homeland Security	https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachD.pdf

Smart Border Alliance RFID Feasibility Study Final Report Attachment E – RFID Security And Privacy White Paper	US Department of Homeland Security	https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf
Test Operations Procedure (TOP) 03-2-616A Electromagnetic Radiation Hazards Testing For Non-Ionizing Radio Frequency Transmitting Equipment	US Defense Technical Information Center (DTIC),	http://www.dtic.mil/dtic/tr/fulltext/u2/a577863.pdf
Electromagnetic Environmental Effects Requirements for Systems – MIL-STD-46C	US Department of Defense Interface Standard	http://everyspec.com/MIL-STD/MIL-STD-0300-0499/MIL-STD-464C_28312/
RFID Tags – Privacy Threats and Countermeasures	European Commission	https://ec.europa.eu/jrc/sites/default/files/jrc78156_report_rfid_en.pdf
OECD Policy Guidance – A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives.	OECD Directorate for Science, Technology and Industry	http://www.oecd.org/sti/ieconomy/40892347.pdf
Technical Guideline TR-03126-5 Technical Guidelines for the Secure Use of RFID (TG RFID) Subdocument 5: Application area "Electronic Employee ID Card" Version 1.0	BSI – The German Federal Office for Information Security	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_03126_5_Application_area_Electronic_Employee_ID_Card.pdf?__blob=publicationFile
Establishing Security Best Practices in Access Control	Rohr *et al*	http://www.git-security.com/file/track/5743/1

References - Standards

11.6.57. Further references on standards can be found at:

References	Publisher	Source
EPC Tag Data Standard Version 1.9, Ratified, Nov-2014	GS1/EPCglobal	http://www.gs1.org/epcrfid-epcis-id-keys/epc-rfid-tds/1-9
EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 2.0.1	GS1/EPCglobal	http://www.icao.int/Security/mrtd/pages/Document9303.aspx
ICAO Doc 9303, Machine Readable Travel Documents Parts 1-12	International Civil Aviation Organization (ICAO)	http://www.iso.org
ISO/IEC 7816-1:2011 - Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics	ISO	http://www.iso.org
ISO/IEC 7816-2:2007 - Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts	ISO	http://www.iso.org
ISO/IEC 7816-3:2006 Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols	ISO	http://www.iso.org
ISO/IEC 7816-4:2013 - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange	ISO	http://www.iso.org
ISO/IEC 7816-5:2004 - Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers	ISO	http://www.iso.org
ISO/IEC 7816-6:2004 - Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange	ISO	http://www.iso.org
ISO/IEC 7816-7:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)	ISO	http://www.iso.org

ISO/IEC 7816-8:2004 Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations	ISO	http://www.iso.org
ISO/IEC 7816-9:2004 - Identification cards -- Integrated circuit cards -- Part 9: Commands for card management	ISO	http://www.iso.org
ISO/IEC 7816-10:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards	ISO	http://www.iso.org
ISO/IEC 7816-11:2004 - Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	ISO	http://www.iso.org
ISO/IEC 7816-12:2005 - Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures	ISO	http://www.iso.org
ISO/IEC 7816-13:2007 - Identification cards -- Integrated circuit cards -- Part 13: Commands for application management in a multi-application environment	ISO	http://www.iso.org
ISO/IEC 7816-15:2004 - Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application	ISO	http://www.iso.org
ISO 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics	ISO	http://www.iso.org
ISO/IEC 14443-2:2010 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface	ISO	http://www.iso.org
ISO/IEC 14443-3:2011 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision	ISO	http://www.iso.org
ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol	ISO	http://www.iso.org
ISO/IEC 15961-1:2013 Information technology -- Radio frequency identification (RFID) for item management: Data protocol -- Part 1: Application interface	ISO	http://www.iso.org
ISO/IEC 15963:2009 Information technology – Radio frequency identification for item management – Unique identification for RF tags	ISO	http://www.iso.org
ISO/IEC 18000-1:2008 Information technology -- Radio frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized	ISO	http://www.iso.org
ISO/IEC 18000-2:2009 Information technology -- Radio frequency identification for item management -- Part 2: Parameters for air interface communications below 135 kHz	ISO	http://www.iso.org
ISO/IEC 18000-3:2010 Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz	ISO	http://www.iso.org
ISO/IEC 18000-4:2015 Information technology -- Radio frequency identification for item management -- Part 4: Parameters for air interface communications at 2,45 GHz	ISO	http://www.iso.org

ISO/IEC 18000-6:2013 Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General	ISO	http://www.iso.org
ISO/IEC 18000-7:2014 Information technology -- Radio frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz	ISO	http://www.iso.org
ISO/IEC 18000-61:2012 Information technology -- Radio frequency identification for item management -- Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A	ISO	http://www.iso.org
ISO/IEC 18000-62:2012 Information technology -- Radio frequency identification for item management -- Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B	ISO	http://www.iso.org
ISO/IEC 18000-63:2015 Information technology -- Radio frequency identification for item management -- Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C	ISO	http://www.iso.org
ISO/IEC 18000-64:2012 Information technology -- Radio frequency identification for item management -- Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D	ISO	http://www.iso.org
ISO/IEC TR 18047-4:2004 Information technology -- Radio frequency identification device conformance test methods -- Part 4: Test methods for air interface communications at 2,45 GHz	ISO	http://www.iso.org
ISO/IEC TR 18047-7:2010 Information technology -- Radio frequency identification device conformance test methods -- Part 7: Test methods for active air interface communications at 433 MHz	ISO	http://www.iso.org
ISO/IEC TR 24710:2005 Information technology -- Radio frequency identification for item management -- Elementary tag licence plate functionality for ISO/IEC 18000 air interface definitions	ISO	http://www.iso.org
ISO/IEC TR 24729-1:2008 Information technology -- Radio frequency identification for item management -- Implementation guidelines -- Part 1: RFID-enabled labels and packaging supporting ISO/IEC 18000-6C	ISO	http://www.iso.org
ISO/IEC 24753:2011 Information technology -- Radio frequency identification (RFID) for item management -- Application protocol: encoding and processing rules for sensors and batteries	ISO	http://www.iso.org
ISO/IEC 24791-2:2011 Information technology -- Radio frequency identification (RFID) for item management -- Software system infrastructure -- Part 2: Data management	ISO	http://www.iso.org
ISO/IEC TR 20017:2011 Information technology -- Radio frequency identification for item management -- Electromagnetic interference impact of ISO/IEC 18000 interrogator emitters on implantable pacemakers and implantable cardioverter defibrillators	ISO	http://www.iso.org

ISO/IEC TR 29123:2007 Identification Cards – Proximity Cards – Requirements for the enhancement of interoperability	ISO	http://www.iso.org

Legislation and Regulation

11.6.58. Further references onLegislation and Regulation can be found at:

References	Publisher	Source
Radiocommunications Act 1989	Parliamentary Counsel Office	http://www.legislation.govt.nz
Radiocommunications Regulations 2001, Reprint as at 1 February 2015 (SR 2001/240)	Parliamentary Counsel Office	http://www.legislation.govt.nz
Radiocommunications Regulations (Prohibited Equipment - Radio Jammer Equipment) Notice 2011	New Zealand Gazette Office, Government Information Services, Department of Internal Affairs	https://gazette.govt.nz/notice/id/2011-go4051
Radio Spectrum Management	Ministry of Business, Innovation and Employment	http://www.rsm.govt.nz/

Rationale & Controls

11.6.59. Risk Assessment

11.6.59.R.01. Rationale

As with many technologies, adoption of RFID has the potential to introduce a wide range of risks in addition to the risks that already exist for agency systems. This may include privacy risks, depending on the use, information held and implementation of the RFID system. A risk assessment is an essential tool in determining and assessing the range and extent of risk and threat in the use of RFID devices.

11.6.59.R.02. Rationale

Risks to RFID system vary according to the technology used, system engineering, the systems architecture, application, context and deployment scenario. A holistic approach to risk at each stage of the system life cycle and each for system component is essential if a robust security strategy is to be developed.

11.6.59.R.03. Rationale

The identification of classes of tags is fundamental to managing the risks of RFID devices in secure spaces. Classes 0 and 1 pose little risk. Other classes of tag (2 to 5), however, have limited data storage capability and active tags include transmitter functionality which introduces higher levels of risk. RFID readers are, by definition, transmitters and are not permitted in secure spaces.

11.6.59.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2956]

Agencies MUST conduct and document a risk assessment *before* implementing or adopting an RFID solution.

11.6.59.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:2957]

This risk assessment MUST be the basis of a security architecture design.

11.6.60. Security Architecture

11.6.60.R.01. Rationale

The foundation of strong security architecture in RFID follows three important principles:

- **Controlled access to the data** – only authorised entities (people, systems, devices) can read and write information to and from the RFID tags (EPC number, tag identifier, kill password, access password and user memory) and RFID databases;
- **Control over access to the system** – only authorised entities can configure or add devices to the system, and all devices on the system are authentic and trustworthy;
- **Confidence and trust** – back-end systems are designed and implemented in accordance with the current version of the NZISM.

11.6.60.R.02. Rationale

Sensitive data should be held in a secure RFID Enterprise Subsystem and retrieved using the tag's unique identifier with only an identifier stored on the tag itself. The Enterprise RFID subsystem should be established as a separate domain where data can be more adequately protected. This structure makes it more difficult for adversaries to obtain information from the tag through scanning or eavesdropping. Data encryption and access control is often more cost-effectively performed in the enterprise subsystem than in the RF subsystem.

11.6.60.R.03. Rationale

Some RFID systems may cover several organisations, for example in supply chains. In such cases, multiple organisations may require access to databases that contain tag identifiers and passwords. The security architecture should incorporate strong security controls including the authentication of external entities, incident management, audit logging and other essential security controls.

11.6.60.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2962]

Agencies MUST develop a strong security architecture to protect RFID databases and RFID systems.

11.6.60.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:2963]

Agencies MUST minimise the information stored on RFID tags and in the RFID subsystem.

11.6.60.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2964]

Agencies SHOULD disable any rewrite functions on RFID devices.

11.6.60.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2965]

Agencies SHOULD apply the access control requirements of the NZISM (Chapter 11 - Communications Systems and Devices) to RFID systems.

11.6.61. Policy

11.6.61.R.01. Rationale

An RFID Usage Policy is an essential component of an agency's privacy policy, addressing topics such as how personal information is stored and shared. The RFID usage policy should also address privacy issues associated with the tag identifier formats and the potential disclosure of information based solely on the tag identifier format selected. Agencies MAY be required to ensure that devices that collect and store data comply with relevant regulation and guidance, such as the Privacy Act and the HIPAA. Refer also to Chapter 20 – Data Management.

11.6.61.R.02. Rationale

Any RFID implementation should also be incorporated into the agency's security policies. Refer also to Chapter 5 – Information Security Documentation.

11.6.61.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2969]

Agencies SHOULD develop, implement and maintain an RFID Usage Policy.

11.6.61.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2970]

Agencies SHOULD incorporate RFID into the agency's security policies and information security documentation.

11.6.62. Inspections

11.6.62.R.01. Rationale

Many system component manufacturers use RFID tags to track shipments. RFID tags may be embedded in the packaging, printed on the reverse of labels, attached to or embedded in the device itself. The ability to identify and track devices may pose a security concern for secure areas or equipment deployed in high security applications.

11.6.62.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2973]

Agencies MUST conduct visual and technical inspections of packaging and devices to determine if RFID devices have been attached and either permanently disable or remove such devices.

11.6.62.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2974]

Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices have been attached and if these RFID devices pose a security concern.

11.6.62.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2975]

Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices or labelling have been tampered with and whether this is a security concern.

11.6.63. Shielding

11.6.63.R.01. Rationale

RF shielding is designed to limit the propagation of RF signals outside of the shielded area. Shielding helps to prevent unauthorised reading, access to or modification of the RFID tag data or interfering with RFID readers. Shielding can be applied to small, individual items, such as passports and credit cards or to large elements such as shipping containers. The requirement for shielding is determined by the risk assessment and an engineering assessment.

11.6.63.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2978]

Agencies SHOULD consider undertaking an RF engineering assessment where security concerns exist or where the RFID systems are to be used in areas with high levels of RF activity.

11.6.63.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2979]

Shielding SHOULD be considered where eavesdropping or RF radiation is a concern, as determined by the risk assessment.

11.6.64. Positioning of Tags and Readers

11.6.64.R.01. Rationale

In order to minimise unnecessary electromagnetic radiation tags and readers should be carefully positioned. Care should be taken in use of RFID readers in proximity to:

- Fuel, ordnance, and other hazardous materials,
- Humans and sensitive products (e.g., blood, medicine) that may be harmed by sustained exposure to RF radiation,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radio and Wi-Fi systems to avoid interference.

11.6.64.R.02. Rationale

Tag location cannot always be controlled, such as when tags are used to track mobile items or goods in transit. Other difficulties occur with persistent radio interference. In these situations, relocation of readers and tags may provide a solution. Consideration should be given to alternative but cost-effective RF protection measures, such as grounded wire fencing. The engineering assessment undertaken to determine the shielding requirements will assist in determining such measures.

11.6.64.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2983]

Agencies SHOULD consider placement of tags and location of readers to avoid unnecessary electromagnetic radiation.

11.6.65. Encoding and Encryption

11.6.65.R.01. Rationale

If an adversary reads an identifier that is encoded with a published format, such as in the EPC standard, an adversary may be able to obtain useful information such as the manufacturer or issuer of the item, as well as the type of item. Because RFID tags hold limited information and identifier formats are published in standards, it may be important to use identifier formats that do not reveal any information about tagged items or the agency using the RFID system. This will be determined in the risk assessment. Encoding schemes to limit information revealed from unauthorised scanning may include serially or randomly assigning identifiers.

11.6.65.R.02. Rationale

Adversaries can often obtain valuable information from the identifier alone. For example, knowledge of the EPC manager ID and object class bits may reveal the make and model of tagged objects in a container. If individual items or boxes of items are tagged, the quantities may also be discernible. An adversary might target containers based on their contents.

11.6.65.R.03. Rationale

The smallest tags generally used for consumer items, such as clothing, do not have enough computing power to support data encryption. At best these tags can cater for PIN-style or password-based protection. Data can, however, be encrypted before it is stored on a tag. In these designs, encryption is undertaken by the RFID subsystem or the RFID reader. This is an effective means of protecting the data on a tag. Refer also to Chapter 17 – Cryptography.

11.6.65.R.04. Rationale

The current Gen 2 standard provides for an on-chip 16-bit Pseudo-Random Number Generator (RNG) and a 16-bit Cyclic Redundancy Code (CRC-16) to protect tag/reader channels. Neither of these encryption methods is strong because of the short bit length in the RNG and because CRCs are not suitable for protection against malicious alteration of data.

11.6.65.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:2989]

Agencies MUST follow the requirements of the NZISM in the selection and implementation of cryptographic protocols and algorithms, and in key management, detailed in Chapter 17 - Cryptography.

11.6.65.C.02. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2990]

Agencies SHOULD encrypt data before it is written to RFID tags.

11.6.65.C.03. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2991]

Agencies SHOULD assign RFID identifiers using formats that limit information about tagged items or about the agency operating the RFID system.

11.6.66. Authentication

11.6.66.R.01. Rationale

Both an RFID reader and RFID tag share a common secret key that can be used in combination with a hash algorithm to provide one-way or mutual authentication between tag and reader. This is known as a **Keyed-Hash Message Authentication Code (HMAC)**. When HMAC is applied to messages, it also assures the integrity of data in the messages. HMAC is not specified in any RFID standard, but the capability is generally available in vendor products. HMAC is often used where the risk of eavesdropping is high and passwords alone are considered to offer an inadequate authentication mechanism. This will be determined by the risk assessment. HMAC is also used where applications require evidence of a tag's authenticity.

11.6.66.C.01. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2994]

Agencies SHOULD consider the use of HMAC when tag authenticity is required.

11.6.67. Password Management

11.6.67.R.01. Rationale

RFID tags generally require passwords before execution of commands such as reading and writing of tag data, memory access control, and the tag kill feature. Passwords are an important control in maintaining the security and integrity of the RFID system. Refer also to Chapter 16 – Access Control.

11.6.67.R.02. Rationale

Tags should not share passwords, although this may not be practical in all cases. In applications such as supply chains, multiple organisations may require access to databases that contain tag identifiers and passwords. In such cases external entities must be authenticated and incident management, audit logging and other security controls are essential. While in traditional IT systems, passwords are often changed on a periodic basis, in RFID systems, such changes may be impractical, especially if the tags are not always accessible to the agency assigning the passwords.

11.6.67.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:2998]

Agencies MUST assign passwords for critical RFID functions.

11.6.67.C.02. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2999]

Agencies SHOULD follow the guidance for passwords management in the NZISM (Chapter 16 – Access Control).

11.6.68. Temporary Deactivation of Tags

11.6.68.R.01. Rationale

The RF interface on some tags can be temporarily deactivated. In a supply chain application, for example, tags may be turned off to prevent unauthorised access to the tags during shipment. This feature is useful when communication between readers and a tag is infrequent allowing

the tag to be activated when required but limiting vulnerability to rogue transactions if left operational for extended periods with no authorised activity. Temporary deactivation can also extend battery life in powered tags.

11.6.68.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3002]

Agencies SHOULD consider temporary deactivation of RFID tags where the tag is likely to be inactive for extended periods.

11.6.69. Incident Management

11.6.69.R.01. Rationale

Incident management and audit procedures, logging and time stamps help detect and manage security breaches. These are important tools in protecting systems and managing security breaches.

11.6.69.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3006]

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 – Information Security Documentation, Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

11.6.70. Disposal

11.6.70.R.01. Rationale

Tag disposal and recycling procedures that permanently disable or destroy sensitive data reduces the possibility that they could be used later for tracking or targeting, and prevents access to sensitive data stored on tags. In addition the continued operating presence of a tag after it has performed its intended function can pose a business intelligence or privacy risk, including tracking, targeting or access to sensitive data on the tag.

11.6.70.R.02. Rationale

Disposal may be undertaken electronically by using a tag's "kill" feature or using a strong electromagnetic field to permanently deactivate a tag's circuitry. Alternatively physical destruction can be achieved by tearing or shredding. Where a tag supports an electronic deactivation mechanism, tags should be electronically deactivated before physical destruction.

11.6.70.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3010]

Agencies SHOULD consider secure disposal procedures and incorporate these into the RFID Usage Policy. Refer also to Chapter 13 – Decommissioning and Disposal.

11.6.71. Operator Training and User Awareness

11.6.71.R.01. Rationale

Operator training can help ensure that personnel using the RFID system have the necessary skills and knowledge follow appropriate guidelines and policies. If HERF/HERO/HERP risks are present, appropriate security training covers mitigation techniques, such as safe handling distances.

11.6.71.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3047]

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of RFID services (See Section 9.1 – Information Security Awareness and Training).

11.6.72. Secure Spaces

11.6.72.R.01. Rationale

The identification of classes of tags is fundamental to managing the risks of RFID devices in secure spaces. Classes 0 and 1 pose little risk. Other classes of tag (2 to 5), however, have limited data storage capability and active tags include transmitter functionality which introduces higher levels of risk. RFID readers are, by definition, transmitters and are not permitted in secure spaces. Some exceptions may be permitted for testing, and inspection and monitoring purposes. Any such exceptions must be carefully controlled and monitored.

11.6.72.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:3052]

Any RFID tags of class 3, 4, or 5 MUST NOT be permitted in secure spaces.

11.6.72.C.02. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:3054]

RFID readers MUST NOT be permitted in secure spaces.

11.6.72.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3055]

Class 2 RFID tags SHOULD NOT be permitted in secure spaces.

Abbreviations

11.6.73.

Term	Meaning
EMV	Europay, MasterCard, and Visa technical standard
EPC	Electronic Product Code
HERF	Hazards of Electromagnetic Radiation to Fuel
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to Personnel

HMAC	Keyed-Hash Message Authentication Code
RFID	Radio Frequency Identification
SAM	Secure Access Module/ Secure Application Module

Terms

11.6.74.

Term	Meaning
EMV	Europay, MasterCard, and Visa technical standard for payment cards, payment terminals and automated teller machines (ATMs)
EPC	An Electronic Product Code (EPC) is a universal identifier that gives a unique identity to a specific physical object. In most instances, EPCs are encoded on RFID tags attached to the object and used for stock tracking and management purposes. Many types of assets can be tagged including fixed assets, documents, transport containers and clothing items.
Radio Frequency Identification (RFID)	RFID is technology utilising electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, item, animal, or person. RFID is increasingly used as replacement for bar codes. An RFID system consists of three components: an antenna, transceiver (usually the RFID reader) and a transponder (also known as a tag).
Secure Access Module	A **Secure Access Module** (or Secure Application Module) is used to enhance the security and cryptographic performance of devices. SAMs are commonly found in devices needing to perform secure transactions, such as payment terminals. It can be used for cryptographic computation and secure authentication against smart cards or contactless EMV cards. Physically a SAM card can either be a separate component and plugged into a device when required or incorporated into an integrated circuit.
Tag	The transponder in an RFID system, frequently found attached to an item or object to provide electronic identification.

11.7. Card Access Control Systems

Objective

11.7.1. To ensure Access Control Systems incorporating contactless RFID or smart cards are used safely and securely in order to protect privacy, prevent unauthorised access and to prevent the compromise of secure spaces.

Context

Scope

11.7.2. This section provides information relating to the risks, security and secure use of RFID or smart cards in access control systems. This section does not discuss biometric access control systems.

11.7.3. The previous section (11.6. Radio Frequency Identification Devices) provides background information and technical detail of the RFID aspects and should be read in conjunction with this section.

Background

11.7.4. Contactless access control systems based on RFID (Radio Frequency Identification) has largely replaced earlier technologies such as magnetic swipe cards in almost all security-critical applications. Two generations of RFID access cards exist:

- an earlier generation of cards, which use only basic proprietary security mechanisms; and
- a more recent generation that incorporates advances in CMOS and smart card technology to implement cryptography and other protective measures.

11.7.5. Older access control systems often incorporated a magnetic strip and were easily cloned. More recent systems support the use of PINs in addition to RFID. Unfortunately PINs are also sometimes stored on the cards, often unencrypted and unprotected, and thus facilitating attacks on both the card and the PIN.

11.7.6. Access control systems typically comprise four components:

- A reader that programmes the access cards for particular employees and their permitted access to parts of the site, building to secure areas.
- A transceiver at each control point to communicate with cards.
- A controller to control the locks of access points (doors).
- The backend system that hosts all permissions and authorised data and interfaces with the reader, transceiver and controllers.

11.7.7. Traditionally access control systems were hosted by stand-alone equipment. Modern access control system may be hosted on standard computer equipment and hosted in the organisation's datacentre. It is possible that a system intrusion can target access control systems, making the switches, gates and locks remotely accessible.

11.7.8. Low frequency RFID badge systems use 125KHz, (ISO 11784/5 and ISO 14223). Newer high frequency RFID cards use 13.56MHz (ISO 15693, ISO 14443

and ISO 18000-3).

11.7.9. Some cards also operate at UHF frequencies of 850-960Mhz (ISO 18000-6). Some cards are designed to operate at low and high frequencies by embedding multiple antennae in the cards.

11.7.10. The ISO/IEC 14443 standard for contactless smart card communications defines two types of contactless cards ("A" and "B") and allows for communications at distances up to 10 cm operating at 13.56 MHz.

11.7.11. The alternative ISO/IEC 15693 standard allows communications at distances up to 50 cm. The ISO/IEC 7816 standard (in 15 parts) defines the physical, electrical interface and operating characteristics of these cards.

11.7.12. UHF cards follow the   EPC Global Gen2 standard and the ISO 18000-6 standards and are designed to operate at distances of up to 10 metres.

Smart Cards

11.7.13. Smart cards typically incorporate an embedded integrated circuit typically incorporating a microchip with internal memory, a read-only CSN (Card Serial Number) or a UID (User Identification). The card connects to a reader with direct physical contact or a contactless radio frequency (RFID) interface. With an embedded microchip, smart cards can store large amounts of data, carry out on-card functions (such as encryption and authentication) and interact intelligently with a smart card reader. Smart card technology can be found in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in mobile phones, and USB-based tokens. Smart cards are widely used in payment card (debit and credit cards and electronic wallets) and access control systems.

11.7.14. In common with other RFID devices, smart cards incorporate an antenna embedded in the body of the card (or key fob, watch or token). When the card is brought within range of the reader, the chip in the card is powered on. Once powered on, an RF communication protocol is initiated and communication established between the card and the reader for data transfer.

11.7.15. Smart cards typically incorporate protective mechanisms including authentication, secure data storage, encryption, tamper-resistance and secure communication. Support for biometric authentication may also be incorporated.

Near Field Communication (NFC)

11.7.16. NFC is an RFID technology that enables two electronic devices to establish communication by bringing them within 4 cm of each other. As with other "proximity" technologies, NFC employs electromagnetic induction between two loop antennae when NFC devices exchange information. NFC operates in the globally available unlicensed radio frequency band of 13.56 MHz conforming to the ISO/IEC 18000-3 standard. In access control applications these devices are sometimes known as "prox cards".

Attacks

11.7.17. In addition to attacks on RFID components described in the previous section, access control cards can be susceptible to relay and chip hacking attacks.

11.7.18. Relay attacks rely on rogue readers to activate the tag even when not in proximity to a legitimate reader. The card holder will be unaware that such an attack is underway. An effective defence is to incorporate distance-to-reader verification although few RFID systems incorporate this mechanism.

11.7.19. Signals between cards and a legitimate reader can be intercepted at distances of up to a metre. Greater distances are possible with higher powered equipment, special antennae and in low interference environments. The signals and data, including card credentials, are captured off-line and used to clone access cards. Again the card holder will be unaware that such an attack is underway.

11.7.20. Chip hacking is facilitated by physical access to the card but can be mitigated by second factor authentication, encryption of data on the card and card tamper detection.

11.7.21. Threats, vulnerabilities and mitigations of RFID access control systems are summarised in the table below:

Threat/Vulnerability	Mitigation
Interception of the RFID signals	Encryption of RF links Harden RFID elements
Implants	Physical security CCTV Tamper resistant readers
Cryptographic attacks	Use of approved cryptographic algorithms and protocols Strong key management Incident detection and management Use of evaluated products
Replay Authentications	Robust Random Number Generation on readers
Key extraction reader attacks through side channel analysis or fault injection	Use of evaluated products with SAM chips Incident detection and management
Attack on authentication keys on the card	Key diversification Strong key management Incident detection and management
Chip Hacking	Use of approved cryptographic algorithms and protocols on the card Tamper protection Incident detection and management
Malware	Update and patching for all system components Incident detection and management

Backend systems	System hardening
	Update and patching for all system components
	Intrusion detection
	Incident detection and management

Product Selection

11.7.22. A number of protection profiles related to smartcards and related devices and systems are provided on the Common Criteria website. Refer also to Chapter 12 – Product Security.

Secure Access Module

11.7.23. A Secure Access Module (or Secure Application Module - SAM) is used to enhance the security and cryptographic performance of devices. SAMs are commonly found in devices needing to perform secure transactions, such as payment terminals. It can be used for cryptographic computation and secure authentication against smart cards or contactless payment cards.

11.7.24. Physically a SAM card can either be a separate component and plugged into a device when required or incorporated into an integrated circuit. A typically use is for the secure storage of cryptographic keys or other sensitive data. SAM hardware and software are designed to prevent information leakage and incorporates countermeasures against electromagnetic radiation, timing measurements, and other side channel attacks. These properties mean that SAMs offer a much higher level of protection than the terminals and readers, which often utilise general-purpose computers.

11.7.25. SAM's typically support 3DES and AES cryptographic algorithms and SHA hashing algorithms in their hardware cryptographic co-processor implementations. Refer to Chapter 17 for information on approved cryptographic algorithms and protocols. It is important to note that 3DES is approved for use on legacy systems only and SHA-1 is not an approved hashing algorithm.

Card Protection

11.7.26. RFID blocking wallets and RFID card sleeves are available to block RFID frequencies. These are typically used for the protection of credit and other payment, access, transit cards and e-passports as a countermeasure for skimming attacks.

References - Guidance

11.7.27. Further references on Guidance can be found at:

References	Publisher	Source
Establishing Security Best Practices in Access Control	Rohr, Nohl and Plotz	http://www.git-security.com/file/track/5743/1
Common Criteria Protection Profiles	Common Criteria	https://www.commoncriteriaportal.org/pps/
Defending Risky Electronic Access Points into a "Closed" Industrial Control System (ICS) Network Perimeter	NSA	https://www.nsa.gov/ia/_files/security_configuration/Defending_Risky_Electronic_Access_Points.pdf

References - Standards

11.7.28. Further references on standards can be found at:

References	Publisher	Source
ISO/IEC 7816-1:2011 - Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics	ISO	http://www.iso.org/
ISO/IEC 7816-2:2007 - Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts	ISO	http://www.iso.org/
ISO/IEC 7816-3:2006 Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols	ISO	http://www.iso.org/
ISO/IEC 7816-4:2013 - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange	ISO	http://www.iso.org/
ISO/IEC 7816-5:2004 - Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers	ISO	http://www.iso.org/
ISO/IEC 7816-6:2004 - Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange	ISO	http://www.iso.org/

ISO/IEC 7816-7:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)	ISO	http://www.iso.org/
ISO/IEC 7816-8:2004 Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations	ISO	http://www.iso.org/
ISO/IEC 7816-9:2004 - Identification cards -- Integrated circuit cards -- Part 9: Commands for card management	ISO	http://www.iso.org/
ISO/IEC 7816-10:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards	ISO	http://www.iso.org/
ISO/IEC 7816-11:2004 - Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	ISO	http://www.iso.org/
ISO/IEC 7816-12:2005 - Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures	ISO	http://www.iso.org/
ISO/IEC 7816-13:2007 - Identification cards -- Integrated circuit cards -- Part 13: Commands for application management in a multi-application environment	ISO	http://www.iso.org/
ISO/IEC 7816-15:2004 - Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application	ISO	http://www.iso.org/
ISO/IEC 10373-7:2008 - Identification cards -- Test methods -- Part 7: Vicinity cards	ISO	http://www.iso.org/
ISO 11784:1996 Amd 2:2010- Radio frequency identification of animals -- Code structure	ISO	http://www.iso.org/
ISO 14223-1:2011 - Radiofrequency identification of animals -- Advanced transponders -- Part 1: Air interface	ISO	http://www.iso.org/
ISO 14223-2:2010 - Radiofrequency identification of animals -- Advanced transponders -- Part 2: Code and command structure	ISO	http://www.iso.org/
ISO 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics	ISO	http://www.iso.org/
ISO/IEC 14443-2:2010 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface	ISO	http://www.iso.org/
ISO/IEC 14443-3:2011 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision	ISO	http://www.iso.org/
ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol	ISO	http://www.iso.org/

ISO/IEC 18000-3:2010 Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz	ISO	http://www.iso.org/
ISO/IEC 18000-6:2013 Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General	ISO	http://www.iso.org/
ISO/IEC TR 29123:2007 Identification Cards – Proximity Cards – Requirements for the enhancement of interoperability	ISO	http://www.iso.org/
ISO/IEC 15693-1:2010 - Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 1: Physical characteristics	ISO	http://www.iso.org/
ISO/IEC 15693-2:2006 - Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization	ISO	http://www.iso.org/
ISO/IEC 15693-3:2009 Amd 3:2015- Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 3: Anticollision and transmission protocol	ISO	http://www.iso.org/

Rationale and Controls

11.7.29. Risk Assessment

11.7.29.R.01. Rationale

As with many technologies, adoption of RFID access cards has the potential to introduce a wide range of risks in addition to the risks that already exist for agency systems. This may compromise the cards and enable unauthorised access, in addition to RFID risks discussed in the previous section. A risk assessment is an essential tool in determining and assessing the range and extent of risk and threat in the use of RFID access cards.

11.7.29.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3130]

Agencies MUST conduct and document a risk assessment before implementing or adopting an RFID access card system.

11.7.29.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3131]

This risk assessment MUST be the basis of a security architecture design.

11.7.30. Security Architecture

11.7.30.R.01. Rationale

The foundation of strong security architecture in RFID follows these important principles:

1. **Physical Security** - over readers, secure areas, issued and unissued access cards;

2. **Controlled access to the data** – only authorised entities (people, systems, devices) can read and write information to the cards, card databases and backend systems;

3. **Control over access to the system** – only authorised entities can configure or add devices to the system, and all devices on the system are authentic and trustworthy;

4. **Confidence and trust** – back-end systems are designed and implemented in accordance with the current version of the NZISM. This includes intrusion detection and incident management mechanisms and procedures.

11.7.30.R.02. Rationale

Some access systems may cover several organisations or sites. In such cases, multiple organisations or sites may require access to databases that contain personnel identifiers, passwords and access permissions. The security architecture should incorporate strong security controls including the authentication of external entities, incident management, audit logging and other essential security controls.

11.7.30.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3138]

Agencies MUST develop a strong security architecture to protect access to databases and systems.

11.7.30.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3139]

Agencies SHOULD apply the NZISM access controls (Chapter 11) and cryptographic controls (Chapter 17) to access card systems.

11.7.30.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3141]

Agencies SHOULD consider the application of the following design elements:

- Implement a Demilitarized Zone (DMZ) to isolate card systems from other parts of the organisation's network and from high-risk Internet Protocol (IP) network connections;
- Secure or remove connections between the Internet and card system network segments;
- Secure or remove vulnerable dialup modem links;
- Secure or remove vulnerable wireless radio links and network access points; and
- Network activity monitoring for unusual or anomalous access activity and well as intrusion detection.

11.7.31. Policy

11.7.31.R.01. Rationale

An Access Card Usage Policy is an essential component addressing topics such as how personal information is stored and shared, card holder responsibilities and procedures to manage card loss or damage. Refer also to Chapter 20 – Data Management.

11.7.31.R.02. Rationale

Any access card implementation should also be incorporated into the agency's security policies. Refer also to Chapter 5 – Information Security Documentation.

11.7.31.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3156]

Agencies SHOULD develop, implement and maintain an Access Card Usage Policy.

11.7.31.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3157]

Agencies SHOULD incorporate access cards into the agency's security policies and information security documentation.

11.7.32. Physical Security

11.7.32.R.01. Rationale

Physical security over readers, door controls, cables and control systems, as well as the cards themselves is fundamental to the operation of a secure system.

11.7.32.R.02. Rationale

In order to minimise unnecessary electromagnetic radiation readers and control equipment should be carefully positioned. Care should be taken with the use of card readers in proximity to:

- Fuel, ordnance, and other hazardous materials,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radio systems to avoid interference.

11.7.32.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3162]

Agencies SHOULD select systems that provide resistance to physical or electronic tampering.

11.7.32.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3163]

Agencies SHOULD implement systems to minimise the risk of physical or electronic tampering.

11.7.32.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3165]

Agencies SHOULD consider placement of tags and location of readers to avoid unnecessary electromagnetic radiation.

11.7.32.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3166]

Agencies SHOULD consider and select other physical controls in accordance with the PSR.

11.7.33. Card Data Protection

11.7.33.R.01. Rationale

Cards are invariably retained by the card holder and subject to loss, theft or being misplaced. Cards are also not always within the control of the card holder outside of normal office hours. Measures to protect cards in these situations are fundamental to the maintenance of the integrity and security of the access control system.

11.7.33.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3171]

Agencies MUST follow the requirements of the NZISM in the selection and implementation of cryptographic protocols and algorithms, and in key management, detailed in Chapter 17 - Cryptography.

11.7.33.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3173]

Agencies SHOULD encrypt data before it is written to cards.

11.7.33.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3175]

Agencies SHOULD consider the use of cards systems incorporating Secure Access Modules (SAMs).

11.7.34. Incident Management

11.7.34.R.01. Rationale

Incident management and audit procedures, logging and time stamps help detect and manage security breaches. These are important tools in protecting systems and managing security breaches.

11.7.34.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3180]

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 –

11.7.35. Disposal

11.7.35.R.01.   Rationale

Card disposal and recycling procedures that permanently disable or destroy sensitive data reduces the possibility that they could be used later for tracking or targeting, and prevents access to sensitive data stored on cards. In addition the continued operating presence of a card after it has performed its intended function can pose an unauthorised access, business intelligence or privacy risk, including tracking and targeting of personnel or access to sensitive data on the access card.

11.7.35.R.02.   Rationale

Disposal may be undertaken by electronically by using a card's wipe feature or using a strong electromagnetic field to permanently deactivate a tag's circuitry. Alternatively physical destruction can be achieved by tearing or shredding. Where a tag supports an electronic deactivation mechanism, tags should be electronically deactivated before physical destruction.

11.7.35.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3189]

Agencies SHOULD consider secure disposal procedures and incorporate these into the Access Card Usage Policy. Refer also to Chapter 13 – Decommissioning and Disposal.

12. Product Security

12.1. Product Selection and Acquisition

Objective

12.1.1.   Products providing security functions for the protection of classified information are formally evaluated in order to provide a degree of assurance over the integrity and performance of the product.

Context

Scope

12.1.2.   This section covers information on the selection and acquisition of any product that provide security functionality for the protection of information. It DOES NOT provide information on the selection or acquisition of products that do not provide security functionality or physical security products.

Selecting products without security functions

12.1.3.   Agencies selecting products that do not provide a security function or selecting products that will not use their security functions are free to follow their own agency or departmental acquisition guidelines.

Product specific requirements

12.1.4.   Where consumer guides exist for evaluated products, agencies should identify and assess any potential conflicts with this manual. Where further advice is required, consult the GCSB.

Convergence

12.1.5.   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.

12.1.6.   Most products will exhibit some element of convergence. When products have converged elements, agencies will need to comply with the relevant areas of this manual for the discrete technologies when deploying the converged product.

12.1.7.   As an example, when agencies choose to use evaluated media, such as encrypted flash memory media, the requirements for evaluated products, media and cryptographic security apply.

Assurance

12.1.8.   In Common Criteria (CC), assurance is the confidence that a Target of Evaluation (TOE) meets the Security Functional Requirements (SFR) of the product.

Determining Assurance

12.1.9.   In order to determine the level of assurance (the EAL), the CC standard requires tests, checks and evaluations in several areas. Higher levels of assurance require more extensive design, documentation, testing and evaluation. Determining assurance requires assessment of the following elements:

- Development;
- Guidance documents;
- Life-cycle support;
- Security Target evaluation;
- Tests; and
- Vulnerability assessment.

Augmented Assurance

12.1.10. It is possible to "augment" an evaluation to provide additional assurance without changing the fundamental assurance level. This mechanism allows the addition of assurance components not specifically required for a specific level of evaluation or the substitution of assurance components from the specification of another hierarchically higher assurance component. Of the assurance constructs defined in the CC, only EALs may be augmented. An augmented EAL is often indicated by a "+"-sign (for example EAL4+). The concept of negative augmentation or an "EAL minus" is not recognised by

the standard.

High Assurance

12.1.11. High Assurance is a generic term encompassing EAL levels 5, 6 and 7. ASD run an independent High Assurance Evaluation scheme which is not related to AISEP or an EAL rating.

Evaluated Products List

12.1.12. The Evaluated Products List (EPL) records 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; or
- an Australasian Information Security Evaluation Program (AISEP) approved evaluation.

12.1.13. The AISEP Evaluated Products List (EPL) is maintained by the Australian Signals Directorate (ASD) and provides a listing of approved products for the protection of classified information. Other EPL's are available through the Common Criteria website.

Evaluation level mapping

12.1.14. The Information Technology Security Evaluation Criteria (ITSEC) and Common Criteria (CC) assurance levels used in the EPL are similar, but not identical, in their relationship. The table below shows the relationship between the two evaluation criteria.

12.1.15. This manual refers only to Common Criteria Evaluation Assurance Levels (EALs). The table below maps ITSEC evaluation assurance levels to Common Criteria EALs. EAL's are defined in the Common Criteria Standard – part 3.

Criteria	Assurance level							
Common Criteria	N/A	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	E0	N/A	E1	E2	E3	E4	E5	E6

Recognition arrangements

12.1.16. The AISEP programme has a number of recognition arrangements regarding evaluated products. Before choosing a product that has not been evaluated by the AISEP, agencies are encouraged to contact the GCSB to enquire whether the product will be recognised for New Zealand use once it has complete evaluation in a foreign scheme.

12.1.17. Two such recognition arrangements are for the Common Criteria Recognition Arrangement up to the assurance level of EAL2 with the lifecycle flaw remediation augmentation and for degausser products listed on the National Security Agency/Central Security Service's EPLD.

Australasian Information Security Evaluation Program (AISEP)

12.1.18. The AISEP exists to ensure that a range of evaluated products are available to meet the needs of Australian and New Zealand Government agencies.

12.1.19. The AISEP performs the following functions:

- evaluation and certification of products using the Common Criteria;
- continued maintenance of the assurance of evaluated products; and
- recognition of products evaluated by a foreign scheme with which the AISEP has a mutual recognition agreement (generally the Common Criteria Recognition Agreement – CCRA).

Protection Profiles

12.1.20. A Protection Profile (PP) describes the security functionality that must be included in a Common Criteria evaluation to meet a range of defined threats. PPs also define the activities to be taken to assess the security functions of a product. Agencies can have confidence that a product evaluated against an AISEP or GCSB approved PP addresses the defined threats. Approved PPs are published on the AISEP Evaluated Product List.

12.1.21. The introduction of PP's is to reduce the time required for evaluation, compared with the traditional approach to allow the AISEP to keep pace with the rapid evolution, production and release of security products and updates. Cryptographic security functionality is included in the scope of evaluation against an approved Protection Profile.

12.1.22. To facilitate the transition to AISEP approved Protection Profiles, a cap of Evaluation Assurance Level (EAL) 2 applies for all traditional AISEP (EAL based evaluations), including for technologies with no existing approved Protection Profile. EAL 2 is considered to represent a sensible trade-off between completion time and meaningful security assurance gains.

12.1.23. Evaluations conducted in other nations' Common Criteria schemes will continue to be recognised by the GCSB under the AISEP.
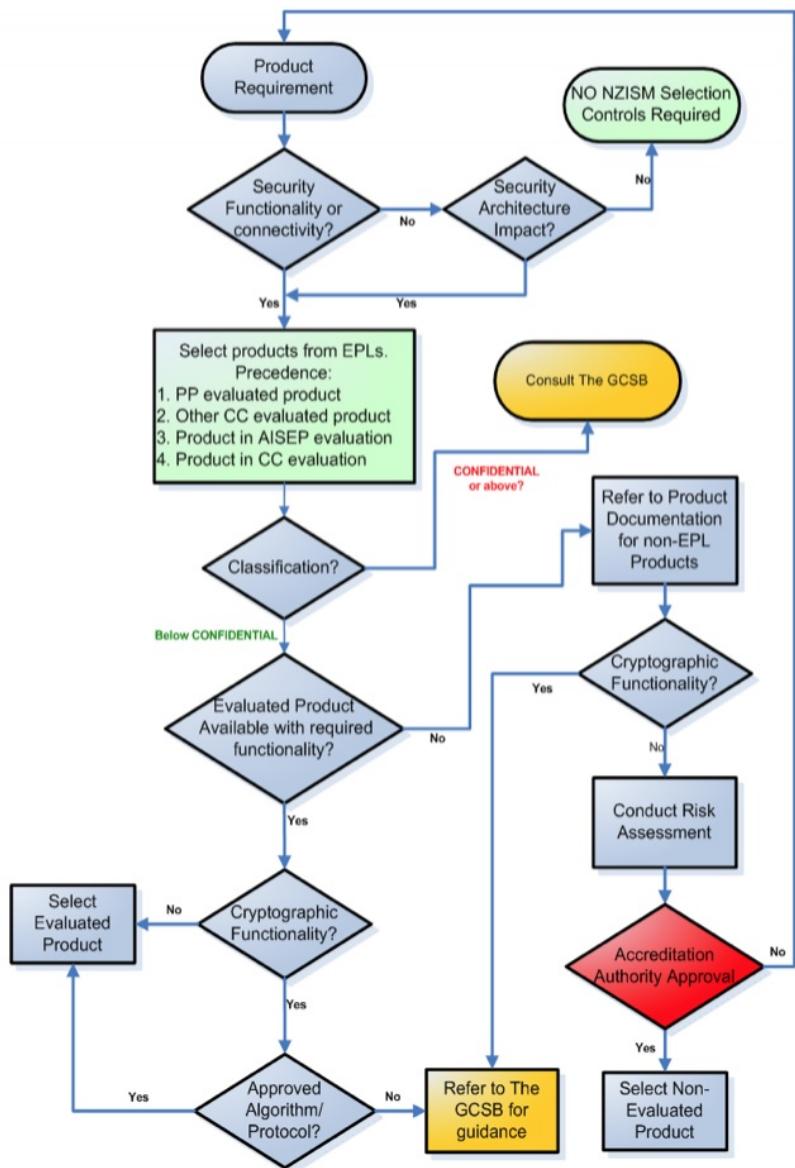
12.1.24. Some High Assurance evaluations continue to be conducted in European Approved Testing Facilities and use the EAL rating scheme. ASD run an independent High Assurance Evaluation scheme which is not related to AISEP or an EAL rating.

12.1.25. It is important that Agencies check the evaluation has examined the security enforcing functions by reviewing the target of evaluation/security target and other testing documentation.

12.1.26. The UK utilises several product evaluation schemes such as the CESG Assisted Products Service (CAPS), CESG Assured Service (CAS) and IT Security Evaluation Criteria (ITSEC). Agencies should consult the GCSB if further clarity on the utilisation of these evaluation schemes and products is required.

Product Selection

12.1.27. The UK utilises several product evaluation schemes such as the CESG Assisted Products Service (CAPS), CESG Assured Service (CAS) and IT Security Evaluation Criteria (ITSEC). Agencies should consult the GCSB if further clarity on the utilisation of these evaluation schemes and products is required.

References

12.1.28.

Topic	Publisher	Source
Evaluated Products List (EPL)	ASD	https://www.cyber.gov.au/publications/evaluated-products-list
Australian Information Security Evaluation Program (AISEP)	ASD	https://www.cyber.gov.au/programs/australasian-information-security-evaluation-program
Common Criteria	CC	http://www.commoncriteriaportal.org/
Common Criteria Certified Products	CC	http://www.commoncriteriaportal.org/products
Product & Services Marketplace	NCSC, UK	https://www.ncsc.gov.uk/marketplace
National Information Assurance Partnership (NIAP)	NIAP	https://ww.niap-ccevs.org
Government Rules of Sourcing	Ministry of Business Innovation & Employment (MBIE)	http://www.procurement.govt.nz/procurement/pdf-library/agencies/rules-of-sourcing/government-rules-of-sourcing-April-2013.pdf

PSR references

12.1.29. Relevant PSR requirements can be found at:

Reference	Title	Source

PSR Mandatory Requirements	GOV5, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Supply chain security	https://www.protectivesecurity.govt.nz/governance/supply-chain-security/
Managing specific scenarios	Outsourced ICT facilities Outsourcing, Offshoring and supply chains	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/outsourced-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/

Rationale & Controls

12.1.30. Evaluated product selection preference order

12.1.30.R.01. Rationale

In selecting products for use, agencies should note that completed evaluations provide greater assurance than those products that are still undergoing evaluation or have not completed any formal evaluation activity. This assurance gradation is reflected in the preference order for selecting security products. If an agency selects a product that is ranked lower in the preference order, the justification for this decision MUST be recorded.

12.1.30.R.02. Rationale

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, the GCSB may advise agencies on appropriate risk reduction strategies.

12.1.30.R.03. Rationale

It is important to recognise that a product that is under evaluation has not, and might never, complete all relevant evaluation processes.

12.1.30.R.04. Rationale

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 the GCSB, could override this standard by specifying more rigorous requirements for particular functions and device use.

12.1.30.R.05. Rationale

Additionally, where an EAL rating is mandated for a product to perform a cryptographic function for the protection of data at rest or in transit, as specified within Chapter 17 – Cryptography, products that have not completed an Approved Evaluation do not satisfy the requirement.

12.1.30.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3284]

Agencies MUST select products in the following order of preference:

- a protection profile (PP) evaluated product;
- products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA);
- products in evaluation in the AISEP;
- products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or
- If products do not fall within any of these categories, contact the GCSB.

12.1.30.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3286]

When choosing a product, agencies MUST document the justification for any decision to choose a product that is still in evaluation and accept any security risk introduced by the use of such a product.

12.1.30.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3287]

Agencies SHOULD select products in the following order of preference:

- a protection profile (PP) evaluated product;
- products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA);
- products in evaluation in the AISEP;
- products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or
- If products do not fall within any of these categories, normal selection criteria (such as functionality and security) will apply.

12.1.31. Evaluated product selection

12.1.31.R.01. Rationale

A product listed on the EPL might not meet the security requirements of an agency. 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. As such, an agency should ensure that a product is suitable by reviewing all available documentation. In the case of Common Criteria certified

products, this documentation includes the protection profile, target of evaluation, security target, certification report, consumer guide and any qualifications and limitations contained in the entry on the EPL.

12.1.31.R.02. Rationale

Products that are in evaluation will not have a certification report and may not have a published security target. A protection profile will, as a rule, exist. A draft security target can be obtained from the GCSB 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.

12.1.31.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3294]

Agencies SHOULD select products that have their desired security functionality within the scope of the product's evaluation and are applicable to the agency's intended environment.

12.1.32. Product specific requirements

12.1.32.R.01. Rationale

Whilst this manual may recommend a minimum level of assurance in the evaluation of a product's security functionality not all evaluated products may be found suitable for their intended purpose even if they 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.

12.1.32.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3299]

Agencies MUST check consumer guides for products, where available, to determine any product specific requirements.

12.1.32.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3304]

Where product specific requirements exist in a consumer guide, agencies MUST comply with the requirements outlined in the consumer guide.

12.1.32.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:3306]

Agencies selecting high assurance products and HGCE MUST contact the GCSB and comply with any product specific requirements, before any purchase is made.

12.1.33. Sourcing non-evaluated software

12.1.33.R.01. Rationale

Software downloaded from websites on the Internet can 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.

12.1.33.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3310]

Agencies SHOULD:

- obtain software from verifiable sources and verify its integrity using vendor supplied checksums; and
- validate the software's interaction with the operating systems and network within a test environment prior to use on operational systems.

12.1.34. Delivery of evaluated products

12.1.34.R.01. Rationale

It is important that agencies ensure that the selected product is the actual product received. If the product differs from the evaluated version, then NO assurance can be gained from an evaluation being previously performed.

12.1.34.R.02. Rationale

For products evaluated under the ITSEC or the Common Criteria scheme at EAL2 or higher, delivery information is available from the developer in the delivery procedures document.

12.1.34.R.03. Rationale

For products that do not have evaluated delivery procedures, it is recommended that agencies assess whether the vendor's delivery procedures are sufficient to maintain the integrity of the product.

12.1.34.R.04. Rationale

Other factors that the assessment of the delivery procedures for products might consider include:

- the intended environment of the product;
- likely attack vectors;
- the types of attackers that the product will defend against;
- the resources of any potential attackers;
- the likelihood of an attack;
- the level of importance of maintaining confidentiality of the product purchase; and
- the level of importance of ensuring adherence to delivery timeframes.

12.1.34.R.05. Rationale

Delivery procedures can vary greatly from product to product. For most products the standard commercial practice for packaging and delivery can be sufficient for agencies requirements. More secure delivery procedures can include measures to detect tampering or masquerading. Some examples of specific security measures include tamper evident seals, cryptographic checksums and signatures, and secure transportation.

12.1.34.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3318]

Agencies procuring high assurance products and HGCE MUST contact the GCSB and comply with any product specific delivery procedures.

12.1.34.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3320]

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

12.1.35. Delivery of non-evaluated products

12.1.35.R.01. Rationale

When a non-evaluated product is purchased agencies should determine if the product has arrived in a state that they were expecting it to and that there are no obvious signs of tampering.

12.1.35.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3325]

Agencies SHOULD 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, including checking:

- any labelling changes;
- any damage; and
- any signs of tampering.

12.1.36. Leasing arrangements

12.1.36.R.01. Rationale

Agencies should consider security and policy requirements when entering into a leasing agreement for IT equipment in order to avoid potential information security incidents during maintenance, repairs or disposal processes.

12.1.36.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3330]

Agencies SHOULD ensure that leasing agreements for IT equipment takes into account the:

- difficulties that could be encountered when the equipment needs maintenance;
- control of remote maintenance, software updates and fault diagnosis;
- if the equipment can be easily sanitised prior to its return; and
- the possible requirement for destruction if sanitisation cannot be performed.

12.1.37. Ongoing maintenance of assurance

12.1.37.R.01. Rationale

Developers that have demonstrated a commitment to ongoing maintenance or evaluation are more likely to be responsive to ensuring that security patches are independently assessed.

12.1.37.R.02. Rationale

A vendor's commitment to assurance continuity can be gauged through the number of evaluations undertaken and whether assurance maintenance has been performed on previous evaluations.

12.1.37.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3337]

Agencies SHOULD choose products from developers that have made a commitment to the ongoing maintenance of the assurance of their product.

12.2. Product Installation and Configuration

Objective

12.2.1. Evaluated products use evaluated configurations.

Context

Scope

12.2.2. This section covers information on installing and configuring products providing security functionality. It does not provide information on the installation and configuration of general products or physical security products.

Evaluated configuration

12.2.3. A product is considered to be operating in its evaluated configuration if:

- functionality is used that was within 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; and
- the environment complies with assumptions or organisational security policies stated in the product's security target or similar document.

Unevaluated configuration

12.2.4. A product is considered to be operating in an unevaluated configuration when it does not meet the requirements of an evaluated configuration.

Rationale & Controls

12.2.5. Installation and configuration of evaluated products

12.2.5.R.01. Rationale

An evaluation of products provides assurance that the product will work as expected with a clearly defined set of constraints. These constraints, defined by the scope of the evaluation, generally consist of what security functionality can be used, and how the products are configured and

operated.

12.2.5.R.02. Rationale

Using an evaluated product in manner which it was not intended could result in the introduction of new threats and vulnerabilities that were not considered by the initial evaluation.

12.2.5.R.03. Rationale

For products evaluated under the Common Criteria and ITSEC, 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.

12.2.5.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3387]

Agencies MUST ensure that high assurance products and HGCE are installed, configured, operated and administered in accordance with all product specific policy.

12.2.5.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3389]

Agencies SHOULD install, configure, operate and administer evaluated products in accordance with available documentation resulting from the product's evaluation.

12.2.6. Use of evaluated products in unevaluated configurations

12.2.6.R.01. Rationale

To ensure that a product will still provide the assurance desired by the agency when used in a manner for which it was not intended, a security risk assessment MUST be conducted upon the altered configuration. The further that a product deviates from its evaluated configuration, the less assurance can be gained from the evaluation.

12.2.6.R.02. Rationale

Given the potential threat vectors and the value of the classified information being protected, high assurance products and HGCE MUST be configured in accordance with the GCSB's guidelines.

12.2.6.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3401]

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; and
- the environment in which the unevaluated product is to be used.

12.2.6.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:3404]

High assurance products and HGCE MUST NOT be used in unevaluated configurations.

12.3. Product Classifying and Labelling

Objective

12.3.1. IT equipment is classified and appropriately labelled.

Context

Scope

12.3.2. This section covers information relating to the classification and labelling of both evaluated and non-evaluated IT equipment.

Non-essential labels

12.3.3. Non-essential labels are labels other than classification and asset labels.

Rationale & Controls

12.3.4. Classifying IT equipment

12.3.4.R.01. Rationale

Much of today's technology incorporates an internal data storage capability. When media is used in IT equipment there is no guarantee that the equipment has not automatically accessed classified information from the media and stored it locally to the device, without the knowledge of the system user. As such, the IT equipment needs to be afforded the same degree of protection as that of the associated media.

12.3.4.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3423]

Agencies MUST classify IT equipment based on the highest classification of information the equipment and any associated media within the equipment, are approved for processing, storing or communicating.

12.3.5. Labelling IT equipment

12.3.5.R.01. Rationale

The purpose of applying protective markings to all assets in a secure 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 itself.

12.3.5.R.02. Rationale

Applying protective markings to assets also assists in determining the appropriate usage, sanitisation, disposal or destruction requirements of the asset based on its classification. This is of particular importance in data centres and computer rooms.

12.3.5.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3427]

Agencies MUST clearly label all IT equipment capable of storing or processing classified information, with the exception of HGCE, with the appropriate protective marking.

12.3.5.C.02.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3428]

Agencies MUST clearly label all IT equipment in data centres or computer rooms with an asset identification and the level of classification to which that equipment has been accredited.

12.3.6.   Labelling high assurance products

12.3.6.R.01.   Rationale

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.

12.3.6.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:3431]

Agencies MUST NOT have any non-essential labels applied to external surfaces of high assurance products.

12.3.7.   Labelling HGCE

12.3.7.R.01.   Rationale

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 with GCSB approval.

12.3.7.C.01.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3434]

Agencies SHOULD seek GCSB authorisation before applying labels to external surfaces of HGCE.

12.4. Product Patching and Updating

Objective

12.4.1.   To ensure security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities and performance risks.

Context

Scope

12.4.2.   This section covers information on patching both evaluated and non-evaluated software and IT equipment.

Rationale & Controls

12.4.3.   Vulnerabilities and patch availability awareness

12.4.3.R.01.   Rationale

It is important that agencies monitor relevant sources for information about new vulnerabilities and security patches. This way, agencies can take pro-active steps to address vulnerabilities in their systems.

12.4.3.C.01.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3444]

Agencies SHOULD monitor relevant sources for information about new vulnerabilities and security patches for software and IT equipment used by the agency.

12.4.4.   Patching vulnerabilities in products

12.4.4.R.01.   Rationale

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 are released to address known security vulnerabilities. Applying these patches should be considered as part of an agency's overall risk management strategy.

12.4.4.R.02.   Rationale

Given the potential threat vectors and the value of the classified information being protected, high assurance products MUST NOT be patched by an agency without specific direction from the GCSB. If a patch is released for a high assurance product, the GCSB will conduct an assessment of the patch and might revise the product's usage guidance. Likewise, for patches released for HGCE, the GCSB will subsequently conduct an assessment of the cryptographic vulnerability and might revise usage guidance in the consumer guide for the product.

12.4.4.C.01.   ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3448]

Agencies MUST apply all critical security patches as soon as possible and within two (2) days of the release of the patch or update.

12.4.4.C.02.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3449]

Agencies MUST implement a patch management strategy, including an evaluation or testing process.

12.4.4.C.03.   ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:3450]

Agencies MUST NOT patch high assurance products or HGCE without the patch being approved by the GCSB.

12.4.4.C.04.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3451]

Agencies SHOULD apply all critical security patches as soon as possible and preferably within two (2) days of the release of the patch or update.

12.4.4.C.05.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3452]

Agencies SHOULD apply all non-critical security patches as soon as possible.

12.4.4.C.06.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3453]

Agencies SHOULD ensure that security patches are applied through a vendor recommended patch or upgrade process.

12.4.5. When security patches are not available

12.4.5.R.01.   Rationale

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 measures to detect attacks attempting to exploit the vulnerability.

12.4.5.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3455]

Where known vulnerabilities cannot be patched, or security patches are not available, agencies SHOULD implement:

- controls to resolve the vulnerability such as:
    - disable the functionality associated with the vulnerability though product configuration;
    - ask the vendor for an alternative method of managing the vulnerability;
    - install a version of the product that does not have the identified vulnerability;
    - install a different product with a more responsive vendor; or
    - engage a software developer to correct the software.

- controls to prevent exploitation of the vulnerability including:
    - apply external input sanitisation (if an input triggers the exploit);
    - apply filtering or verification on the software output (if the exploit relates to an information disclosure);
    - apply additional access controls that prevent access to the vulnerability; or
    - configure firewall rules to limit access to the vulnerable software.

- controls to contain the exploit including:
    - apply firewall rules limiting outward traffic that is likely in the event of an exploitation;
    - apply mandatory access control preventing the execution of exploitation code; or
    - set file system permissions preventing exploitation code from being written to disk;
    - white and blacklisting to prevent code execution; and

- controls to detect attacks including:
    - deploy an IDS;
    - monitor logging alerts; or
    - use other mechanisms as appropriate for the detection of exploits using the known vulnerability.

- controls to prevent attacks including:
    - deploy an IPS or HIPS; or
    - use other mechanisms as appropriate for the diversion of exploits using the known vulnerability, such as honey pots and Null routers.

12.4.6. Firmware updates

12.4.6.R.01.   Rationale

As firmware provides the underlying functionality for hardware it is essential that the integrity of any firmware images or updates are maintained.

12.4.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3460]

Agencies MUST ensure that any firmware updates are performed in a manner that verifies the integrity and authenticity of the source and of the updating process or updating utility.

12.4.7. Unsupported products

12.4.7.R.01.   Rationale

Once a cessation date for support is announced for software or IT equipment, agencies will increasingly find it difficult to protect against vulnerabilities found in the software or IT equipment as no security patches will be made available by the manufacturer after support ceases.

12.4.7.R.02.   Rationale

Once a cessation date for support is announced agencies should assess the timeline, investigate new solutions that will be appropriately supported and establish a plan to implement the new solution.

12.4.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3465]

Agencies SHOULD assess the security risk of continued use of software or IT equipment when a cessation date for support is announced or when the product is no longer supported by the developer.

12.5. Product Maintenance and Repairs

Objective

12.5.1. Products are repaired by cleared or appropriately escorted personnel.

Context

Scope

12.5.2. This section covers information on maintaining and repairing both evaluated and non-evaluated IT equipment.

12.5.3.   Maintenance and repairs

12.5.3.R.01.   Rationale

Making unauthorised repairs to high assurance products or HGCE can impact the integrity of the product or equipment.

12.5.3.R.02.   Rationale

Using cleared technicians on-site at an agency's facilities is considered the most desired approach to maintaining and repairing IT 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.

12.5.3.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3481]

Agencies MUST seek GCSB approval before undertaking any repairs to high assurance products or HGCE.

12.5.3.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3483]

Maintenance and repairs of IT equipment containing media SHOULD be carried out on-site by an appropriately cleared technician.

12.5.4.   Maintenance and repairs by an uncleared technician

12.5.4.R.01.   Rationale

Agencies choosing to use uncleared technicians to maintain or repair IT equipment on-site at an agency's facilities, or off-site at a company's facilities, should be aware of the requirement for cleared personnel to escort the uncleared technicians during maintenance or repair activities.

12.5.4.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3492]

If an uncleared technician is used to undertake maintenance or repairs of IT 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; and
- has the authority to direct the technician.

12.5.4.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3493]

If an uncleared technician is used to undertake maintenance or repairs of IT equipment, agencies SHOULD sanitise and reclassify or declassify the equipment and associated media before maintenance or repair work is undertaken.

12.5.4.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3494]

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

12.5.4.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3495]

If an uncleared technician is used to undertake maintenance or repairs of IT equipment, the technician SHOULD be escorted by someone who is sufficiently familiar with the product to understand the work being performed.

12.5.5.   Off-site maintenance and repairs

12.5.5.R.01.   Rationale

Agencies choosing to have IT 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.

12.5.5.R.02.   Rationale

Agencies choosing to have IT 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.

12.5.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3498]

Agencies having IT 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 are maintained at all times.

12.5.6.   Maintenance and repair of IT equipment from secure areas

12.5.6.R.01.   Rationale

Where equipment is maintained or repaired offsite, agencies should identify any co-located equipment of a higher classification. This higher classification equipment may be at risk of compromise from modifications or repairs to the lower classification equipment.

12.5.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3504]

Offsite repairs and maintenance SHOULD treat all equipment in accordance with the requirements for the highest classification of information processed, stored or communicated in the area that the equipment will be returned to.

12.5.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3507]

Agencies SHOULD conduct or arrange to have technical inspections conducted on all equipment returned to the secure area after maintenance or repair.

12.6. Product Sanitisation and Disposal

12.6.1.   All IT equipment is sanitised and disposed of in an approved and secure manner.

Scope

12.6.2. This section covers information on sanitising and disposing of both evaluated and non-evaluated IT equipment. Additional information on the sanitisation, destruction and disposal of media can be found in Chapter 13 – Decommissioning and Disposal.

12.6.3. Media typically found installed in IT equipment are 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 and volatile memory such as RAM cards. Some technologies, such as an FPGA, may integrate memory capabilities.

Rationale & Controls

12.6.4. Sanitisation or destruction of IT equipment

12.6.4.R.01. Rationale

In order to prevent the disclosure of classified information into the public domain agencies will need to ensure that IT equipment is either sanitised or destroyed before being declassified and authorised for released into the public domain. Refer also to Chapter 13 - Media and

IT Equipment Management, Decommissioning and Disposal.

12.6.4.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3537]

Agencies MUST sanitise or destroy, then declassify, IT equipment containing **any** media before disposal.

12.6.4.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3540]

IT equipment and associated media that have processed or stored NZEO information, and cannot be sanitised, MUST be returned to New Zealand for sanitisation or destruction, declassification and disposal.

12.6.5. Disposal of IT equipment

12.6.5.R.01. Rationale

When disposing of IT equipment, agencies need to sanitise or destroy and subsequently declassify any media within the product that are capable of storing classified information. Once the media have 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 by the agency.

12.6.5.R.02. Rationale

The GCSB provides specific advice on how to securely dispose of high assurance products, HGCE and TEMPEST rated 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.

12.6.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3545]

Agencies MUST have a documented process for the disposal of IT equipment.

12.6.5.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3547]

Agencies MUST contact the GCSB and comply with any requirements for the disposal of high assurance products.

12.6.5.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:3549]

Agencies MUST contact the GCSB and comply with any requirements for the disposal of HGCE.

12.6.5.C.04. Control System Classification(s): All Classifications; Compliance: MUST [CID:3550]

Agencies MUST contact GCSB and comply with any requirements for the disposal of TEMPEST rated IT equipment or if the equipment is non-functional.

12.6.5.C.05. Control System Classification(s): All Classifications; Compliance: MUST [CID:3552]

Agencies MUST formally sanitise and then authorise the disposal of IT equipment, or waste, into the public domain.

12.6.6. Sanitising printer cartridges and copier drums

12.6.6.R.01. Rationale

Electrostatic drums can retain an image of recently printed documents providing opportunity for unauthorised access to information. Some printer cartridges may have integrated 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 drum or cartridge.

12.6.6.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3555]

Agencies MUST print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.

12.6.6.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3557]

Agencies SHOULD print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.

12.6.7. Destroying printer cartridges and copier drums

12.6.7.R.01. Rationale

When printer cartridges with integrated copier drums or discrete drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them.

12.6.7.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3561]

Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, MUST destroy the cartridge or drum.

12.6.7.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3563]

Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, SHOULD destroy the cartridge or drum.

12.6.8. Disposal of televisions and monitors

12.6.8.R.01. Rationale

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.

12.6.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3566]

Agencies MUST visually inspect video screens by turning up the brightness to the maximum level to determine if any classified information has been burnt into or persists on the screen, before redeployment or disposal.

12.6.9. Sanitising televisions and monitors

12.6.9.R.01. Rationale

All types of video screens are capable of retaining classified 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 whilst LCD screens can be affected by image persistence which can led to LED/OLED burn-in.

12.6.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3572]

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. If burn-in cannot be corrected the screen MUST be processed through a destruction facility.

12.6.10. LCD/LED, plasma and non-CRT monitor types

12.6.10.R.01. Rationale

Current generations of monitors incorporate controllers to manage power up/power down, manage the display, operate any USB or other ports and manage the video data stream. The controller requires memory to operate and it incorporates some data storage capability and full write/read access to the display. It also retains settings and configuration. The underlying technology is often based on an FPGA and invariably requires some form of memory capability in order to operate.

Researchers have demonstrated that images can be recovered by directly accessing the controller and associated memory or analysing the orientation of the liquid crystals.

In addition monitors can be compromised to actively monitor or covertly steal data and even manipulate what is displayed on the screen. Other attacks exploiting monitors have also been demonstrated.

12.6.10.R.02. Rationale

Refer to Chapter 12 – Product Security and Chapter 13 – Media & IT Equipment Management, Decommissioning and Disposal for additional guidance.

12.6.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6997]

Because of the risks that data can be recovered from monitors, it is essential that any redeployment or disposal of monitors MUST follow the guidance in the NZISM.

12.7. Supply Chain

Objective

12.7.1. Technology supply chains are established and managed to ensure continuity of supply and protection of sensitive related information.

Context

12.7.2. A supply chain is the movement of materials as they move from their source (raw materials) through manufacture to the end customer. A supply chain can include materials acquisition, purchasing, design, manufacturing, warehousing, transportation, customer service, and supply chain management. It requires people, information and resources to move a product from manufacturer to supplier to customer. Every supply chain carries some risk which may include product protection; counterfeit products and goods and defective products. ICT supply chains are invariably global and complex.

12.7.3. Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (e.g. through supply contracts, interagency agreements, lines of business arrangements, service-level agreements), licensing agreements, and/or supply chain exchanges. The growing use of external service providers and new relationships being established with those providers present new and difficult challenges for organisations, especially in the area of information system security. These challenges include:

- Defining the types of external information system services provided to organisations;
- Describing how those external services are protected; and
- Obtaining the necessary assurances that the risks to organisational operations and assets, individuals, other organisations, and national security arising from the use of the external services are acceptable.

12.7.4. The degree of confidence that the risk from using external services is at an acceptable level depends on the assurance external organisations provide and trust that organisations place in external service providers. In some cases, the level of trust is based on the amount of direct control organisations are able to exert on external service providers in the use of security controls and assurance on the effectiveness of those controls.

12.7.5. The level of control is usually established by the terms and conditions of the contracts or service-level agreements with the external service providers and can range from extensive control (e.g., negotiating contracts or agreements that specify detailed security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services).

12.7.6. From an Information Assurance viewpoint, there are five key aspects to supply chain risk:

1. Protection of sensitive information and systems;

2. Continuity of supply;

3. Product assurance;

4. Security validation; and

5. National Procurement Policy

Protection of sensitive information and systems

12.7.7. This relates to the security of the supply chain, products and information relating to the intended use, purchaser, location and type of equipment.

Continuity of supply

12.7.8. This is the traditional set of risks associated with supply chain. As supply chains have globalised and components are sourced from a number of countries, a disruption to supply may have a global effect.

Product assurance

12.7.9. This relates to assurance that the product, technology or device performs as designed and specified and includes the provenance of the product, equipment, or device.

Security validation

12.7.10. Security validation checks the performance and security of the equipment. The security design elements and features of the equipment or product will need to be separately considered from any operational drivers.

National procurement policy

12.7.11. All agencies are required to follow the guidance of the Government Rules of Procurement. Some exemptions are permitted under Rule 13 including that of security, "essential security interests: Measures necessary for the protection of essential security interests, procurement indispensable for national security or for national defence…". Care must be taken to follow these rules wherever possible.

Scope

12.7.12. This manual provides additional guidance for managing supply chain security risks associated with the acquisition (lease or purchase) of ICT equipment or services for use in NZ Government systems.

References

12.7.13. While NOT an exhaustive list, further information on procurement and supply chain can be found at:

Title	Publisher	Source
Government Use of Offshore Information and Communication Technologies (ICT) Service Providers - Advice on Risk Management April 2009	State Services Commission	http://www.ict.govt.nz/assets/ICT-System-Assurance/offshore-ICT-service-providers-april-2009.pdf
The new Government Rules of Sourcing	Procurement.govt.NZ	http://www.business.govt.nz/procurement/for-agencies/key-guidance-for-agencies/the-new-government-rules-of-sourcing
Government Rules of Sourcing - Rules for planning your procurement, approaching the market and contracting	Ministry of Business Innovation and Employment	http://www.business.govt.nz/procurement/pdf-library/agencies/rules-of-sourcing/government-rules-of-sourcing-April-2013.pdf
Special Publication 800-161, Supply Chain Risk Management	Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)	http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf
Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NISTIR 7622, Notional Supply Chain Risk Practices for Federal Information Systems	NIST	http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf
Commercial Procurement & Relationships	UK Cabinet Office	https://www.gov.uk/government/organisations/cabinet-office
CIO Council Government ICT Offshoring (International Sourcing) Guidance	UK Cabinet Office	https://www.gov.uk/government/publications/government-ict-offshoring-international-sourcing-guidance
Commonwealth Procurement Rules	Department of Finance and deregulation (Financial Management Group)	http://www.finance.gov.au/procurement/docs/cpr_commonwealth_procurement_rules_july_2012.pdf
ISO 31000:2018, Risk management – Guidelines	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz

HB 231:2004, Information Security Risk Management Guidelines	ISO / IEC Standards NZ	http://www.standards.co.nz
ISO Guide 73:2009, Risk management - Vocabulary	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz
ISO/IEC 31010:2009, Risk management - Risk assessment techniques	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz
ISO/IEC 27002:2013, Information technology - security techniques - code of practice for information security controls	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27002.html http://www.standards.co.nz
ISO/IEC 27005:2012 Information technology - Security Techniques - Information Security Risk Management	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27005.html http://www.standards.co.nz
ISO 28000 Supply chain security management system standard	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz

Rationale & Controls

12.7.14. Risk Management

12.7.14.R.01. Rationale

ICT supply chains can introduce particular risks to an agency. In order to manage these risks, in addition to other identified ICT risks, supply chain risks are incorporated into an agency's assessment of risk and the Security Risk Management Plan (SRMP). Identified risks are managed through the procurement process and through technical checks and controls (See Section 5.3 – Security Risk Management Plans and Chapter 4 – System Certification and Accreditation).

12.7.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3634]

Agencies SHOULD incorporate the consideration of supply chain risks into an organisation-wide risk assessment and management process.

12.7.14.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3638]

Agencies SHOULD monitor supply chain risks on an ongoing basis and adjust mitigations and controls appropriately.

12.7.14.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3639]

Agencies SHOULD follow the Government Rules of Procurement.

12.7.15. Contractor or Supplier Capability

12.7.15.R.01. Rationale

Agencies can assess the capability of a contractor and any subcontractors to meet their security of information, supply and product requirements.

12.7.15.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3644]

Agencies SHOULD require tenderers and contractors to provide information:

- identifying any restrictions on the disclosure, transfer or use of technology arising out of export controls or security arrangements; and
- demonstrating that their supply chains comply with the security of supply requirements set out in the contract documents.

12.7.15.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3646]

Agencies SHOULD request information from contractors and subcontractors to assess their ability to protect information.

12.7.16. Security of Information

12.7.16.R.01. Rationale

After conducting a risk assessment, agencies and suppliers have the means and capability to protect classified information throughout the tendering and contracting process.

12.7.16.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3651]

Agencies MUST include contractual obligations on all contractors and subcontractors to safeguard information throughout the tendering and contracting procedure.

12.7.16.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3653]

Agencies SHOULD include contractual obligations to safeguard information throughout the tendering and contracting procedure.

12.7.16.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3654]

Agencies SHOULD reject contractors and subcontractors where they do not possess the necessary reliability to exclude risks to national security; or have breached obligations relating to security of information during a previous contract in circumstances amounting to grave misconduct.

12.7.17. Continuity of Supply

12.7.17.R.01. Rationale

You can also require suppliers to provide commitments on the continuity of supply. These can include commitments from the supplier to

ensure:

- delivery time;
- stock levels;
- visibility of the supply chain; and
- supply chain resilience.

12.7.17.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3658]

Agencies SHOULD ensure that changes in their supply chain during the performance of the contract will not adversely affect the continuity of supply requirements.

12.7.18. Product Assurance

12.7.18.R.01. Rationale

In addition to the product selection and acquisition guidance in this section, agencies are able to identify and mitigate risks through supply chain visibility, provenance, security validation and pre-installation tests and checks.

12.7.18.R.02. Rationale

Agencies, with the cooperation of their suppliers, should establish the provenance of any products and equipment. Provenance is defined as a record of the origin, history, specification changes and supply path of the products or equipment.

12.7.18.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3669]

Agencies MUST require suppliers and contractors to provide the provenance of any products or equipment.

12.7.18.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3674]

Agencies SHOULD require suppliers and contractors to provide the provenance of any products or equipment.

12.7.19. Security validation

12.7.19.R.01. Rationale

Validation of the performance and security of the equipment is a vital part of the ongoing integrity and security of agency systems. The security design elements and features of the equipment or product will need to be separately considered from any operational drivers. Where compromises in security performance, capability or functionality are apparent, additional risk mitigation, controls and countermeasures may be necessary.

12.7.19.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3691]

Agencies SHOULD validate the security of the equipment against security performance, capability and functionality requirements.

12.7.19.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3693]

Where deficiencies in security performance, capability and functionality are identified, agencies SHOULD implement additional risk mitigation measures.

12.7.20. Pre-Installation Tests and Checks

12.7.20.R.01. Rationale

An essential part of quality and security assurance is the delivery inspection, pre-installation and functional testing of any equipment. In particular, large systems that integrate equipment from different suppliers or that have specialised configuration and operational characteristics may require additional testing to provide assurance that large scale disruptions and security compromises are avoided.

12.7.20.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3698]

Agencies MUST consult with the GCSB on pre-installation, security verification and related tests before the equipment is used in an operational system.

12.7.20.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3700]

Agencies SHOULD inspect equipment on receipt for any obvious signs of tampering, relabelling or damage.

12.7.20.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3701]

Agencies SHOULD inspect equipment on receipt and test the operation before installation.

12.7.20.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3703]

Agencies SHOULD conduct installation verification and related tests before the equipment is used in an operational system.

12.7.20.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3704]

Where any software, firmware or other forms of programme code are required for the initialisation, operation, servicing or maintenance of the equipment, malware checks SHOULD be conducted before the equipment is installed in an operational system.

12.7.21. Equipment Servicing

12.7.21.R.01. Rationale

Some larger or complex systems can have dependencies on particular infrastructures, equipment, software or configurations. Although these types of systems can be less flexible in responding to the rapid changes in technologies, the risks are outweighed by the functionality of the system. In such cases, the continuing support and maintenance of essential components is vital.

12.7.21.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3709]

For equipment that is expected to have an extended operational life in a critical system, and in the event that the supplier is no longer able to

supply these, agencies SHOULD provide for the acquisition of:

- necessary licences;
- information to produce spare parts, components, assemblies;
- testing equipment; and
- technical assistance agreements.

13. Media and IT Equipment Management, Decommissioning and Disposal

13.1. System Decommissioning

Objective

13.1.1. To ensure systems are safely decommissioned and that software, system logic and data are properly transitioned to new systems or archived in accordance with agency, legal and statutory requirements.

Context

Scope

13.1.2. This section discusses the retirement and safe decommissioning of systems. Specific requirements on media handling, usage, sanitisation, destruction and disposal are discussed later in this chapter. System decommissioning is the retirement or termination of a system and its operations. System decommissioning does NOT deal with the theft or loss of equipment.

Definitions

13.1.3. A system decommissioning will have one or more of the following characteristics:

- Ending a capability completely i.e. no migration, redevelopment or new version of a capability occurs;
- Combining parts of existing capabilities services into a new, different system;
- As part of wider redesign, where a capability is no longer provided and is decommissioned or merged with other capabilities or systems.

13.1.4. ICT requirements evolve as business needs change and technology advances. In some cases this will lead to the retirement and decommissioning of obsolete systems or systems surplus to requirements.

13.1.5. Security requires a structured approach to decommissioning in order to cease information system operations in a planned, orderly and secure manner. It is also important that the approach for decommissioning systems is consistent and coordinated. Sanitisation is important to eliminate any remnant data that could be retrieved by unauthorised parties. These procedures include the following:

- A migration plan;
- A decommissioning plan;
- Archiving;
- Safe disposal of equipment and media;
- Robust procedures to manage any residual data and associated risk; and
- Audit and final signoff.

13.1.6. As a final step, a review of the decommissioning should be undertaken to ensure no important elements, data or equipment have been overlooked.

References

13.1.7.

Title	Publisher	Source
Risk Management And Accreditation Of Information Systems Also Released As HMG Infosec Standard No. 2, August 2005	UK Centre for the Protection of National Infrastructure (CPNI)	http://www.cpni.gov.uk/Documents/Publications/2005/2005003-Risk_management.pdf
NIST Special Publication 800-88 Guidelines for Media Sanitization, Rev.1, December, 2014	National Institute of Standards and Technology (NIST), U.S. Department of Commerce	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
Better Practice Checklist – Decommissioning Government Websites, March 2011	Australian Government Information Management Office (AGIMO)	http://agict.gov.au/policy-guides-procurement/better-practice-checklists-guidance/bpc-decommissioning

PSR references

13.1.8. Relevant PSR requirements can be found at:

Reference	Title	Source

PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Supply chain security	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/governance/supply-chain-security/
Managing specific scenarios	Secure your ICT facilities Physical Security for ICT systems	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/

Rationale & Controls

13.1.9. Agency Policy

13.1.9.R.01.   Rationale

Information systems are often supported by service and supply contracts and may also be subject to obligations to provide a service, capability or information. Decommissioning of a system will require the termination of these contracts and service obligations. Other aspects of system decommission may be subject to security, regulatory or legislative requirements. An Agency policy will provide a comprehensive approach to system decommissioning from the inception of a system, thus facilitating the termination of supply contracts and service obligations while managing any risks to the Agency.

13.1.9.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3829]

When the Information System reaches the end of its service life in an organisation, policy and procedures SHOULD be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements.

13.1.10. Migration plan

13.1.10.R.01.   Rationale

Once the decision to decommission a system has been taken, it is important to migrate processes, data, users and licences to replacement systems or to cease activities in an orderly fashion. It is also important to carefully plan the decommissioning process in order to avoid disruption to other systems, ensure business continuity, ensure security, protect privacy and meet any archive and other regulatory and legislative requirements. The basis of a decommissioning plan is a risk assessment.

13.1.10.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3832]

Agencies SHOULD undertake a risk assessment with consideration given to proportionality in respect of:

- scale and impact of the processes;
- data;
- users;
- licences;
- usage agreements; and
- service to be migrated or decommissioned.

13.1.10.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3833]

The risk assessment SHOULD include the following elements:

- Evaluation of the applications inventory and identification of any redundancies;
- Identification of data owners and key stakeholders;
- Identification of types of information (Active or Inactive) processed and stored;
- Identification of software and other (including non-transferable) licences;
- Identification of access rights to be transferred or cancelled;
- Identification of any emanation control equipment or security enhancements;
- Consideration of short and long term reporting requirements;
- Assessment of equipment and hardware for redeployment or disposal;
- Identification of any cloud-based data and services; and
- User re-training.

13.1.10.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3834]
Agencies SHOULD consider the need for a Privacy Impact Assessment.

13.1.10.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3835]
Agencies SHOULD identify relevant service and legal agreements and arrange for their termination.

13.1.11. Decommissioning plan

13.1.11.R.01. Rationale

The decommissioning of a system can be a complex process. A decommissioning plan is an important tool in properly managing the safe decommissioning of a system and in providing reasonable assurance that due process and agency policy has been followed.

13.1.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3838]

The decommissioning plan will be based on the migration plan and SHOULD incorporate the following elements:

- An impact analysis;
- Issue of notification to service providers, users and customers;
- Issue of notification of decommissioning to all relevant interfaces and interconnections;
- Timeframe, plan and schedule;
- Data integrity and validation checks before archiving;
- Transfer or redeployment of equipment and other assets;
- Transfer or cancellation of licences;
- Removal of redundant equipment and software;
- Removal of redundant cables and termination equipment;
- Removal of any emanation control equipment or security enhancements;
- Return or safe disposal of any emanation control equipment or security enhancements;
- Updates to systems configurations (switches, firewalls etc.);
- Equipment and media sanitisation including any cloud-based data & services(discussed later in this chapter);
- Equipment and media disposal (discussed later in this chapter);
- Any legal considerations for supply or service contract terminations;
- Asset register updates; and
- Retraining for, or redeployment of, support staff.

13.1.12. Archiving

13.1.12.R.01. Rationale

Availability and integrity requirements in respect of information may persist for legal and other statutory or compliance reasons and require transfer to other ownership or custodianship for archive purposes. This will also require assurance that the data can continue to be accessed when required (availability) and assurance that it remains unchanged (integrity).

13.1.12.R.02. Rationale

Confidentiality requirements must also be considered. If an information system has been processing sensitive information or contains sensitive security components, which attract special handling requirements, it will require robust purging and overwrites or destruction. There are a number of methods and proprietary products available for such purposes.

13.1.12.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3842]

Agencies SHOULD identify data retention policies, regulation and legislation.

13.1.12.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3844]

Agencies SHOULD ensure adequate system documentation is archived.

13.1.12.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3845]

Agencies SHOULD archive essential software, system logic, system documentation and other system data to allow information to be recovered from archive.

13.1.13. Audit and Final signoff

13.1.13.R.01. Rationale

Update the organisation's tracking and management systems to identify the specific information system components that are being removed from the inventory. To comply with governance, asset management and audit requirements, the Agency's Accreditation Authority will certify that appropriate processes have been followed. This demonstrates good governance and avoids privacy breaches.

13.1.13.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3850]

The Agency's Accreditation Authority SHOULD confirm IA compliance on decommissioning and disposal.

13.1.13.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3852]

The Agency's Accreditation Authority SHOULD confirm secure equipment and media disposal.

13.1.13.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3853]

The Agency's Accreditation Authority SHOULD confirm asset register updates.

13.1.13.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3855]

Once all security relevant activities associated with decommissioning and disposal have been completed and verified, a Security Decommissioning Compliance Certificate SHOULD be issued by the Agency's Accreditation Authority.

13.1.14. Final Review

13.1.14.R.01. Rationale

As a final step, a review of the decommissioning should be undertaken to ensure no important elements, data, equipment, contractual or legislative, obligations have been overlooked.

13.1.14.C.01. Control

Agencies SHOULD undertake a post-decommissioning review.

13.2. Media Handling

Objective

13.2.1. Media is properly classified, labelled and registered in order to clearly indicate the required handling instructions and degree of protection to be applied.

Context

Scope

13.2.2. This section covers information relating to classifying, labelling and registering media. Information relating to classifying and labelling IT equipment can be found in Section 12.3 - Product Classifying and Labelling.

Exceptions for labelling and registering media

13.2.3. Labels are not needed for internally mounted fixed media if the IT equipment containing the media is labelled. Likewise fixed media does not need to be registered if the IT equipment containing the media is registered.

References

13.2.4. Additional information relating to media handling is contained in:

Title	Publisher	Source
ISO/IEC 27001:2013 10.7, Media Handling	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html https://www.standards.govt.nz/

PSR references

13.2.5. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Retire information and assets securely	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/physical-security/understand-the-physical-security-lifecycle/retire-information-and-assets-securely/
Managing specific scenarios	Secure your ICT facilities Physical Security for ICT systems	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/

Rationale & Controls

13.2.6. Reclassification and declassification procedures

13.2.6.R.01. Rationale

When reclassifying or declassifying media the process is based on an assessment of risk, including:

- the classification of the media and associated handling instructions;
- the effectiveness of any sanitisation or destruction procedure used;
- the planned redeployment; and
- the intended destination of the media.

13.2.6.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3896]

Agencies MUST document procedures for the reclassification and declassification of media.

13.2.7. Classifying media storing information

13.2.7.R.01. Rationale

Media that is not classified or not correctly classified may be stored, identified and handled inappropriately.

13.2.7.R.02. Rationale

Incorrect or no classification may result in access by a person or persons without the appropriate security clearance.

13.2.7.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3904]

Agencies MUST classify media to the highest classification of data stored on the media.

13.2.8. Classifying media connected to systems of higher classifications

13.2.8.R.01. Rationale

Unless connected through a data diode or similar infrastructure, there is no guarantee that classified information was not copied to the media while it was connected to a system of higher classification than the classification level of the media itself.

13.2.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3910]

Agencies MUST classify any media connected to a system of a higher classification at the higher system classification until confirmed not to be the case.

13.2.9. Classifying media below that of the system

13.2.9.R.01. Rationale

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 handling instructions of the classification of the information it stores rather than the classification of the system it is connected to or used with.

13.2.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3915]

Agencies intending to classify media below the classification of the system to which it is connected to MUST ensure that:

- the media is read-only;
- the media is inserted into a read-only device; or
- the system has a mechanism through which read-only access can be assured such as approved data diodes, write-blockers or similar infrastructure.

13.2.10. Reclassifying media to a lower classification

13.2.10.R.01. Rationale

Agencies must follow the reclassification process as illustrated in Section 13.6 – Media Disposal.

13.2.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3922]

Agencies wishing to reclassify media to a lower classification MUST ensure that:

- a formal decision is made to reclassify, or redeploy the media; and
- the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed.

13.2.11. Reclassifying media to a higher classification

13.2.11.R.01. Rationale

The media will always need to be protected in accordance with the classification of the information it stores. As such, if the classification of the information on the media changes, then so will the classification of the media.

13.2.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3979]

Agencies MUST reclassify media if:

- information copied onto the media is of a higher classification; or
- information contained on the media is subjected to a classification upgrade.

13.2.12. Labelling media

13.2.12.R.01. Rationale

Labelling helps all personnel to identify the classification of media and ensure that they afford the media the correct protection measures.

13.2.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3982]

Agencies MUST label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.

13.2.12.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3983]

Agencies MUST ensure that the classification of all media is easily visually identifiable.

13.2.12.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:3984]

When using non-textual (colour, symbol) protective markings for operational security reasons, agencies MUST document the labelling scheme and train personnel appropriately.

13.2.12.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3985]

Agencies SHOULD label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.

13.2.13. Labelling sanitised media

13.2.13.R.01. Rationale

It is not possible to effectively sanitise and subsequently reclassify SECRET or TOP SECRET non-volatile media to a classification lower than SECRET. Media of other classifications may be reclassified (See Section 13.6 – Media Disposal).

13.2.13.C.01. ControlSystem Classification(s): Secret, Top Secret; Compliance: MUST [CID:3988]

Agencies MUST label non-volatile media that has been sanitised and reclassified for redeployment with a notice similar to:

Warning: media has been sanitised and reclassified from [classification] to [classification]. Further lowering of classification only via destruction.

13.2.14. Registering media

13.2.14.R.01. Rationale

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.

13.2.14.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3991]

Agencies MUST register all media with a unique identifier in an appropriate register.

13.2.14.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3992]

Agencies SHOULD register all media with a unique identifier in an appropriate register.

13.3. Media Usage

Objective

13.3.1. Media is used with systems in a controlled and accountable manner.

Context

Scope

13.3.2. This section covers information on using media with systems. Further information on using media to transfer data between systems can be found in Section 20.1 - Data Transfers.

PSR references

13.3.3. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Retire information and assets securely	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/physical-security/understand-the-physical-security-lifecycle/retire-information-and-assets-securely/
Managing specific scenarios	Secure your ICT facilities Physical Security for ICT systems	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/secure-your-ict-facilities/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/

Rationale & Controls

13.3.4. Using media with systems

13.3.4.R.01. Rationale

To prevent classified data spills agencies will need to prevent classified media from being connected to, or used with, systems of a lesser classification than the protective marking of the media.

13.3.4.R.02. Rationale

Where media is used for backup purposes, the media will be certified for use at the highest level of classification to be backed-up. Refer also to Section 6.4 – Business Continuity and Disaster Recovery.

13.3.4.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4075]

Agencies MUST NOT use media containing classified information with a system that has a classification lower than the classification of the media.

13.3.5. Storage of media

13.3.5.R.01. Rationale

The security requirements for storage and physical transfer of classified information and IT equipment are specified in the Protective Security Requirements (PSR).

13.3.5.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4078]

Agencies MUST ensure that storage facilities for media containing classified information meets the minimum physical security storage requirements as specified in the Protective Security Requirements (PSR).

13.3.6. Connecting media to systems

13.3.6.R.01. Rationale

Some operating systems provide functionality to automatically execute or read certain types of programs that reside on optical media and flash memory media when connected. 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.

13.3.6.R.02. Rationale

An attacker can create a file on optical media or a connectable device that the operating system will attempt to automatically execute. When the operating system executes the file, it can have the same effect as when a system user explicitly executes malicious code. The operating system executes the file without asking the system user for permission.

13.3.6.R.03. Rationale

Some operating systems will cache information on media to improve performance. As such, inserting media of a higher classification into a system of a lower classification could cause data to be read and saved from the device without user intervention.

13.3.6.R.04. Rationale

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.

13.3.6.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4086]

Agencies MUST disable any automatic execution features within operating systems for connectable devices and media.

13.3.6.C.02. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4089]

Agencies MUST prevent unauthorised media from connecting to a system via the use of:

- device access control software;
- seals;
- physical means; or
- other methods approved by the Accreditation Authority.

13.3.6.C.03. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:4091]

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.

13.3.7. IEEE 1394 (FIREWIRE) interface connections

13.3.7.R.01. Rationale

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 access to the system memory, an attacker can read or write directly to memory.

13.3.7.R.02. Rationale

The best defence against this vulnerability is to disable access to FireWire ports using either software controls or physically disabling the FireWire ports so that devices cannot be connected. Alternatively select equipment without FireWire capability.

13.3.7.C.01. Control **System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST** [CID:4096]

Agencies MUST disable IEEE 1394 interfaces.

13.3.7.C.02. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:4097]

Agencies SHOULD disable IEEE 1394 interfaces.

13.3.8. Transferring media

13.3.8.R.01. Rationale

As media is often transferred through areas not certified to process the level of classified information on the media, additional protection mechanisms need to be implemented.

13.3.8.R.02. Rationale

Applying encryption to media may reduce the requirements for storage and physical transfer as outlined in the PSR. The reduction of any 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.

13.3.8.R.03. Rationale

Further information on reducing storage and physical transfer requirements can be found in Section 17.1 - Cryptographic Fundamentals.

13.3.8.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4102]

Agencies MUST ensure that processes for transferring media containing classified information meets the minimum physical transfer requirements as specified in the PSR.

13.3.8.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4103]

Agencies SHOULD encrypt data stored on media with at least an Approved Cryptographic Algorithm (See Section 17.2 – Approved Cryptographic Algorithms) if it is to be transferred to another area or location.

13.3.9. Using media for data transfers

13.3.9.R.01. Rationale

Agencies transferring data between systems of different security domains or classifications are strongly encouraged to use media such as write-once CDs and DVDs. This will limit opportunity for information from the higher classified systems to be accidently transferred to lower classified systems. This procedure will also make each transfer a single, auditable event.

13.3.9.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4111]

Data transfers between systems of different classification SHOULD be logged in an auditable log or register.

13.3.9.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4114]

Agencies transferring data manually between two systems of different security domains or classifications SHOULD NOT use rewriteable media.

13.3.10. Media in secure areas

13.3.10.R.01. Rationale

Certain types of media including USB, FireWire and eSATA capable devices MUST be disabled or explicitly approved as an exception by the Accreditation Authority for a TOP SECRET environment (the GCSB). This provides an additional level of system user awareness and security.

13.3.10.R.02. Rationale

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.

13.3.10.C.01. Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:4121]

Agencies MUST NOT permit any media that uses external interface connections within a TOP SECRET area without prior written approval from the Accreditation Authority.

13.4. Media and IT Equipment Sanitisation

Objective

13.4.1.   Media and IT Equipment that is to be redeployed or is no longer required is sanitised.

Context

Scope

13.4.2.   This section covers information relating to sanitising media and IT Equipment. Further information relating to sanitising IT equipment can be found in Section 12.6 - Product Sanitisation and Disposal

Definition

13.4.3.   Sanitisation is defined as the process of removal of data and information from the storage device such that data recovery using any known technique or analysis is prevented or made unfeasible. The process includes the removal of all useful data from the storage device, including metadata, as well as the removal of all labels, markings, classifications and activity logs. Methods vary depending upon the nature, technology used and construction of the storage device or equipment and may include degaussing, incineration, shredding, grinding, knurling or embossing and chemical immersion.

Sanitising media and IT Equipment

13.4.4.   The process of sanitisation does not automatically change the classification of the media or IT Equipment, nor does sanitisation necessarily involve the destruction of media or IT Equipment.

Product selection

13.4.5.   Agencies are permitted to use non-evaluated products to sanitise media and IT Equipment. However, the product will still need to meet the specifications and achieve the requirements for sanitising media and IT Equipment as outlined in this section.

Hybrid hard drives, Solid State Drives and Flash Memory Devices

13.4.6.   Hybrid hard drives, solid state drives and flash memory devices are difficult or impossible to sanitise effectively. In most cases safe disposal will require destruction, this includes any equipment with integrated memory capability. The sanitisation and post sanitisation treatment requirements for redeployment of such devices should be carefully observed.

New Zealand Eyes Only (NZEO) Materials

13.4.7.   NZEO endorsed material requires additional protection at every level of classification. In general terms, media and IT Equipment containing NZEO material should be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this section. Media and IT Equipment that has contained NZEO material must not be disposed of to e-recyclers or sold to any third party.

References

13.4.8.

Title	Publisher	Source

Data Remanence in Semiconductor Devices	Peter Gutmann IBM T.J.Watson Research Center	http://www.cypherpunks.to/~peter/usenix01.pdf
RAM testing tool memtest86+		http://www.memtest.org/
MemtestG80 and MemtestCL: Memory Testers for CUDA- and OpenCL-enabled GPUs	Simbios project funded by the National Institutes of Health	https://simtk.org/home/memtest
HDDerase **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.**	A freeware tool developed by the Center for Magnetic Recording Research at the University of California San Diego.	https://cmrr.ucsd.edu/resources/secure-erase.html?_ga=2.231749531.545206853.1522881172-221519987.1522881172
AISEP Evaluated Products List (EPL)	Australasian Information Security Evaluation Program	https://www.cyber.gov.au/publications/evaluated-products-list
ATA Secure Erase	ATA ANSI specifications	http://www.ansi.org/
Secure sanitisation of storage media	NCSC, UK	https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
Reliably Erasing Data From Flash-Based Solid State Drives	Wei, Grupp, Spada and Swanson Department of Computer Science and Engineering, University of California, San Diego	https://www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf
The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE	Edith Cowan University Research Online. Australian Digital Forensics Conference	http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1110&context=adf
2010 Zombie Hard disks - Data from the Living Dead	Edith Cowan University Research Online. Australian Digital Forensics Conference	http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1085&context=adf
The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market	Edith Cowan University Research Online. Australian Digital Forensics Conference	http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1079&context=adf
NSA/CSS Storage Device Declassification Manual December 2007	NSA	http://www.nsa.gov/resources/everyone/Media-destruction/assets/files/storage-device-declassification-manual.pdf

Rationale & Controls

13.4.9. Sanitisation procedures

13.4.9.R.01.   Rationale

Sanitising media and IT Equipment prior to reuse or redeployment in a different environment ensures that classified information is not inadvertently accessed by an unauthorised individual or inadequately protected.

13.4.9.R.02.   Rationale

Using approved sanitisation methods provides a high level of assurance that no remnant data is on the media and IT Equipment.

13.4.9.R.03.   Rationale

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.

13.4.9.R.04.   Rationale

When sanitising media, it is necessary to read back the contents of the media to verify that the overwrite process completed successfully.

13.4.9.R.05.   Rationale

If the sanitising process cannot be successfully completed, destruction will be necessary.

13.4.9.R.06.   Rationale

It is important to note that "factory reset" or similar terms**do not** constitute sanitisation of media.

13.4.9.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4169]

Agencies MUST document conditions and procedures for the sanitisation of media and IT Equipment.

13.4.10. Media that cannot be sanitised

13.4.10.R.01. Rationale

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.

13.4.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4176]

Agencies MUST destroy the following media types **prior to disposal**, as they cannot be effectively sanitised:

- microfiche;
- microfilm;
- optical discs;
- printer ribbons and the impact surface facing the platen;
- programmable read-only memory (PROM, EPROM, EEPROM);
- flash memory and solid state or hybrid data storage devices;
- read-only memory; and
- faulty magnetic media that cannot be successfully sanitised.

13.4.11. Volatile media sanitisation

13.4.11.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to research on recovering the contents of volatile media.

13.4.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4181]

Agencies MUST sanitise volatile media by:

- overwriting all locations of the media with an arbitrary pattern;
- followed by a read back for verification; and
- removing power from the media for at least 10 minutes.

13.4.12. Treatment of volatile media following sanitisation

13.4.12.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

There is published literature that supports the existence of short-term data remanence effects in volatile media. Data retention time is reported to range from 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 data 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 TOP SECRET volatile media MUST always remain at this classification, even after sanitisation.

13.4.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4184]

Following sanitisation, volatile media MUST be treated as indicated in the table below.

Pre-sanitisation classification / Endorsement	Post-sanitisation classification / Endorsement
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED and all lower classifications	UNCLASSIFIED

13.4.13. Non-volatile magnetic media sanitisation

13.4.13.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

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 classified 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.

13.4.13.R.02. Rationale

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 classified 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, and remnant data will exist in these locations. Whilst 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.

13.4.13.R.03. Rationale

The ATA secure erase command is 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.

13.4.13.C.01. Control

    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; or
- 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.

13.4.13.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4190]

    Agencies MUST boot from separate media to the media being sanitised when undertaking sanitisation.

13.4.13.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4191]

    Agencies SHOULD reset the host protected area and drive configuration overlay table of non-volatile magnetic hard disks prior to overwriting the media.

13.4.13.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4192]

    Agencies SHOULD attempt to overwrite the growth defects table (g-list) on non-volatile magnetic hard disks.

13.4.13.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4193]

    Agencies SHOULD use the ATA security erase command for sanitising non-volatile magnetic hard disks instead of using block overwriting software.

13.4.14. Treatment of non-volatile magnetic media following sanitisation

13.4.14.R.01. Rationale

    The following guidance applies in cases where media is to be redeployed.

    Highly classified non-volatile magnetic media cannot be sanitised below its original classification because of concerns with the sanitisation of the host protected area, device configuration overlay table and growth defects table.

13.4.14.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4200]

    Following sanitisation, non-volatile magnetic media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED	UNCLASSIFIED

13.4.15. Non-volatile EPROM media sanitisation

13.4.15.R.01. Rationale

    The following guidance applies in cases where media is to be redeployed.

    When erasing non-volatile EPROM, the manufacturer's specified ultraviolet erasure time is multiplied by a factor of three to provide an additional level of certainty in the process. Verification is provided by read-back.

13.4.15.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4205]

    Agencies MUST sanitise non-volatile EPROM media by erasing as per 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.

13.4.16. Non-volatile EEPROM media sanitisation

13.4.16.R.01. Rationale

    The following guidance applies in cases where media is to be redeployed.

    A single overwrite with a pseudo random pattern is considered good practice for sanitising non-volatile EEPROM media.

13.4.16.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4208]

    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.

13.4.17. Treatment of non-volatile EPROM and EEPROM media following sanitisation

13.4.17.R.01. Rationale

    The following guidance applies in cases where media is to be redeployed.

    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.

13.4.17.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4212]

Following sanitisation, non-volatile EPROM and EEPROM media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED	UNCLASSIFIED

13.4.18. Non-volatile flash memory & FPGA media sanitisation

13.4.18.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

Wear levelling ensures that writes are distributed evenly across each memory block in flash memory. Where possible flash memory SHOULD be overwritten with a pseudo random pattern twice, rather than once, as this helps to ensure that all memory blocks are overwritten during sanitisation. Verification is provided by read-back.

13.4.18.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4215]

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.

13.4.19. Treatment of non-volatile flash memory & FPCA media following sanitisation

13.4.19.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

Owing 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. It is for these reasons that TOP SECRET, SECRET and CONFIDENTIAL flash memory media MUST always remain at their respective classification, even after sanitisation.

13.4.19.R.02. Rationale

Non-volatile flash memory may be redeployed within systems of the same classification only after **all** manufacturer's sanitation procedures have been followed. Destruction and Disposal are covered in sections 13.5 - Media Destruction and 13.6 - Media Disposal respectively.

13.4.19.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4218]

Following sanitisation, non-volatile flash memory media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	CONFIDENTIAL
RESTRICTED	UNCLASSIFIED

13.4.19.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:5426]

Where manufacturer sanitation procedures cannot be determined, items MUST be destroyed.

13.4.20. Sanitising solid state drives

13.4.20.R.01. Rationale

Solid state drives operate a Flash Translation Layer (FTL) to interface with the storage devices – usually NAND chips. Current sanitation techniques address the FTL, rather than destroying the underlying data. It is possible to bypass the FTL, thus accessing the underlying data. With current technology, there is no effective means of sanitising solid state drives.

13.4.20.R.02. Rationale

Solid state drives also use wear equalisation or levelling techniques which can leave data remnants.

13.4.20.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4222]

Solid state drives MUST be destroyed before disposal.

13.4.20.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4223]

Solid state drives MUST be sanitised using ATA Secure Erase sanitation software before redeployment.

13.4.20.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4224]

Solid state drives MUST NOT be redeployed in a lower classification environment.

13.4.21. Hybrid Drives

13.4.21.R.01.   Rationale

Hybrid drives combine solid state memory devices with magnetic disk technologies. As such they are subject to the same difficulties in effective sanitisation as solid state devices.

13.4.21.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4227]

Hybrid drives MUST be treated as solid state drives for sanitisation purposes.

13.4.22. Sanitising media and IT Equipment prior to reuse

13.4.22.R.01.   Rationale

Sanitising media and IT Equipment prior to reuse at the same or higher classification assists with enforcing the need-to-know principle within the agency. This includes any material with an NZEO endorsement.

13.4.22.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4230]

Agencies SHOULD sanitise all media and IT Equipment prior to reuse at the same or higher classification.

13.4.23. Verifying sanitised media and IT Equipment

13.4.23.R.01.   Rationale

Verifying the sanitisation of media and IT Equipment with a different product to the one conducting the sanitisation process provides an independent level of assurance that the sanitisation process was conducted correctly.

13.4.23.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4234]

Agencies SHOULD verify the sanitisation of media and IT Equipment using a different product from the one used to perform the initial sanitisation.

13.5. Media and IT Equipment Destruction

Objective

13.5.1.   Media and IT Equipment that cannot be sanitised is destroyed before disposal.

Context

Scope

13.5.2.   This section covers information relating to the destruction of media and IT equipment. Further information relating to the destruction of IT equipment can be found in Section 12.6 - Product Sanitisation and Disposal

New Zealand Eyes Only (NZEO) Materials

13.5.3.   NZEO endorsed material requires additional protection at every level of classification.

13.5.4.   In general terms, media and IT Equipment containing NZEO material should be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this section. Media and IT Equipment that has contained NZEO material must not be disposed of, to e-recyclers or sold to any third party.

References

13.5.5.   Further references can be found at:

Topic	Publisher	Source
Secure Destruction of Sensitive Items	CPNI	https://www.cpni.gov.uk/secure-destruction

Rationale & Controls

13.5.6.   Destruction procedures

13.5.6.R.01.   Rationale

Documenting procedures for media and IT Equipment destruction will ensure that destruction is carried out in an appropriate and consistent manner within the agency.

13.5.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4270]

Agencies MUST document procedures for the destruction of media and IT Equipment.

13.5.7.   Media and IT Equipment destruction

13.5.7.R.01.   Rationale

The destruction methods given are designed to ensure that recovery of data is impossible or impractical. Health and safety training and the use of safety equipment may be required with these methods.

13.5.7.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4276]

To destroy media and IT Equipment agencies MUST use at least one of the methods shown in the following table.

Item	Destruction methods

	Furnace/ Incinerator	Hammer mill	Disintegrator	Grinder/ Sander	Cutting	Degausser
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
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No
Semi-conductor memory	Yes	Yes	Yes	No	No	No
Other Circuit Boards	Yes	Yes	Yes	No	No	No

13.5.8. Media and IT Equipment destruction equipment

13.5.8.R.01. Rationale

A variety of equipment for media and IT Equipment destruction exists. Evaluated products will provide assurance that the product will be effective. Approved products are discussed in Chapter 12 - Product Security.

13.5.8.R.02. Rationale

Where a product is not an evaluated product or is NOT listed in the PSR. Consult the GCSB for advice.

13.5.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4302]

Agencies MUST employ approved equipment for the purpose of media and IT Equipment destruction.

13.5.8.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4304]

Where agency owned approved destruction equipment is not available agencies MUST use an approved destruction facility for media and IT Equipment destruction.

13.5.9. Storage and handling of media and IT Equipment waste particles

13.5.9.R.01. Rationale

Following destruction, normal accounting and auditing procedures do not apply. As such, it is essential that when an item is recorded as being destroyed, destruction is assured.

13.5.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4343]

Agencies MUST, at minimum, store and handle the resulting waste for all methods, as for the classification given in the table below.

Initial media or IT Equipment classification	Screen aperture size particles can pass through	
	Less than or equal to **3mm** Treat as	Less than or equal to **6mm** Treat as
■ TOP SECRET	UNCLASSIFIED	**RESTRICTED**
■ SECRET	UNCLASSIFIED	**RESTRICTED**
■ CONFIDENTIAL	UNCLASSIFIED	**RESTRICTED**
■ RESTRICTED	UNCLASSIFIED	UNCLASSIFIED

Particle size: measured in any direction, should not exceed stated measurement.

13.5.10. Degaussers

13.5.10.R.01. Rationale

Coercivity varies between media and IT Equipment types and between brands and models of the same type. Care is needed when determining the desired coercivity as 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.

13.5.10.R.02. Rationale

Since 2006 perpendicular magnetic media have become available. Some degaussers are only capable of sanitising longitudinal magnetic media. As such, care needs to be taken to ensure that a suitable degausser is used when sanitising perpendicular magnetic media.

13.5.10.R.03. Rationale

Some degaussers will have product specific requirements. Agencies will need to comply with any directions provided by the GCSB to ensure that degaussers are being used in the correct manner to achieve an effective destruction outcome. Refer also to Chapter 12 - Product Security.

13.5.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4349]

Agencies MUST use a degausser of sufficient field strength for the coercivity of the media and IT Equipment.

13.5.10.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4350]

Agencies MUST use a degausser which has been evaluated as capable for the magnetic orientation (longitudinal or perpendicular) of the media.

13.5.10.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4352]

Agencies MUST comply with product specific directions provided by the manufacturers, along with any provided by the GCSB.

13.5.11. Supervision of destruction

13.5.11.R.01. Rationale

To ensure that classified media and IT Equipment is appropriately destroyed it will need 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. To provide accountability and traceability, a destruction register should be maintained.

13.5.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4357]

Agencies MUST perform the destruction of media and IT Equipment under the supervision of at least one person cleared to the highest classification of the media or IT Equipment being destroyed.

13.5.11.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4358]

Personnel supervising the destruction of media or IT Equipment MUST:

- supervise the handling of the media or IT Equipment to the point of destruction; and
- ensure that the destruction is completed successfully.

13.5.11.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4359]

The Destruction Register SHOULD record:

- Date of destruction;
- Operator and witness;
- Media or IT Equipment classification; and
- Media or IT Equipment type, characteristics and serial number.

13.5.12. Supervision of accountable material destruction

13.5.12.R.01. Rationale

As accountable material is more sensitive than standard classified media and IT Equipment, it needs to be supervised by at least two personnel and have a destruction certificate signed by the personnel supervising the process. This includes any NZEO material.

13.5.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4363]

Agencies MUST perform the destruction of accountable material under the supervision of at least two personnel cleared to the highest classification of the media or IT Equipment being destroyed.

13.5.12.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4364]

Personnel supervising the destruction of accountable media and IT Equipment MUST:

- supervise the handling of the material to the point of destruction;
- ensure that the destruction is completed successfully;
- sign a destruction certificate; and
- complete the relevant entries in the destruction register.

13.5.13. Outsourcing media and IT Equipment destruction

13.5.13.R.01. Rationale

Agencies may wish to outsource media and IT Equipment destruction for efficiency and cost reasons.

13.5.13.C.01. Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:4367]

Agencies MUST NOT outsource the supervision and oversight of the destruction of TOP SECRET or NZEO media and IT Equipment or other accountable material to a non-government entity or organisation.

13.5.13.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4368]

Agencies outsourcing the destruction of media and IT Equipment to a commercial facility MUST use an approved facility and comply with the procedures and instructions in this Chapter.

13.5.14. Transporting media and IT Equipment for offsite destruction

13.5.14.R.01. Rationale

Requirements on the safe handling and physical transfer of media and IT Equipment between agencies or to commercial facilities can be found in the PSR.

13.5.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4371]

Agencies SHOULD sanitise media and IT Equipment prior to transporting it to an offsite location for destruction.

13.6. Media and IT Equipment Disposal

Objective

13.6.1.   Media and IT equipment is declassified and approved by the CISO, or delegate, for release before disposal into the public domain.

Context

Scope

13.6.2.   This section covers information relating to the disposal of media and IT equipment. Further information relating to the disposal of IT equipment can be found in Section 12.6 - Product Sanitisation and Disposal

13.6.3.   NZEO endorsed material requires additional protection at every level of classification.

13.6.4.   In general terms, media and IT equipment containing NZEO material should be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this section. Media and IT equipment that has contained NZEO material must not be disposed of, to e-recyclers or sold to any third party.

13.6.5.   Note the discussion in section 13.4 - Media and IT equipment sanitisation, on the challenges and difficulties in effectively sanitising media of all types.

Rationale & Controls

13.6.6.   Declassification prior to disposal

13.6.6.R.01.   Rationale

Prior to its disposal, media and IT equipment needs to be declassified to ensure that classified information is not accidentally released into the public domain.

13.6.6.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4385]

Agencies MUST declassify all media and IT equipment prior to disposing of it into the public domain.

13.6.6.C.02.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4386]

Media and IT equipment that cannot be effectively sanitised or declassified MUST be destroyed and not released into the public domain.
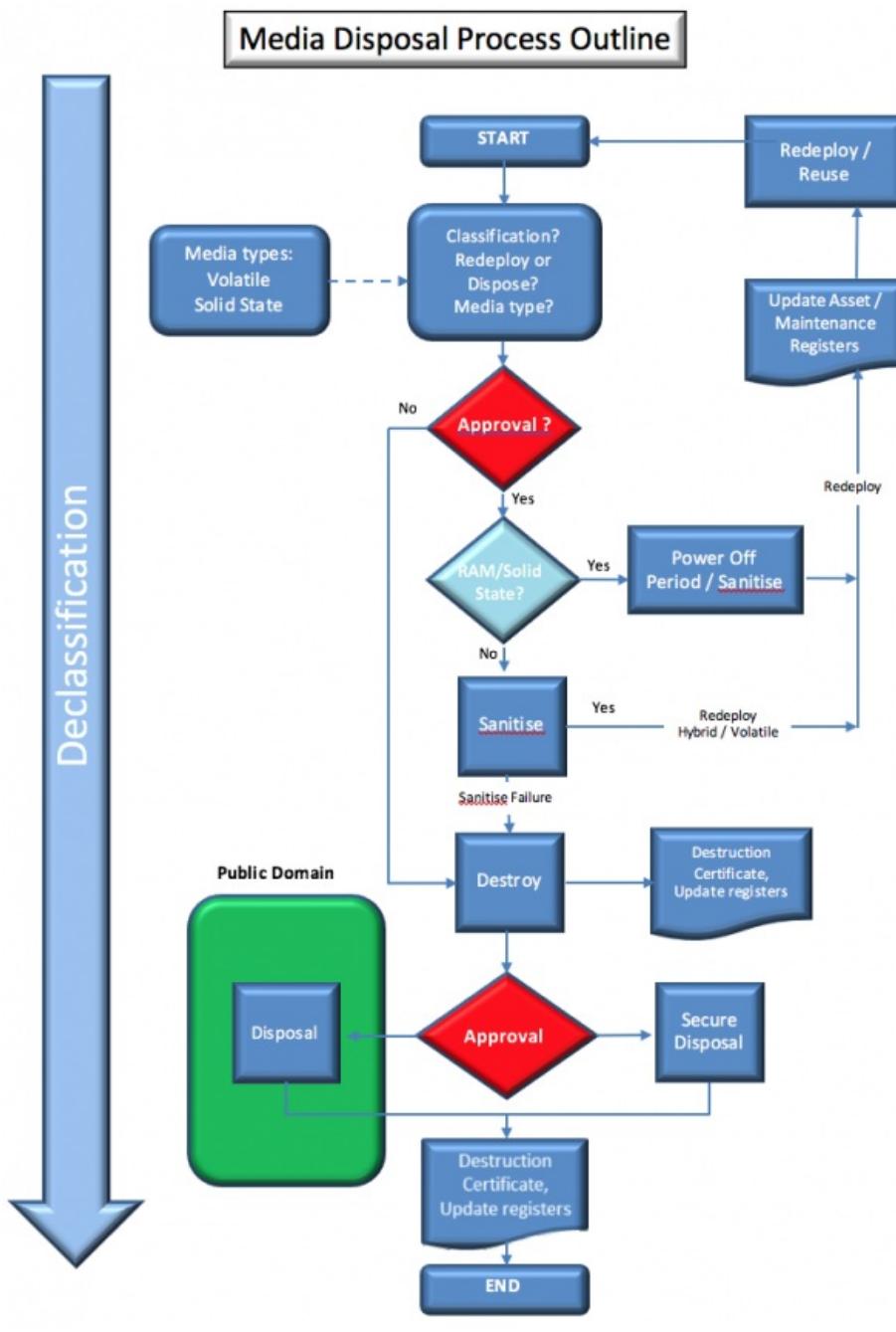
13.6.7.   Disposal procedures

13.6.7.R.01.   Rationale

The following diagram illustrates the mandated disposal process. Note declassification describes the entire process, including any reclassifications, approvals and documentation, before media and media waste can be released into the public domain.

13.6.7.C.01.   ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4389]

Agencies MUST document procedures for the disposal of media and IT equipment.

Media Disposal Process Outline

13.6.8. Declassifying media

13.6.8.R.01. Rationale

The process of reclassifying, sanitising or destroying media does not provide sufficient assurance for media to be declassified and released into the public domain. In order to declassify media, formal administrative approval is required before releasing the media or waste into the public domain.

13.6.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4392]

Agencies declassifying media MUST ensure that:

- the reclassification of all classified information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed; and
- formal approval is granted before the media is released into the public domain.

13.6.9. Disposal of media

13.6.9.R.01. Rationale

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. This can include the removal of labels, markings and serial numbers.

13.6.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4395]

Agencies MUST dispose of media in a manner that does not draw undue attention to its previous classification.

13.6.10. New Zealand Eyes Only (NZEO) Materials

13.6.10.R.01. Rationale

NZEO endorsed material requires additional protection at every level of classification and creates a special case in the destruction and disposal

process.

13.6.10.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4398]

Media and IT equipment that has contained NZEO material MUST be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this chapter.

13.6.10.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4399]

For disposal of all NZEO endorsed materials, an approved destruction facility MUST be used.

13.6.10.C.03. ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:4400]

Media and IT equipment that has contained NZEO material MUST NOT be disposed of via e-recyclers or sold to any third party.

13.6.11. Approved Secure Destruction Facilities

13.6.11.R.01. Rationale

An approved secure destruction facility may be agency-owned or a commercial facility.

13.6.11.R.02. Rationale

A number of regulatory and legislative requirements including those relating to health, safety, environmental protection, hazardous materials handling disposal and export, will have to be met by any such facility.

13.6.11.R.03. Rationale

It may not be economically viable for individual agencies to own and maintain such facilities. In such cases the use of a commercial facility may be the only practical alternative.

13.6.11.R.04. Rationale

To ensure secure destruction facilities have the capability, capacity and equipment to securely destroy media and IT equipment to the specifications detailed in the NZISM, a formal approval is required. An inspection of the facility and any necessary testing of the equipment will determine suitability for operation as a secure destruction facility. If the results of the inspection and testing are satisfactory, a formal approval is issued. Periodic re-inspections are conducted to ensure on-going compliance with the NZISM requirements.

13.6.11.R.05. Rationale

Commercial organisations may apply to the GCSB for approval as a secure destruction facility under the NZISM.

13.6.11.R.06. Rationale

The Director-General of the GCSB will issue such approvals if satisfied that the standards detailed in the NZISM have been satisfactorily been met and can be maintained.

13.6.11.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:5711]

Where agencies establish their own disposal/destruction facilities, these facilities MUST be **approved** by the Director-General GCSB.

13.6.12. Use of Approved Secure Destruction Facilities

13.6.12.R.01. Rationale

Agencies may not have the facilities to securely dispose of media and IT equipment to the specifications detailed in the NZISM (Refer to 13.5.7 Media and IT Equipment Destruction and 13.5.9 Storage and handling of media waste particles). In these circumstances the use of an approved secure disposal or destruction facility (agency owned or a commercial facility) is permitted **provided** all other procedures in this Chapter are followed.

13.6.12.R.02. Rationale

The GCSB maintains a register of approved secure disposal/destruction facilities.

13.6.12.R.03. Rationale

In practical terms this requires tracking, supervision and oversight (witnessed) to the point where the disposal/destruction process is complete. Procedures are detailed in Section 13.5 - Media and IT Equipment Destruction.

13.6.12.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:5716]

Agencies MUST use an **approved** secure disposal/destruction facility for the destruction of media and IT equipment.

14. Software security

14.1. Standard Operating Environments

Objective

14.1.1. Standard Operating Environments (SOE) are hardened in order to minimise attacks and compromise through known vulnerabilities and attack vectors.

Context

Scope

14.1.2. This section covers information on the hardening of software used on workstations and servers on systems within agency control.

Characterisation

14.1.3. Characterisation is a technique used to analyse and record a system's configuration. It is important as it can be used as a baseline to verify the system's integrity at a later date. It is also important that the baseline has high levels of integrity and assurance to avoid reinfecting systems or reintroducing compromises when restoring from baselines.

14.1.4. In virtual environments a baseline is usually a "snapshot" or image take at a point in time. If the image or snapshot is infected, then restoring from that image can result in further compromise. See also Section 22.2 – Virtualisation and 22.3 – Virtual Local Area Networks.

14.1.5. 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; or
- for a Windows system, taking a system difference snapshot.

References

14.1.6. Further references can be found at:

Title	Publisher	Source
ISO/IEC 27001:2013, A.12.4.1 Control of Operational Software	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
ISO/IEC 27001:2013, A.12.6.1 Control of Technical Vulnerabilities	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
Independent testing of different antivirus software and their effectiveness	AV Comparatives	http://www.av-comparatives.org/

PSR references

14.1.7. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Analyse evolving threats and vulnerabilities	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/operate-and-maintain/analyse-evolving-threats-and-vulnerabilities/
Managing specific scenarios	Transacting online with the public	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/transacting-online-with-the-public/

Rationale & Controls

14.1.8. Developing hardened SOEs

14.1.8.R.01. Rationale

Antivirus and anti-malware software, while an important defensive measure, 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.

14.1.8.R.02. Rationale

The use of antivirus and anti-malware software, while adding value to the defence of workstations, cannot be relied solely upon to protect the workstation. As such agencies still need to deploy appropriately hardened SOEs to assist with the protection of workstations against a broader range of security risks.

14.1.8.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1149]

Agencies SHOULD develop a hardened SOE for workstations and servers, covering:

- removal of unneeded software and operating system components;
- removal or disabling of unneeded services, ports and BIOS settings;
- disabling of unused or undesired functionality in software and operating systems;
- implementation of access controls on relevant objects to limit system users and programs to the minimum access required;
- installation of antivirus and anti-malware 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; and
- protection of audit and other logs through the use of a one way pipe to reduce likelihood of compromise key transaction records.

14.1.9. Maintaining hardened SOEs

14.1.9.R.01. Rationale

Whilst 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 are not able to disable or bypass security functionality and antivirus and other security software is appropriately maintained with the latest signatures and updates.

14.1.9.R.02. Rationale

End Point Agents monitor traffic and apply security policies on applications, storage interfaces and data in real-time. Administrators actively block or monitor and log policy breaches. The End Point Agent can also create forensic monitoring to facilitate incident investigation.

14.1.9.R.03. Rationale

End Point Agents can monitor user activity, such as the cut, copy, paste, print, print screen operations and copying data to external drives and other devices. The Agent can then apply policies to limit such activity.

14.1.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1158]

Agencies MUST ensure that for all servers and workstations:

- a technical specification is agreed for each platform with specified controls;
- a standard configuration created and updated for each operating system type and version;
- system users do not have the ability to install or disable software without approval; and
- installed software and operating system patching is up to date.

14.1.9.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1159]

Agencies SHOULD ensure that for all servers and workstations:

- malware detection heuristics are set to a high level;
- malware pattern signatures are checked for updates on at least a daily basis;
- malware pattern signatures are updated as soon as possible after vendors make them available;
- all disks and systems are regularly scanned for malicious code; and
- the use of End Point Agents is considered.

14.1.10. Default passwords and accounts

14.1.10.R.01. Rationale

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.

14.1.10.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1162]

Agencies MUST reduce potential vulnerabilities in their SOEs by:

- removing unused accounts;
- renaming or deleting default accounts; and
- replacing default passwords before or during the installation process.

14.1.10.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1163]

Agencies SHOULD reduce potential vulnerabilities in their SOEs by:

- removing unused accounts;
- renaming or deleting default accounts; and
- replacing default passwords, before or during the installation process.

14.1.11. Server separation

14.1.11.R.01. Rationale

Servers with a high security risk can include Web, email, file, Internet Protocol Telephony (IPT) servers, Mobile Device Manager (MDM) servers and gateway components. It is important to clearly identify all services and connections to design a complete and secure server separation architecture. Refer also to Chapter 19 – Gateway Security.

14.1.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1169]

Where servers with a high security risk have connectivity to unsecure public networks, agencies SHOULD:

- use appropriately designed and configured gateways;
- consider the use of cross-domain solutions;
- segment networks;
- maintain effective functional segregation between servers allowing them to operate independently;
- minimise communications between servers at both the network and file system level as appropriate; and
- limit system users and programs to the minimum access needed to perform their duties.

14.1.12. Characterisation

14.1.12.R.01. Rationale

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. Characterisation 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.

14.1.12.R.02. Rationale

Characterisation is also directly related to business continuity and disaster recovery and is influenced by Business Impact Analyses and Risk Assessments. Grouping elements by business applications and setting priority and criticality of the elements to the business may assist in determining the most appropriate and useful characterisations.

14.1.12.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1185]

Agencies SHOULD:

- characterise all servers whose functions are critical to the agency, and those identified as being at a high security 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 change control process;
- as part of the agency's ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred;
- perform the characterisation from a trusted environment rather than the standard operating system wherever possible; and
- resolve any detected changes in accordance with the agency's information security incident management procedures.

14.1.12.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1189]

Agencies SHOULD use an Approved Cryptographic Algorithm to perform cryptographic checksums for characterisation purposes.

14.1.12.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1190]

Agencies SHOULD consider characterisations in the context of a BCP or DRP and any related Business Impact Analyses and Risk Assessments.

14.1.13. Automated outbound connections by software

14.1.13.R.01. Rationale

Applications that include beaconing functionality include those that initiate a connection to the vendor site over the Internet and inbound remote management.

14.1.13.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1193]

Agencies SHOULD review all software applications to determine whether they attempt to establish any unauthorised or unplanned external connections.

14.1.13.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1194]

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.

14.1.13.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1195]

If automated outbound connection functionality is included, agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.

14.1.14. Knowledge of software used on systems

14.1.14.R.01. Rationale

Information about installed software, that could be disclosed outside the agency, can include:

- user agent on Web requests disclosing the Web browser type;
- network and email client information in email headers; and
- email server software headers.

This information could provide a malicious entity with knowledge of how to tailor attacks to exploit vulnerabilities in the agency's systems.

14.1.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1198]

Agencies SHOULD limit information that could be disclosed outside the agency about what software, and software versions are installed on their systems.

14.2. Application Whitelisting

Objective

14.2.1.   Only approved applications are used on agency controlled systems.

Context

Scope

14.2.2.   This section covers information on the use of technical controls to restrict the specific applications that can be accessed by a user or group of users.

References

14.2.3.   Further information on application whitelisting as implemented by Microsoft can be found at:

Title	Publisher	Source
Using Software Restriction Policies to Protect Against Unauthorized Software	Microsoft	http://technet.microsoft.com/en-us/library/bb457006.aspx
APPLOCKER	Microsoft	https://docs.microsoft.com/en-nz/windows/security/threat-protection/applocker/applocker-overview
Implementing Application Whitelisting January 2018	ASD	http://www.asd.gov.au/publications/protect/Application_Whitelisting.pdf
NIST Special Publication 800-167 - Guide to Application Whitelisting	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf
Application Whitelisting Using Microsoft AppLocker	NSA	https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
Application Whitelisting Explained	CSE	https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsb95-eng_0.pdf
Guidelines for Application Whitelisting in Industrial Control Systems	DHS - The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	Guidelines for Application Whitelisting in Industrial Control Systems

Rationale & Controls

14.2.4. Application whitelisting

14.2.4.R.01. Rationale

Application whitelisting can be an effective mechanism to prevent the successful compromise of an agency system resulting from the exploitation of a vulnerability in an application or the execution of malicious code.

14.2.4.R.02. Rationale

Defining a list of trusted executables, a whitelist, is a practical and secure method of securing a system rather than relying on a list of bad executables (black list) to be prevented from running.

14.2.4.R.03. Rationale

Application whitelisting is considered only one part of a defence-in-depth strategy in order to prevent a successful attack, or to help mitigate consequences arising from an attack.

14.2.4.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1234]

Agencies SHOULD implement application whitelisting as part of the SOE for workstations, servers and any other network device.

14.2.5. System user permissions

14.2.5.R.01. Rationale

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 execute code to this limited set of applications reduces the attack surface of the system.

14.2.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1242]

Agencies MUST ensure that a system user cannot disable the application whitelisting mechanism.

14.2.5.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1246]

Agencies SHOULD prevent a system user from running arbitrary executables.

14.2.5.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:896]

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.

14.2.5.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:898]

Agencies SHOULD ensure that application whitelisting does not replace the antivirus and anti-malware software within a system.

14.2.6. System administrator permissions

14.2.6.R.01. Rationale

Since the consequences of running malicious code as a privileged user are much more severe than an unprivileged user, an application whitelisting implementation should be strictly enforced for system administrators.

14.2.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:907]

Agencies SHOULD ensure that system administrators are not automatically exempt from application whitelisting policy.

14.2.7. Application whitelisting configuration

14.2.7.R.01. Rationale

A decision to execute a routine, application, or other programme should be made based on a validated cryptographic hash as it is more secure than a decision based on the executable's signature, path or parent folder.

14.2.7.R.02. Rationale

In order for application whitelisting to be effective an agency MUST initially gather information on necessary executables and applications in order to ensure that the implementation is fully effective.

14.2.7.R.03. Rationale

Different application whitelisting controls, such as restricting execution based on cryptographic hash, filename, pathname or folder, have various advantages and disadvantages. Agencies need to be aware of this when implementing application whitelisting.

14.2.7.R.04. Rationale

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.

14.2.7.R.05. Rationale

Executables may create multiple processes in the course of execution. These may be identified through exanibation of programme specifications, testing ina "sand-boxed" environment before development and logs of any processes spawned or created.

14.2.7.R.06. Rationale

Spawned processes may behave in ways that can compromise system security, change security settings and modify access permissions. Clearly this can be undesirable behaviour.

14.2.7.R.07. Rationale

Adequate logging information can allow system administrators to further refine the application whitelisting implementation and detect a pattern of deny decisions for a system user.

14.2.7.R.08. Rationale

An example of relevant information that could be included in logs for application whitelisting implementations would be decisions to deny execution incorporating information that would present a reviewer with evidence of misuse.

14.2.7.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:934]

Agencies SHOULD ensure that the default policy is to deny the execution of software.

14.2.7.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:936]

Agencies SHOULD ensure that application whitelisting is used in addition to a strong access control list model and the use of limited privilege accounts.

14.2.7.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:940]

Agencies SHOULD plan and test application whitelisting mechanisms and processes thoroughly prior to implementation.

14.2.7.C.04. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:942]

Agencies SHOULD restrict the decision whether to run an executable based on the following, in the order of preference shown:

1. validates cryptographic hash;

2. executable absolute path;

3. digital signature; and

4. parent folder.

14.2.7.C.05. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:945]

Agencies SHOULD restrict the process creation permissions of any executables which are permitted to run by the application whitelisting controls.

14.2.7.C.06. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:5529]

Agencies SHOULD validate executable behaviour, in particular process creation, permission changes and access control modifications through examination, testing, monitoring and restriction of the permissions.

14.2.7.C.07. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:947]

Logs from the application whitelisting implementation SHOULD include all relevant information.

14.3. Web Applications

Objective

14.3.1. Access to Web content is implemented in a secure and accountable manner.

Context

Scope

14.3.2. This section covers information on Web browsers, plug-ins and active content including the development and implementation of appropriate use policies. The requirements in this section apply equally to the Web accessed via the Internet as well as websites accessed on an agency intranet.

References

14.3.3. A Web whitelisting software application that allows for the management of whitelists can be obtained from:

Title	Publisher	Source
Dynamic Web Whitelisting for Squid	SourceForge	http://whitetrash.sourceforge.net/

14.3.4. Examples of client-side JavaScript controls are available at:

Title	Publisher	Source
NoScript Firefox extension	Inform Action	http://noscript.net

Rationale & Controls

14.3.5.   Web usage policy

14.3.5.R.01.   Rationale

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 development, and awareness raising amongst system users, of a Web usage policy.

14.3.5.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1272]

Agencies MUST develop and implement a policy governing appropriate Web usage.

14.3.6.   Web proxy

14.3.6.R.01.   Rationale

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 agency Web usage policies.

14.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1592]

Agencies SHOULD use a Web proxy for all Web browsing activities.

14.3.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1593]

An agency's Web proxy SHOULD authenticate system users and provide logging that includes at least the following details about websites accessed:

- address (uniform resource locator);
- time/date;
- system user;
- internal IP address; and
- external IP address.

14.3.6.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1594]

Agencies SHOULD NOT permit downloading of executable files from external websites unless there is a demonstrable and approved business requirement.

14.3.7.   Applications and plug-ins

14.3.7.R.01.   Rationale

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.

14.3.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1597]

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

14.3.8.   Inspection of TLS

14.3.8.R.01.   Rationale

As TLS encrypted Web traffic travelling over HTTPS connections can deliver content without any filtering, agencies can reduce this security risk by using TLS inspection so that the Web traffic can be filtered.

14.3.8.R.02.   Rationale

An alternative of using a whitelist for HTTPS websites can allow websites that have a low security risk of delivering malicious code and have a high privacy requirement like Web banking, to continue to have end-to-end encryption.

14.3.8.R.03.   Rationale

It is however, important to note that there are many recorded cases of websites generally considered to be a low security risk that have been compromised.

14.3.8.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1602]

Agencies permitting TLS through their gateways SHOULD implement:

- a solution that decrypts and inspects the TLS traffic as per content filtering requirements; or
- a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked.

14.3.9. Legal advice on the Inspection of TLS traffic

14.3.9.R.01. Rationale

Encrypted TLS traffic may contain personally identifiable information. Agencies should seek legal advice on whether inspecting such traffic is in breach of the Privacy Act or other legislation. User policies should incorporate an explanation of the security drivers and acknowledgement from users on the policy contents and requirements. Refer to Chapter 9 – Personnel Security and Chapter 15 – Email Security.

14.3.9.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1605]

Agencies SHOULD seek legal advice regarding the inspection of encrypted TLS traffic by their gateways.

14.3.10. Whitelisting / Blacklisting websites

14.3.10.R.01. Rationale

Defining a whitelist of permitted websites and blocking all unlisted websites limits one of the most common data delivery and exfiltration techniques used by malicious code. However, if agency personnel have a legitimate requirement to access a numerous and rapidly changing list of websites, agencies will need to consider the practicality and costs of such an implementation. In such cases black listing is a limited but none-the-less effective measure.

14.3.10.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1609]

Agencies SHOULD implement whitelisting for all HTTP traffic being communicated through their gateways.

14.3.10.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1608]

Agencies using a whitelist on their gateways to specify the external addresses, to which encrypted connections are permitted, SHOULD specify whitelist addresses by domain name or IP address.

14.3.10.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1610]

If agencies do not whitelist websites they SHOULD blacklist websites to prevent access to known malicious websites.

14.3.10.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1611]

Agencies blacklisting websites SHOULD update the blacklist on a frequent basis to ensure that it remains effective.

14.3.11. Client-side active content

14.3.11.R.01. Rationale

Software that runs on agency systems SHOULD be controlled by the agency. 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.

14.3.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1614]

Agencies SHOULD block client-side active content, such as Java and ActiveX, which are assessed as having a limited business impact.

14.3.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1615]

Agencies SHOULD:

- use client-side controls that allow JavaScript on a per website basis; and
- add JavaScript functions used only for malicious purposes to the agency Web content filter or IDS/IPS.

14.3.12. Web content filter

14.3.12.R.01. Rationale

Using a Web proxy provides agencies with an opportunity to filter potentially harmful information to system users and their workstations.

14.3.12.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1618]

Agencies SHOULD use the Web proxy to filter content that is potentially harmful to system users and their workstations.

14.3.13. Website Passwords

14.3.13.R.01. Rationale

Some websites require the use of a userID and password as the authentication mechanism. The management of passwords on these websites is often insecure and there are numerous examples of compromises where tens of thousands, and sometimes millions of passwords are compromised in a single incident. Where the same password is used on multiple websites, an incident can potentially compromise the user's account on every website using that password. It is important to treat these websites as insecure and manage passwords appropriately.

14.3.13.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:1621]

Users MUST NOT use agency userid and login passwords as credentials for external websites.

14.3.13.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1622]

Users SHOULD NOT store web site authentication credentials (userID and password) on workstations, remote access devices (such as laptops) or BYO devices.

14.3.13.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1623]

Users SHOULD NOT use the same password for multiple websites.

14.4. Software Application Development

Objective

14.4.1. Secure programming methods and testing are used for application development in order to minimise the number of coding errors and introduction of security vulnerabilities.

Context

Scope

14.4.2. This section covers information relating to the development, upgrade and maintenance of application software used on agency systems.

References

14.4.3. Additional information relating to software development is contained in:

Title	Publisher	Source
ISO/IEC 27001:2013, A.12.5 Security in Development and Support Processes	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
OWASP Secure Coding Practices - Quick Reference Guide	OWASP	https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
Secure Code Review	MITRE Corporation	https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/secure-code-review
Build Security In	DHS – US-CERT	https://www.us-cert.gov/bsi
Application Security - Application Security & Development A To Z	US Defense Information Security Agency (DISA)	http://iase.disa.mil/stigs/app-security/app-security/Pages/index.aspx
Writing Secure Code - Michael Howard and David LeBlanc	Microsoft Press	ISBN Book 978-0-7356-1722-3 ISBN eBook 978-0-7356-9146-9

Rationale & Controls

14.4.4. Software development environments

14.4.4.R.01. Rationale

Recognised good practice segregates development, testing and production environments to limit the spread of malicious code and minimise 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 attacker.

14.4.4.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1635]

Agencies SHOULD ensure that software development environments are configured such that:

- there are at least three separate environments covering:
  - development;
  - testing; and
  - production.

- information flow between the environments is strictly limited according to a defined and documented change policy, with access granted only to system users with a clear business requirement;
- new development and modifications only take place in the development environment; and
- write access to the authoritative source for the software (source libraries & production environment) is disabled.

14.4.5. Secure programming

14.4.5.R.01. Rationale

Designing software to use the lowest privilege level needed to achieve its task will limit the privileges an attacker could gain in the event they subvert the software security.

14.4.5.R.02. Rationale

Validating all inputs will ensure that the input is within expected ranges, reducing the chance that malicious or erroneous input causes unexpected results.

14.4.5.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1639]

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; and
- validating all inputs.

14.4.6. Software testing

14.4.6.R.01. Rationale

Software reviewing and testing will reduce the possibility of introducing vulnerabilities into a production environment.

14.4.6.R.02. Rationale

Using an independent party for software testing will limit any bias that can occur when a developer tests their own software.

14.4.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1643]

Software SHOULD be reviewed or tested for vulnerabilities before it is used in a production environment.

14.4.6.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1644]

Software SHOULD be reviewed or tested by an independent party as well as the developer.

14.4.6.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1645]

Software development SHOULD follow secure coding practices and agency development standards.

14.5. Web Application Development

Objective

14.5.1. Security mechanisms are incorporated into all Web applications by design and implementation.

Context

Scope

14.5.2. This section covers the deployment of agency Web applications and websites.

Protecting Web servers

14.5.3. Even though Web servers may contain only information authorised for release into the public domain, there still remains a need to protect the integrity and availability of the information. As such, Web servers are to be treated in accordance with the requirements of the classification of the system they are connected to.

Web application components

14.5.4. 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 fewer components, however in general there is a presentation layer, application layer and database layer.

References

14.5.5. Further information on Web application security is available from the Open Web Application Security Project at:

Title	Publisher	Source
The Open Web Application Security Project (OWASP) - Reference	OWASP	http://www.owasp.org
NZ Government Web Toolkit	DIA	https://webtoolkit.govt.nz/guidance/security-and-privacy-management/designing-for-security-and-privacy/security-and-privacy-assurance/
Web Design and Applications	W3C	http://www.w3.org/standards/webdesign/
Web Development – Patterns and Practices	Microsoft	https://msdn.microsoft.com/en-us/library/ff921348.aspx

Rationale & Controls

14.5.6. Agency website content

14.5.6.R.01. Rationale

Reviewing active content on agency Web servers will assist in identifying and mitigating information security issues.

14.5.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1661]

Agencies SHOULD review all active content on their Web servers for known information security issues.

14.5.7. Segregation of Web application components

14.5.7.R.01. Rationale

Web applications are typically very exposed services that provide complex interactions with system users. This greatly increases the security risk of being compromised. By segregating components, the impact of potential application flaws or attacks is limited.

14.5.7.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1664]

Agencies SHOULD minimise connectivity and access between each Web application component.

14.5.8. Web applications

14.5.8.R.01. Rationale

The Open Web Application Security Project guide provides a comprehensive resource to consult when developing Web applications.

14.5.8.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1667]

Agencies SHOULD follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services.

15. Email security

15.1. Email Applications

Objective

15.1.1.   Email messages have appropriate protective markings to facilitate the application of handling instructions.

Context

Scope

15.1.2.   This section covers information on email policy and usage as it applies to content and protective markings. Information on email infrastructure is located in Section 15.2 - Email Infrastructure.

Automatically generated emails

15.1.3.   The requirements for emails within this section equally apply to automatically and manually generated emails.

Exceptions for receiving unmarked email messages

15.1.4.   Where an agency receives unmarked non-government emails as part of its business practice the application of protective markings can be automated.

References

15.1.5.   Further references can be found at:

Title	Publisher	Source
NIST publication SP 800-45 v2, Guidelines on Electronic Mail Security	NIST	http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf
Detecting socially engineered emails August 2012	ASD	http://www.asd.gov.au/publications/csocprotect/Socially_Engineered_Email.pdf

PSR references

15.1.6.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV3, GOV4, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Build security awareness Overview of security classifications	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/governance/build-security-awareness/ https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/overview/
Resource centre	Email Fraud: an INFOSEC case study How do I protectively mark or classify a document	https://www.protectivesecurity.govt.nz/resources-centre/case-studies/email-fraud-an-infosec-case-study/ https://www.protectivesecurity.govt.nz/resources-centre/common-questions/classified-material/how-do-i-protectively-mark-or-classify-a-document/

Rationale & Controls

15.1.7.   Email usage policy

15.1.7.R.01.   Rationale

There are many security risks associated with the unsecure nature of email that are often overlooked. Documenting them will inform information owners about these security risks and how they might affect business operations.

15.1.7.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1684]

Agencies MUST develop and implement a policy governing the use of email.

15.1.8.   Email distribution

15.1.8.R.01.   Rationale

Often the membership, clearance level and nationality of members of email distribution lists is unknown. As such, personnel sending sensitive

emails with NZEO or other nationality releasability marked information could be accidentally causing an information security incident by sending such information to distribution lists.

15.1.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1687]

Agencies MUST ensure that emails containing NZEO or other nationality releasability marked information are sent only to named recipients.

15.1.8.C.02. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:1688]

Agencies MUST NOT transmit emails or other documents, containing NZEO or other nationality releasability marks, to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

15.1.9.   Protective marking standard

15.1.9.R.01.   Rationale

Applying markings that reflect the protective requirements of an email informs the recipient on how to appropriately handle the email and any related documents.

15.1.9.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1691]

Agencies SHOULD comply with the national classification system for the application of protective markings.

15.1.10. Marking tools

15.1.10.R.01.   Rationale

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.

15.1.10.R.02.   Rationale

Limiting the protective markings a system user is allowed to choose, to those for which the system is accredited lessens the chance that a system user inadvertently over-classifies an email and reminds them of the maximum classification of information that is permitted on the system.

15.1.10.R.03.   Rationale

Gateway filters usually check only the most recent protective marking. Care MUST be taken when changing protective markings to a classification lower than that of the original email as this can result in emails being forwarded to systems or individuals NOT authorised and cleared to receive them.   The instructions in the classification system on changing classifications MUST be observed to avoid a security breach.

15.1.10.C.01.   Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:1696]

Agencies MUST NOT allow system users to select protective markings that the system has not been accredited to process, store or communicate.

15.1.10.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1697]

Agencies SHOULD NOT allow a protective marking to be inserted into system user generated emails without their intervention.

15.1.10.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1698]

Agencies SHOULD NOT permit 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.

15.1.11. Marking classified and unclassified emails

15.1.11.R.01.   Rationale

As with paper-based information, all electronic-based information should be marked with an appropriate protective marking in accordance with the classification system. This ensures that appropriate security measures are applied to the information and also assists in preventing the inadvertent release of information into the public domain.

15.1.11.R.02.   Rationale

When a protective marking is applied to an email it is important that it reflects the highest classification in the body of the email and any attachments within the email.

15.1.11.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1702]

All classified and unclassified emails MUST have a protective marking.

15.1.11.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1703]

Email protective markings MUST accurately reflect the highest classification of all elements in an email, including any attachments.

15.1.11.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1704]

Agencies SHOULD include protective markings in the email subject line or header to facilitate early identification of the classification.

15.1.12. Emails from outside the government

15.1.12.R.01.   Rationale

If an email is received from outside government the system user has an obligation to determine the appropriate protective measures for the email if it is to be responded to, forwarded or printed.

15.1.12.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:1707]

Where an unmarked email has originated outside the government, the agency MUST assess the information and determine how it is to be handled in accordance with the classification system.

15.1.13. Marking personal emails

15.1.13.R.01. Rationale

Applying protective markings to personal emails may create system overheads and will be misleading.

15.1.13.R.02. Rationale

Personal emails can be marked as "PERSONAL" or "UNOFFICIAL" to avoid confusion with Official or Classified information.

15.1.13.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1711]

Where an email is of a personal nature and does not contain government information, protective markings SHOULD NOT be used.

15.1.14. Receiving unmarked emails

15.1.14.R.01. Rationale

If an email is received from a New Zealand or overseas government agency without a protective marking the system user has an obligation to contact the originator to seek clarification on the appropriate protection measures for the email or follow established protocols and policy for protective markings.

15.1.14.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1714]

Where an unmarked email has originated from a New Zealand or overseas government agency, personnel SHOULD contact the originator to determine how it is to be handled.

15.1.15. Receiving emails with unknown protective markings

15.1.15.R.01. Rationale

If an email is received with a protective marking that the system user is not familiar with they have an obligation to contact the originator to seek clarification on the protective marking and the appropriate protection measures for the email.

15.1.15.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1717]

Where an email is received with an unknown protective marking from a New Zealand or overseas government agency, personnel SHOULD contact the originator to determine appropriate protection measures.

15.1.16. Printing

15.1.16.R.01. Rationale

The PSR requires that paper-based information have the classification of the information placed at the top and bottom of each piece of paper, in CAPITALS and appearing as the first and last item on each page.

15.1.16.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1720]

Agencies SHOULD configure systems so that the protective markings appear at the top and bottom of every page when the email is printed, in CAPITALS and appearing as the first and last item on each page.

15.1.17. Active Web addresses within emails

15.1.17.R.01. Rationale

Spoofed emails often contain an active Web address directing personnel to a malicious website to either elicit information or infect their workstation with malicious code. In order to reduce the success rate of such attacks agencies can choose to educate their personnel to neither send emails with active Web addresses or to click on Web addresses in emails that they receive.

15.1.17.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1723]

Personnel SHOULD NOT send emails that contain active Web addresses or click on active Web addresses within emails they receive.

15.1.18. Awareness of email usage policies

15.1.18.R.01. Rationale

In order to protect information and systems, system users will need to be familiar with email usage policies.

15.1.18.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1726]

Agencies MUST make their system users aware of the agency's email usage policies.

15.1.19. Monitoring email usage

15.1.19.R.01. Rationale

Agencies may choose to monitor compliance with aspects of email usage policies such as attempts to send prohibited file types or executables, attempts to send excessive sized attachments or attempts to send classified information without appropriate protective markings.

15.1.19.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1729]

Agencies SHOULD implement measures to monitor their personnel's compliance with email usage policies.

15.1.19.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1730]

Agencies SHOULD enforce the use of approved government email systems such as SEEMAIL.

15.1.20. Public Web-based email services

15.1.20.R.01. Rationale

Using public Web-based email services may allow personnel to bypass security measures that agencies will have put in place to protect against malicious code or phishing attempts distributed via email. Web based email services may also by-pass agency context filtering mechanisms.

15.1.20.C.01. Control

> Agencies SHOULD NOT allow personnel to use public Web-based email services, for processing, receiving or sending emails or attachments for official business.

15.2. Email Infrastructure

Objective

15.2.1.   Email infrastructure is hardened, email is secured and protective marking of email messages is enforced.

Context

Scope

15.2.2.   This section covers information on email infrastructure security. Information on using email applications can be found in Section 15.1 - Email Applications and Section 9.3 - Using the Internet.

Anti-Spoofing Controls

15.2.3.   Phishing and malware distribution attacks are common internet security threats. To avoid agency domains being used fraudulently (e.g. for spam or spear-phishing), the following should be implemented:

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC) records

15.2.4.   Correct configuration of these features will help other mail servers authenticate the email they receive from your domains. It is important to note that DMARC is designed to protect against direct domain spoofing only. DMARC does not eliminate the need for additional forms of protection and analysis. It does, however, provide a way for participating senders and receivers to coordinate protective activities and streamline security processes.

15.2.5.   It is also important to note that not all mail service providers enable DMARC, substituting the registration of a free email account as a validation of the user's email account instead. In this case the benefits and reporting associated with DMARC are not available.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

Vocabulary

15.2.6.   The terms "none", "reject" and "quarantine" are used to describe DMARC actions based on policy modes. In this usage:

- "none" means no action on the transmission or receipt of the email but continue to collect data and send reports;
- By default, email under a "reject" policy setting is not delivered. "Reject" either:
    - refuses to accept non-compliant email, or
    - initially accepts the non-compliant email but prevents an email reaching the user. The acceptance process can generate a Delivery Status Notification (block/"bounce") or simply delete/drop the email (block/delete);
- "quarantine" prevents an email from reaching the user but safely storing it so it can be accessed if required (a potentially suspicious email and/or attachment subject to additional scrutiny). Quarantined items can be released following a review and release process.

What is DMARC

15.2.7.   Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication policy and reporting protocol that:

- complements and unifies the existing validation checks performed by SPF and DKIM;
- checks the stated origin of inbound emails using a combination of Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM);
- establishes a recipient email response for emails that fail the check;
- requests recipient email services to report email sources and origins;
- provides visibility over potentially illegitimate or fraudulent email.

15.2.8.   DMARC builds on SPF and DKIM protocols, adding links to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, in order to improve and monitor protection of the recipient domain from fraudulent email.

15.2.9.   Most email services will check your DMARC record and send aggregated reports including details of all email the service received from the agency, and its origin. This assists in identifying if an individual within the agency is sending email inappropriately or if the agency domain is being spoofed.

Background, Reference and Implementation Guidance Sources

15.2.10. The IETF published RFC 7489, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)" March 18th, 2015. RFC 7489. This is the principal standards guidance on the implementation and use of DMARC. Further guidance is available from The Global Cyber Alliance (GCA) - see References below.

Using DMARC

15.2.11. By establishing DMARC, SPF, and DKIM records in DNS, it's possible to advise email service providers which servers should be legitimately sending email from the agency's domain, and what action to take with mail received from any other domains.

15.2.12. In support of DMARC agencies **must** publish an SPF and a DKIM record. Agencies must also ensure emails agencies send (including those from third party services that send on behalf of the agency) have a DKIM signature that matches the signature in the DKIM record.

15.2.13. Agencies can choose to quarantine or reject messages that fail checks. More specifically:

- Sender Policy Framework (SPF) is used to specify legitimate locations of servers which can send email for your domain;
- DomainKeys Identified Mail (DKIM) isn't supported by all mail servers, but if it is, it can be used to cryptographically sign outgoing mail sent by your servers to give email service providers further confidence that it's legitimate;
- DMARC is used to inform email service providers what action they should take if SPF or DKIM (or both) validation fails;

- One important aspect of DMARC is the action you ask email service providers to take when SPF or DKIM validation fails:
    - a policy of **p=none** means that they should allow non-compliant emails to be delivered but report the failure to the agency;
    - a policy of **p=quarantine** requests that they mark the email as spam;
    - a policy of **p=reject** requests the email service provider to refuse to deliver the email.

15.2.14. Many organisations start with a policy of **p=none**, then modify the configuration to **p=reject** as confidence is gained in the accuracy of the configuration and in systems performance.

15.2.15. To notify other organisations of the use of DMARC agencies may publish a text record in their DNS similar to the following:

- v=DMARC1;
- p=quarantine;
- pct=100;
- rua=mailto:dmarc@agency.govt.nz (where agency is the name of the respective agency).

15.2.16. This informs email recipients that:

- you have a DMARC policy (v=DMARC1)
- any messages that fail DMARC checks should be treated as spam (p=quarantine)
- they should treat 100% of your messages this way (pct=100)
- they should send reports of email received back to you (rua=mailto:dmarc@agency.govt.nz)

15.2.17. It is not unusual to experience minor errors in syntax or other elements of DMARC configuration when first implementing DMARC. Some discussion on common problems, issues and solutions can be found on the DMARC website (see the References table below).

15.2.18. It is unwise for an agency to attempt to move to full implementation of DMARC until there is certainty that the configuration and implementation are stable and operating as intended. The following implementation outline is recommended by the GCA/DMARC organisation (see References below):

1. Deploy DKIM & SPF;
2. Ensure mailers are correctly aligning the appropriate identifiers;
3. Publish a DMARC record with the "none" flag set for the policies, which requests data reports;
4. Analyse the data and modify mail streams as appropriate; and
5. Modify DMARC policy flags from "none" to "quarantine" to "reject" as experience dictates.

DMARC Reporting

15.2.19. DMARC reporting provides information to assist an agency's IT system and email administrators. It can also provide an email asset inventory as well as providing data on spam, phishing and other email exploitation techniques.

15.2.20. DMARC can be configured to produce an aggregate report and a forensic report. In some cases agencies may also send reports to an external organisation such as a DMARC reporting service or a third-party IT service provider. Discretion should be used when providing such information to third parties in order to maintain security and privacy.

References

15.2.21. Further information on email security is available from the following sources:

Title	Publisher	Source
RFC 3207, SMTP Service Extension for Secure SMTP over Transport Layer Security	IETF	http://www.ietf.org/rfc/rfc3207.txt
RFC 4408, Sender Policy Framework	IETF	http://www.ietf.org/rfc/rfc4408.txt
RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail	IETF	http://www.ietf.org/rfc/rfc4686.txt
RFC 4871, DomainKeys Identified Mail Signatures	IETF	http://www.ietf.org/rfc/rfc4871.txt
RFC 5617, DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)	IETF	https://tools.ietf.org/html/rfc5617
NIST publication SP 800-45 v2, Guidelines on Electronic Mail Security	NIST	http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf
CPA Security Characteristic Desktop Email Encryption Version 1.0	NCSC UK	https://www.ncsc.gov.uk/content/files/protected_files/document_files/CPA%20SC%20Desktop%20Email%20Encryption%20v1-0.pdf
Sender Policy Framework		www.openspf.org
Measuring the Impact of DMARC's Part in Preventing Business Email Compromise	Global Cyber Alliance	https://www.globalcyberalliance.org
DMARC	DMARC	https://dmarc.org/

Common Problems with DMARC Records	DMARC	https://dmarc.org/2016/07/common-problems-with-dmarc-records/
DMARC Reporting: Key Benefits and Takeaways	Global Cyber Alliance	https://dmarc.globalcyberalliance.org/resource/dmarc-reporting-key-benefits-takeaways/
Use DMARC to validate email in Office 365	Microsoft	https://docs.microsoft.com/en-us/office365/securitycompliance/use-dmarc-to-validate-email
Using Multiple signing Algorithms with the ARC (Authenticated Received Chain) Protocol draft-ietf-dmarc-arc-multi-02	IETF	file:///E:/Background/Standards/IETF/draft-ietf-dmarc-arc-multi-02.pdf
RFC 6376 DomainKeys Identified Mail (DKIM) Signatures	IETF	https://tools.ietf.org/html/rfc6376
RFC 7208 Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.	IETF	https://tools.ietf.org/html/rfc7208
RFC 7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC)	IETF	https://tools.ietf.org/html/rfc7489
RFC 7960 Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows	IETF	https://tools.ietf.org/html/rfc7960
RFC 8463 A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)	IETF	https://tools.ietf.org/html/rfc8463
NIST Special Publication SP800-177	NIST	https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-177.pdf
NIST Technical Note 1945 - Email Authentication Mechanisms: DMARC, SPF and DKIM, February 16, 2017	NIST	https://www.nist.gov/publications/email-authentication-mechanisms-dmarc-spf-and-dkim
Email Security and Anti-Spoofing	NCSC, UK	https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing
Phishing Attacks	NCSC, UK	https://www.gov.uk/content/files/phishing_guidance_final.pdf
Domain-based Message Authentication, Reporting and Conformance (DMARC)	NCSC, UK	https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc
Binding Operational Directive BOD-18-01	DHS	https://cyber.dhs.gov/assets/report/bod-18-01.pdf
Malicious Email Mitigation Strategies	ACSC	https://acsc.gov.au/publications/protect/malicious_email_mitigation.htm
Mitigating spoofed emails – Sender Policy Framework explained	ACSC	http://www.asd.gov.au/publications/csocprotect/Spoof_Email_Sender_Policy_Framework.pdf

Rationale & Controls

15.2.22. Domain-based Message Authentication, Reporting and Conformance (DMARC)

15.2.22.R.01. Rationale

Phishing and malware distribution attacks are common internet security threats. To limit the possibility of agency domains being used fraudulently (e.g. for spam or spear-phishing), agencies should implement:

- A Sender Policy Framework (SPF);
- DomainKeys Identified Mail (DKIM); and
- Domain-based Message Authentication, Reporting & Conformance (DMARC) records.

15.2.22.R.02. Rationale

It is important to note that DMARC depends on the proper implementation of both SPF and DKIM. DMARC records are published in the DNS and provide guidance to the email receiver on actions to take when emails received do not conform to the published record.

15.2.22.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6019]

Before implementing DMARC agencies SHOULD:

- Create a DMARC policy;
- List **all** domains, in particular those used for the sending and/or receiving of email;

- Review the configuration of SPF and DKIM for all active domains and all published domains; and
- Establish one or more monitored inboxes to receive DMARC reports.

15.2.22.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6020]

Agencies SHOULD enable DMARC for all email originating from or received by their domain(s), including:

- sending domain owners SHOULD publish a DMARC record with a related DNS entry advising mail receivers of the characteristics of messages purporting to originate from the sender's domain;
- received DMARC messages SHOULD be managed in accordance with the agency's published DMARC policy; and
- agencies SHOULD produce failure reports and aggregate reports according to the agency's DMARC policies.

15.2.22.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6021]

Agencies SHOULD review DMARC reports on a regular basis and address any identified anomalies or security issues.

15.2.23. Filtering suspicious emails and attachments

15.2.23.R.01. Rationale

The intent of blocking specific types of emails is to reduce the likelihood of phishing emails and emails or attachments containing malicious code entering the agency's networks.

15.2.23.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1745]

Agencies SHOULD configure the following gateway filters:

- inbound and outbound email, including any attachments, that contain:
  - malicious code;
  - content in conflict with the agency's email policy;
  - content that cannot be identified;
  - blacklisted or unauthorised filetypes; and

- 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; and
- all emails arriving via an external connection where the source address uses an internal agency domain name.

15.2.24. Active web addresses (URL) embedded in emails

15.2.24.R.01. Rationale

Spoofed emails often contain an active (embedded) email address directing users to a malicious website in order to infect the workstation or agency systems with malicious code.

15.2.24.R.02. Rationale

An effective defence is to strip and replace active addresses and hyperlinks with text only versions.

15.2.24.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1749]

Email servers SHOULD be configured to strip active addresses and URL's and replace them with text only versions.

15.2.25. Preventing unmarked or inappropriately marked emails

15.2.25.R.01. Rationale

Unmarked or inappropriately marked emails can be blocked at two points, the workstation or the email server. The email server is often the preferred location to block emails as it is a single location under the control of system administrators that can enforce the requirement for the entire network. In addition email servers can apply controls for emails generated by applications.

15.2.25.R.02. Rationale

Whilst blocking at the email server is considered the most appropriate control there is an advantage in also blocking at the workstation. This approach adds an extra layer of security and will also reduce the likelihood of a data spill occurring on the email server.

15.2.25.R.03. Rationale

For classified systems is it important to note that all emails containing classified information MUST be protectively marked. This requirement is outlined in Section 15.1 - Email Applications.

15.2.25.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1754]

Agencies MUST prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server, originating workstation or both.

15.2.25.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1755]

Agencies MUST enforce protective marking of emails so that checking and filtering can take place.

15.2.25.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1756]

Agencies SHOULD enforce protective marking of emails so that checking and filtering can take place.

15.2.26. Blocking of outbound emails

15.2.26.R.01. Rationale

Blocking an outbound email with a valid protective marking or endorsement (e.g. NZEO) that indicates the email exceeds the classification of

the communication path, stops data spills.

15.2.26.R.02. Rationale

Agencies may remove protective markings from emails destined for private citizens and businesses once they have been approved for release from the agency's gateways.

15.2.26.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1760]

Agencies MUST configure systems to block any outbound emails with a protective marking or endorsement indicating that the content of the email exceeds the classification of the communication path.

15.2.26.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1761]

Agencies SHOULD configure systems to log every occurrence of a blocked email.

15.2.27. Blocking of inbound emails

15.2.27.R.01. Rationale

Blocking an inbound email with a valid protective marking that indicates the email or its attachment exceeds the classification the receiving system is accredited to process will prevent a data spill from occurring on the receiving system.

15.2.27.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1764]

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.

15.2.27.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1765]

Agencies SHOULD notify the intended recipient of any blocked emails.

15.2.28. Undeliverable messages

15.2.28.R.01. Rationale

Undeliverable or "bounce" emails are commonly sent by email servers to the original sender when the email cannot be delivered, often because the destination address is invalid. Because of the common spamming practice of spoofing sender addresses, this can result in a large amount of bounce emails being sent to an innocent third party. Sending bounces only to senders that can be verified via the Sender Policy Framework (SPF) or other trusted means avoids contributing to this problem and allows other government agencies and trusted parties to receive legitimate bounce messages. See also 15.2.15 - Sender Policy Framework.

15.2.28.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1768]

Agencies SHOULD send notification of undeliverable, bounced or blocked emails to senders that can be verified via SPF or other trusted means.

15.2.29. Automatic forwarding of emails

15.2.29.R.01. Rationale

Unsecured automatic forwarding of emails can pose a serious risk to the unauthorised disclosure of classified information, for example, a system user may set up a server-side rule to automatically forward all emails to a personal email account. This can result in classified emails being forwarded to the personal email account.

15.2.29.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1771]

Agencies MUST ensure that the requirements for blocking unmarked and outbound emails are also applied to automatically forwarded emails.

15.2.30. Open relay email servers

15.2.30.R.01. Rationale

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 to send emails through the server.

15.2.30.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1774]

Agencies SHOULD disable open email relaying so that email servers will only relay messages destined for the agency's domain(s) and those originating from within that domain.

15.2.31. Email server maintenance activities

15.2.31.R.01. Rationale

Email servers perform a critical business function for many agencies; as such it is important that agencies perform regular email server auditing, security reviews and vulnerability analysis activities.

15.2.31.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1777]

Agencies SHOULD perform regular email server auditing, security reviews and vulnerability analysis activities.

15.2.32. Centralised email gateways

15.2.32.R.01. Rationale

Without a centralised email gateway it is exceptionally difficult to deploy Sender Policy Framework (SPF), DomainKeys Identified Mail (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 with out-of-date blacklists and content filtering.

15.2.32.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1780]

Where an agency has system users that send email from outside the agency's network, an authenticated and encrypted channel MUST be

configured to allow email to be sent via the centralised email gateway.

15.2.32.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1781]

Agencies SHOULD route email through a centralised email gateway.

15.2.32.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1782]

Where backup or alternative email gateways are in place, additional email gateways SHOULD be maintained at the same standard as the primary email gateway.

15.2.33. Transport Layer Security (TLS)

15.2.33.R.01. Rationale

Email can be intercepted anywhere between the originating email server and the destination email server. Email transport between organisations and agencies is usually over the internet or other unsecured public infrastructure so it is important that email interception is carefully managed and suitable controls applied. One effective measure is to use TLS to encrypt the email traffic **between email servers**.

15.2.33.R.02. Rationale

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

15.2.33.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1786]

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.

15.2.33.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1787]

Agencies SHOULD implement TLS between email servers where significant volumes of classified information are passed via email to other agencies.

15.2.34. Sender Policy Framework (SPF)

15.2.34.R.01. Rationale

The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery.
An SPF-protected domain is less attractive to spammers and phishers because the forged e-mails are more likely to be caught in spam filters which check the SPF record. Because an SPF-protected domain is less attractive as a spoofed address, it is less likely to be blacklisted by spam filters and so is less disruptive to email traffic.

15.2.34.R.02. Rationale

Having a proper Sender Policy Framework (SPF) record increases the chances people will get emails you send. Without one, your email has a greater chance of being marked as Spam.

15.2.34.R.03. Rationale

SPF and alternatives such as Sender ID aid 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 mail from a specific domain. If the email server that transmitted the email is not in the list, the verification fails (there are a number of different fail types available).

15.2.34.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1792]

Agencies MUST:

- specify mail servers using SPF or Sender ID; and
- mark, block or identify incoming emails that fail SPF checks for notification to the email recipient.

15.2.34.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1793]

Agencies SHOULD:

- use a hard fail SPF record when specifying email servers; and
- use SPF or Sender ID to verify the authenticity of incoming emails.

15.2.34.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1794]

Agencies SHOULD refer to the SPF recommendations in IETF's RFC 4408.

15.2.35. DomainKeys Identified Mail (DKIM)

15.2.35.R.01. Rationale

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 doesn't match the signed content of the email the verification fails.

15.2.35.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1798]

Agencies SHOULD enable DKIM signing on all email originating from their domain.

15.2.35.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1797]

Agencies SHOULD use DKIM in conjunction with SPF.

15.2.35.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1799]

Agencies SHOULD verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures.

15.2.35.C.04. Control**System Classification(s): All Classifications; Compliance: SHOULD** [CID:1800]

Where agencies operate email distribution list software used by external senders, agencies SHOULD configure the software so that it does not impair the validity of the sender's DKIM signature.

16. Access Control and Passwords

16.1. Identification, Authentication and Passwords

Objective

16.1.1. Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems.

Context

Scope

16.1.2. This section provides information on the identification and authentication of all system users.

16.1.3. Access Control is any mechanism by which an individual, system or application grants or revokes the right to access some location, system, data, or perform some action. Access Control must be supported by an appropriate organisational policy.

16.1.4. In this context a user is a real person. Machine or device to device communication and interaction will also require authentication. It is important to note, however, that the usual mechanisms applied to real persons cannot always be used in device to device authentication, for example, biometrics cannot be used.

16.1.5. In Information Technology, a user will usually register a person's identity supported by some evidence of identity (EoI). This will be accompanied by an authority or approval to access information, usually from a manager or other executive. The authentication system will then issue credentials, usually user ID and password, but may also include tokens or use biometrics. The credentials are the means by which a user (a person) accesses an information technology system and are verified each time a user logs onto a system.

16.1.6. Access Control systems manage access rights, including:

- Physical access to locations;
- File system permissions, including physical documents and files, such as create, read, edit or delete data;
- Program permissions, such as the right to execute a programme;
- Data rights, such as the right to retrieve, print or update information in a database.

Methods for user identification and authentication

16.1.7. Authentication is the process by which a claimed identity is verified and access permissions are confirmed before access is granted.

16.1.8. User authentication can be achieved by various means, including biometrics, cryptographic tokens, software tokens, passphrases, passwords and smartcards. Where this manual refers to passwords it equally applies to passphrases.

16.1.9. Authentication mechanisms are invariably described in terms of factors of authentication as follows:

1. Something you have (preferably NOT the device itself but a SEPARATE authentication device such as a token, RFID card or smartcard). This is also known as the *possession* factor;

2. Something you know such as a PIN, One-Time Password (OTP), reusable password, pattern or other component of a standard authentication mechanism. This is also described as the *knowledge* factor;

3. Something you are (biometrics of various types). This is also described as the *inherence* factor.

16.1.10. Commonly used two factor authentication schemes are combinations of physical presence, a token and a PIN/Password. Biometrics are less commonly used on mobile or remote systems.

Software Tokens

16.1.11. Software Tokens, Soft Tokens or "softokens" are typically applications that run on mobile devices such as smart phones, tablets, laptops other workstations. They are sometimes also known as "virtual tokens". When soft tokens are used the device itself then becomes the "possession factor". Functionality may include:

- Transfer between devices by the user.
- Use of Quick Response (QR) codes to facilitate deployment.
- Manages international time zones changes when travelling.

16.1.12. The soft token (secret) is vulnerable to any attacker that can gain full access to the device through theft, loss or download of malware. This is not as secure as a *separate* hardware token which is more resistant to attack and tampering.

Passwords and Password storage

16.1.13. Password length and composition (character type) has been found to be a primary factor in characterizing password strength [Strength][Composition]. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.

16.1.14. The minimum password length that should be required depends to a large extent on the threat model being addressed. Online attacks where the attacker attempts to log in by guessing the password can be mitigated by limiting the rate of login attempts permitted. In order to prevent an attacker (or a persistent claimant with poor typing skills) from easily inflicting a denial-of-service attack on the subscriber by making many incorrect guesses, passwords need to be complex enough that the rate limiting does not occur after a modest number of erroneous attempts, but does occur before there

is a significant chance of a successful guess.

16.1.15. Offline attacks are sometimes possible when one or more hashed passwords are obtained by the attacker through a database breach. The ability of the attacker to determine one or more users' passwords depends on the way in which the password is stored. Commomly, passwords are salted with a random value and hashed, preferably using a computationally expensive algorithm. Even with such measures, the current ability of attackers to compute many billions of hashes per second with no rate limiting requires passwords intended to resist such attacks to be orders of magnitude more complex than those that are expected to resist only online attacks.

16.1.16. Users should be encouraged to make their passwords as lengthy as they want, within reason. A reasonable upper limit is 64 characters.

16.1.17. Since the size of a hashed password is independent of its length, there is no reason not to permit the use of lengthy passwords (or passphrases) if the user wishes. Extremely long passwords (perhaps megabytes in length) could conceivably require excessive processing time to hash, so it is reasonable to have some limit.

Password Character Set Limitations

16.1.18. Limitations set on credential or password length or on the use of special characters can facilitate brute-force attacks.

16.1.19. A brute-force attack is a trial-and-error method used to discover information such as a user password, a personal identification number (PIN), or to decrypt encrypted data. Automation can be used to generate a large number of consecutive guesses. Similar methods are used by security analysts to test an organisation's system security, often described as penetration testing.

16.1.20. Organisations should not permit the use of short or no-length passwords, restrict the use of character sets or apply encoding restrictions on entry or storage of credentials.

16.1.21. Password length, character variation and use of symbols, numbers and special characters including emoticons will increase the resistance of hash values to attack. These practices will assist in limiting a variety of malicious attacks on IT systems.

Hashing

16.1.22. Hashing is a one-way function where data is mapped to a fixed-length value. It also protects a password by producing ciphertext. Contrast hashing with encryption is a two-way function where the data can be encrypted and decrypted.

16.1.23. In general, applications use secure hashing algorithms for:

- Password Protection;
- Integrity checking: e.g. a tamper-evident seal for a file (checksum);
- Authentication: e.g. Digital signatures, Hashed Message Authentication Codes (HMAC) and pseudo-random number generation (PRNG).

16.1.24. Very large passwords can create system performance issues and choke points. Password hashing reduces all passwords to a fixed length, improving efficiency and reducing the volume of credential traffic.

16.1.25. Approved hash functions have the following characteristics:

- **One-way**: It is computationally infeasible to find any input that maps to any pre-specified output; and
- **Collision Resistant**: It is computationally infeasible to find any two distinct inputs that map to the same output.

Refer also to section 17.4 - Transport Layer Security.

Salting

16.1.26. Refer to 17.2.13 for discussion on the use of salts; and 17.2.25 for the related controls.

Key Stretching

16.1.27. Key stretching is a technique of slowing the hash function as a means of discouraging attacks (making the time spent not worthwhile while increasing the length of the detection window). Typically this is achieved through a high iteration count in the hashing process, in some cases as high as 10,000 iterations. It is important to note the stretching of the key does not alter the entropy (randomness) of the key-space, rather it complicates the method of computing the stretched key.

However note the time versus security trade-off here as key stretching comes at the cost of more time spent in validating user connection requests. This is particularly apparent for transactional or high user-volume websites and networks with large numbers of users.

16.1.28. However, note the time versus security trade off here as key stretching comes at the cost of more time spent in validating user connection requests. This is particularly apparent for transactional or high user-volume websites and networks with large numbers of users.

References

16.1.29. Additional information relating to Access Control and User Authentication can be found at:

Title	Publisher	Source
ISO/IEC 27001:2013, Section 9 Access Control	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
RFC 8492 Secure Password Ciphersuites for Transport Layer Security (TLS) FEB 2019	IETF	https://tools.ietf.org/html/rfc8492
Evidence of Identity	DIA	http://www.dia.govt.nz/DIAWebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument

The NZ Government Authentication Standard	GCDO	http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/
The NZ Government Authentication Standard Appendix A – Definitions	GCDO	http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/guide-authentication-standards-online-services/appendix-def
Special Publication 800-63-2 – August 2013 Electronic Authentication Guideline	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0	IETF	https://tools.ietf.org/pdf/rfc2898.pdf
RFC 8018 PKCS #5: Password-Based Cryptography Specification Version 2.1	IETF	https://tools.ietf.org/pdf/rfc8018.pdf
NIST Special Publication 800-63-3 series - Digital Identity Guidelines	NIST	https://pages.nist.gov/800-63-3/
NIST Special Publication 800-106 Randomized Hashing for Digital Signatures	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-106.pdf
NIST Special Publication 800-107 Revision 1 Recommendation for Applications Using Approved Hash Algorithms	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf
NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Application	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf
The academic paper The Adoption of Single Sign-On and Multifactor Authentication in Organisations – A Critical Evaluation Using TOE Framework Issues in Informing Science and Information Technology Volume 7, 2010	Issues in Informing Science and Information Technology (IISIT)	http://iisit.org/Vol7/IISITv7p161-189DCosta788.pdf
Multi-factor Authentication January 2012	ASD	http://www.asd.gov.au/publications/csocprotect/Multi_Factor_Authentication.pdf
Mitigating the use of stolen credentials to access agency information – August 2012	ASD	http://www.asd.gov.au/publications/csocprotect/Stolen_Credentials.pdf
NIST Special Publication 800-53, Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Establishing Security Best Practices in Access Control	Security Research Labs	www.git-security.com/file/track/5743/1
Windows Server - Interactive logon: Do not display last user name	Microsoft Technet	https://technet.microsoft.com/en-us/library/jj852247.aspx
Windows Server: Network access: Do not allow storage of passwords and credentials for network authentication	Microsoft Technet	https://technet.microsoft.com/en-us/library/jj852185.aspx

PSR references

16.1.30. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV5, GOV6, GOV7, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PERSEC1, PERSEC2, PERSEC3, PERSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/

PSR content protocols	Management protocol for information security Management protocol for personnel security Management Protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Security zones Handling requirements for protectively marked information and equipment Supply chain security Understand the physical security lifecycle	https://www.protectivesecurity.govt.nz/security-zones/ https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/governance/supply-chain-security/ https://www.protectivesecurity.govt.nz/physical-security/understand-the-physical-security-lifecycle/
Managing specific scenarios	Mobile and remote working Working away from the office	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/working-away-from-your-office/

Rationale & Controls

16.1.31. Policies and procedures

16.1.31.R.01. Rationale

Developing policies and procedures will ensure consistency in identification, authentication and authorisation, across agency systems and with relevant standards. Refer also to Section 16.4 – Privileged Access Management.

16.1.31.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1827]

Agencies MUST:

- develop, implement and maintain a set of policies and procedures covering all system users':
  - identification;
  - authentication;
  - authorisation;
  - privileged access identification and management; and
- make their system users aware of the agency's policies and procedures.

16.1.32. System user identification

16.1.32.R.01. Rationale

Having uniquely identifiable system users ensures accountability.

16.1.32.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1829]

Agencies MUST ensure that all system users are:

- uniquely identifiable; and
- authenticated on each occasion that access is granted to a system.

16.1.33. Shared accounts

16.1.33.R.01. Rationale

Sharing passwords and UserIDs (credentials) may be convenient but invariably hampers efforts to identify a specific user and attribute actions to a specific person or system. While agencies and users find convenience in sharing credentials, doing so is highly risky. Shared credentials can defeat accountability and the attribution and non-repudiation principles of access control. This is particularly important where administrative access to networks and servers or access to classified information is provided through shared credentials.

16.1.33.C.01. Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:1832]

Agencies MUST NOT use shared credentials to access accounts.

16.1.33.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1833]

Agencies SHOULD NOT use shared credentials to access accounts.

16.1.34. System user identification for shared accounts

16.1.34.R.01. Rationale

Agencies may have a compelling business reason for the use of shared accounts. These may include Anonymous, Guest and Temporary Employee (such relieving a receptionist) credentials. It may not be possible to attribute the use of such accounts to a specific person.

16.1.34.R.02. Rationale

As shared accounts are non user-specific, agencies will 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.

16.1.34.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1837]

If agencies choose to allow shared, non user-specific accounts they MUST ensure that an independent means of determining the identification of the system user is implemented.

16.1.35. Methods for system user identification and authentication

16.1.35.R.01. Rationale

A personal identification number is typically short in length and employs a small character set, making it susceptible to brute force attacks.

16.1.35.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:1840]

Agencies MUST NOT use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system.

16.1.35.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1841]

Agencies SHOULD ensure that they combine the use of multiple methods when identifying and authenticating system users.

16.1.36. Protecting stored authentication information

16.1.36.R.01. Rationale

Limiting the storage of unprotected authentication information reduces the possibility of an attacker finding and using the information to access a system under the guise of a valid system user.

16.1.36.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:1844]

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.

16.1.37. Protecting authentication data in transit

16.1.37.R.01. Rationale

Secure transmission of authentication information will reduce the risk of interception and subsequent use of the authentication information by an attacker to access a system under the guise of a valid system user.

16.1.37.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1847]

Agencies MUST ensure that system authentication data is protected when in transit on agency networks or All-of-Government systems.

16.1.38. Hashing

16.1.38.R.01. Rationale

Hashing is a means of protecting stored passwords or other authentication data by cryptographically converting the password to fixed length ciphertext. This protects against incidents where an unsanctioned copy of the password or authentication database has been made, exported or the database otherwise compromised. Approved cryptographic protocols are discussed in Chapter 17 - Cryptography. See also section 17.2 - Approved Cryptographic Algorithms for discussion on the use of salts to strengthen the cryptographic resistance of a hash.

16.1.38.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6553]

Password and other authentication data SHOULD be hashed before storage using an approved cryptographic protocol and algorithm.

16.1.39. Identification of foreign nationals

16.1.39.R.01. Rationale

Where systems contain NZEO or other nationalities releasability marked or protectively marked information, and foreign nationals have access to such systems, it is important that agencies implement appropriate security measures to assist in identifying users that are foreign nationals. Such measures will assist in preventing the release of sensitive information to those not authorised to access it.

16.1.39.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1850]

Where systems contain NZEO or other nationalities releasability marked or protectively marked information, agencies MUST provide a mechanism that allows system users and processes to identify users who are foreign nationals, including seconded foreign nationals.

16.1.39.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1851]

Agencies using NZEO systems SHOULD ensure that identification includes specific nationality for all foreign nationals, including seconded foreign nationals.

16.1.40. Password selection policy

16.1.40.R.01. Rationale

Passwords are the primary authentication mechanism for almost all information systems and are fundamental part of access and authentication processes and mechanisms. While there are some limitations in the use of passwords, they remain the most cost effective means available with current technology.

16.1.40.R.02. Rationale

Passwords are subject to three principal groups of risks:

1. Intentional password sharing;
2. Password theft, loss or compromise; and
3. Password guessing and cracking.

16.1.40.R.03.

Associated with these risk groups are four principal methods of attacking passwords:

1. Interactive attempts including password guessing, brute force attacks or some knowledge of the user or agency.

2. Obtaining the password through social engineering or phishing.

3. Compromising the password through oversight, observation, use of keyloggers, cameras etc.

4. Cracking through network traffic interception, misconfiguration, malware, data capture etc. For example a simple eight-letter password can today be brute-forced in minutes by software freely available on the Internet.

16.1.40.R.04.   Rationale

Password controls are designed to manage these risks and attack methods using the controls specified in this section. For example, passwords with at least ten characters utilising upper and lower case, numbers and special characters have a much greater resistance to brute force attacks. When use in combination with controls such as password history and regular password change, passwords can present high resistance to known attack methods.

16.1.40.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1857]

Agencies MUST implement a password policy enforcing:

- a minimum password length of ten characters, consisting of at least three of the following character sets:
  - lowercase characters (a-z);
  - uppercase characters (A-Z);
  - digits (0-9); and
  - punctuation and special characters.

16.1.40.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1858]

Agencies SHOULD implement a password policy enforcing either:

- a minimum password length of 16 characters with no complexity requirement; or
- a minimum password length of ten characters, consisting of at least three of the following character sets:
  - lowercase characters (a-z);
  - uppercase characters (A-Z);
  - digits (0-9); and
  - punctuation and special characters.

16.1.41. Password management

16.1.41.R.01.   Rationale

Changing a password at least every 90 days will limit the time period in which a disclosed password could be used by an unauthorised system user.

16.1.41.R.02.   Rationale

Preventing a system user from changing their password more than once a day will stop the system user from immediately changing their password back to their old password.

16.1.41.R.03.   Rationale

Checking passwords for compliance with the password selection policy will allow system administrators to detect unsafe password selection and ensure that the system user changes it.

16.1.41.R.04.   Rationale

Requiring a system user to change a password on account reset will ensure that the system user has a password known only to that user and is more easily remembered.

16.1.41.R.05.   Rationale

Disallowing predictable reset passwords will reduce the security risk of brute force attacks and password guessing attacks.

16.1.41.R.06.   Rationale

Using different passwords when resetting multiple accounts will prevent a system user whose account has been recently reset from logging into another such account.

16.1.41.R.07.   Rationale

Disallowing passwords from being reused within eight changes will prevent a system user from cycling between a small subset of passwords.

16.1.41.R.08.   Rationale

Disallowing sequential passwords will reduce the security risk of an attacker easily guessing a system user's next password based on their knowledge of the system user's previous password.

16.1.41.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1868]

Agencies MUST:

- ensure that 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; and
- force the system user to change an expired password on initial logon or if reset.

16.1.41.C.02. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:1869]

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; and
- allow system users to use sequential passwords.

16.1.41.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1870]

Agencies SHOULD:

- ensure that 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; and
- force the system user to change an expired password on initial logon or if the password is reset.

16.1.41.C.04. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1871]

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; and
- allow system users to use sequential passwords.

16.1.42. Resetting passwords

16.1.42.R.01. Rationale

To reduce the likelihood of social engineering attacks aimed at service desks, agencies will 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 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; or
- establishing their identity by responding correctly to a number of questions before resetting their own password.

16.1.42.R.02. Rationale

Issuing complex reset passwords maintains the security of the user account during the reset process. This can also present an opportunity to demonstrate the selection of strong passwords.

16.1.42.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1875]

Agencies MUST ensure system users provide sufficient evidence to verify their identity when requesting a password reset for their system account.

16.1.43. Password authentication

16.1.43.R.01. Rationale

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.

16.1.43.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1878]

Agencies SHOULD disable LAN Manager for password authentication on workstations and servers.

16.1.44. Session termination

16.1.44.R.01. Rationale

Developing a policy to automatically logout and shutdown workstations after an appropriate time of inactivity will assist in preventing the compromise of an unattended workstation that contains classified or sensitive information. Such a policy will also reduce the power consumption requirements of the agency during non-operational hours.

16.1.44.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1881]

Agencies SHOULD develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity.

16.1.45. Session and screen locking

16.1.45.R.01. Rationale

Screen and session locking will prevent access to an unattended workstation.

16.1.45.R.02. Rationale

Ensuring that the screen does not appear to be turned off while in the locked state will prevent system users from forgetting they are still logged in and will prevent other system users from mistakenly thinking there is a problem with a workstation and resetting it.

16.1.45.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1885]

Agencies MUST:

- configure systems with a session or screen lock;
- configure the lock to activate:
    - after a maximum of 10 minutes of system user inactivity; or
    - if manually activated by the system user;
- configure the lock to completely conceal all information on the screen;
- ensure that 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; and
- deny system users the ability to disable the locking mechanism.

16.1.45.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1886]

Agencies SHOULD:

- configure systems with a session or screen lock;
- configure the lock to activate:
    - after a maximum of 15 minutes of system user inactivity; or
    - if manually activated by the system user;
- configure the lock to completely conceal all information on the screen;
- ensure that 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; and
- deny system users the ability to disable the locking mechanism.

16.1.46. Suspension of access

16.1.46.R.01. Rationale

Locking a system user account after a specified number of failed logon attempts will reduce the risk of brute force attacks.

16.1.46.R.02. Rationale

Removing a system user account when it is no longer required will prevent personnel from accessing their old account and reduce the number of accounts that an attacker can target.

16.1.46.R.03. Rationale

Suspending inactive accounts after a specified number of days will reduce the number of accounts that an attacker can target.

16.1.46.R.04. Rationale

Investigating repeated account lockouts will reduce the security risk of any ongoing brute force logon attempts and allow security management to act accordingly.

16.1.46.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1892]

Agencies MUST:

- Record all successful and failed logon attempts;
- lock system user accounts after three 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; and
- remove or suspend inactive accounts after a specified number of days.

16.1.46.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1893]

Agencies SHOULD:

- lock system user accounts after three 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; and
- remove or suspend inactive accounts after a specified number of days.

16.1.47. Investigating repeated account lockouts

16.1.47.R.01. Rationale

Repeated account lockouts may be an indication of malicious activity being directed towards compromising a particular account.

16.1.47.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:1896]

Agencies SHOULD ensure that repeated account lockouts are investigated before reauthorising access.

16.1.48. Logon banner

16.1.48.R.01. Rationale

A logon banner for a system serves to remind system users of their responsibilities when using the system. It may also be described as a "Splash Screen" or "User Consent Screen".

16.1.48.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1899]

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.

16.1.48.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1900]

Agencies SHOULD seek legal advice on the exact wording of logon banners.

16.1.48.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1901]

Agency logon banners SHOULD cover issues such as:

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

16.1.49. Displaying when a system user last logged in

16.1.49.R.01. Rationale

Displaying when a system user has last logged onto a system will assist system users in identifying 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 for investigation.

16.1.49.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1904]

Agencies SHOULD configure systems to display the date and time of the system user's previous login during the login process.

16.1.50. Display of Last User Logged on

16.1.50.R.01. Rationale

Agency systems that process or store sensitive information, have monitors displayed in unsecured locations, or are remotely accessed, revealing logged on user's full names or domain account names presents a number of risks. These include user spoofing (user name is now known), presentation of a target of opportunity for unsecured workstations and a potential privacy breach. These risks are higher on shared workstations, such as Internet access workstations.

16.1.50.R.02. Rationale

In Windows and some other systems it is possible that individuals with administrator access can identify last logged information through access to Local Group Policy. This level of access must be carefully controlled and monitored.

16.1.50.R.03. Rationale

Some systems may cache credentials on any workstation or other parts of the system. Caching is frequently found where workstations, laptops or mobile devices require domain credentials when disconnected from the domain. This practice can pose some risk and recommended practice is to disable credential caching except where specifically required for operational purposes.

16.1.50.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1909]

Agencies SHOULD NOT permit the display of last logged on username, credentials or other identifying details.

16.1.50.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1910]

Agencies SHOULD NOT permit the caching of credentials unless specifically required.

16.2. System Access and Passwords

Objective

16.2.1. Access to information on systems is controlled in accordance with agency policy and this manual.

Context

Scope

16.2.2. This section covers information on accessing systems for all system users. Additional information on privileged users can be found in Section 16.3 - Privileged Access and additional information on security clearance, briefing and authorisation requirements can be found in Section 9.2 - Authorisations, Security Clearances and Briefings.

Rationale & Controls

16.2.3.   Access from foreign controlled systems and facilities

16.2.3.R.01. Rationale

If a New Zealand system is to be accessed overseas it will need to be from at least a facility owned by a country that New Zealand has a multilateral or bilateral agreement with. NZEO systems can be accessed only from facilities under the sole control of the government of New Zealand and by New Zealand citizens.

| 16.2.3.C.01. | ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:1920] |

Agencies MUST NOT allow access to NZEO information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.

| 16.2.3.C.02. | ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1921] |

Unless a multilateral or bilateral security agreement is in place, agencies SHOULD NOT allow access to classified information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.

16.2.4. Enforcing authorisations on systems

| 16.2.4.R.01. | Rationale |

Enforcing authorisations of system users through the use of access controls on a system will assist in enforcing the need-to-know principle.

| 16.2.4.C.01. | ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1924] |

Agencies MUST have authorisation of system users enforced by access controls.

16.2.5. Protecting compartmented information on systems

| 16.2.5.R.01. | Rationale |

Compartmented information is particularly sensitive and as such extra measures need to be put in place on systems to restrict access to those with sufficient authorisation, briefings and a demonstrated need-to-know or need- to access.

| 16.2.5.C.01. | ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:1927] |

Agencies MUST restrict access to compartmented information. Such restriction MUST be enforced by the system.

16.2.6. Developing an access control list

| 16.2.6.R.01. | Rationale |

A process is described for developing an access control list to assist agencies in the consistent development of access control lists for their systems.

| 16.2.6.C.01. | ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:1930] |

Agencies SHOULD 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	Obtain agreement from system owners.
4	Establish groups encompassing all system users based on similar functions or security objectives.
5	Determine the group owner or manager for each group of system users.
6	Determine the degree of access to the resource for each system user group.
7	Decide on the level of access for security administration, based on the internal security policy.
8	Identify any classification, protective markings and releasability indicators, (such as NZEO or compartment information).

16.3. Privileged User Access

Objective

16.3.1. <u>only</u>   Trrusted personnel are granted privileged access to systems.

Context

Scope

16.3.2. This section covers information relating specifically to personnel that are granted privileged access to systems. Refer also to Section 16.4 – Privileged Access Management.

Privileged access

16.3.3. Within this section, privileged access is considered to be access which can give a system user:

- 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 all data, files and accounts used by other system users, including backups and media; or
- special access for troubleshooting the system.

References

16.3.4.   Additional information relating to privileged and system accounts, including monitoring, is contained in:

Title	Publisher	Source
ISO/IEC 27001:2013, A.11.2.2 Privilege Management	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
NZISM – Section 6.3 Change Management	GCSB	NZISM – Section 6.3 Change Management
Restricting administrative privileges	ASD	http://www.asd.gov.au/publications/protect/Restricting_Admin_Privileges.pdf
DNSSEC Practice Statement	NZ Registry Services	http://www.nzrs.net.nz

Rationale & Controls

16.3.5.   Use of privileged accounts

16.3.5.R.01.   Rationale

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, information security incidents, or system breaches.

16.3.5.R.02.   Rationale

Privileged access rights allow for system wide changes to be made and as such an appropriate and effective mechanism to log privileged users and strong change management practices will provide greater accountability and auditing capability.

16.3.5.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:1945]

Agencies MUST:

- ensure strong change management practices are implemented;
- ensure that the use of privileged accounts is controlled and accountable;
- ensure that system administrators are assigned and consistently use, an individual account for the performance of their administration tasks;
- keep privileged accounts to a minimum; and
- allow the use of privileged accounts for administrative work only.

16.3.5.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1946]

Agencies SHOULD:

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

16.3.6.   Privileged system access by foreign nationals

16.3.6.R.01.   Rationale

As privileged users may 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.

16.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:1949]

Agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate NZEO information.

16.3.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1950]

Agencies SHOULD NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate classified information.

16.3.7.   Security clearances for privileged users

16.3.7.R.01.   Rationale

When frequent data transfers occur between systems of different classifications, having privileged users from the lesser system cleared to the classification of the higher system will assist in any actions that need to be taken resulting from any data spill.

16.3.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1953]

Agencies involved in frequent transfers of data from another system to their system with a lesser classification SHOULD clear at least one privileged user to the classification of the higher system.

16.4. Privileged Access Management

Objective

16.4.1. To ensure Privileged Access Management (PAM) is incorporated into IT Governance and that privileged accounts are managed in accordance with agency's PAM policy.

Context

Scope

16.4.2. This section provides information and guidance on the establishment and operation of an agency's Privileged Access Management policy and control mechanisms. This is sometimes also described as Privileged Account Management. In the context of this section the terms are synonymous.

16.4.3. Reference to other sections in this document is essential. In particular:

- 3.5   System Users;
- 5.1   Documentation Fundamentals;
- 6.3   Change Management;
- 9.1   Information Security Awareness and Training;
- 16.1   Identification, Authentication and Passwords;
- 16.2   System Access and Passwords;
- 16.3   Privileged User Access;
- 16.7   Multi-Factor Authentication.

Background

16.4.4. **Privileged Access Management (PAM)** – sometimes also described as Privileged Account Management, refers to a set of processes and tools for granting, controlling, monitoring, and auditing privileged access.

16.4.5. A **Privileged Account** is a user account with high levels of access to systems, devices and data. Privileged accounts may, for example, be able to install or remove software, delete data, upgrade operating systems, or modify system or application configurations. They may also have access to data that is not normally accessible to standard users.

16.4.6. Privileged Accounts invariably have direct or indirect access to most or all IT assets of an agency or organisation. When used improperly or maliciously, privileged accounts represent a significant security threat to operations, often exposing sensitive data, impeding operations or damaging IT systems. Any compromise of these accounts is, therefore, a significant business, operational and reputational risk.

16.4.7. Risks associated with privileged accounts have increased in recent years with the expansion of endpoints and use of new technologies including Cloud, Internet of Things (IoT) and the rapid and significant increase in remote and work from home following the onset of the COVID-19 pandemic.

16.4.8. Managing, controlling, monitoring and reviewing privileged access is fundamental to mitigating the risks posed by insider and external threats, privilege escalation threats, preventing unauthorised data access and data breaches, and meeting compliance requirements.

16.4.9. There are many types of privileged access including:

- **Root, Domain** and other **Administrator** accounts are typically used for installing, updating and removing software, changing configurations and administering system passwords.
- **Service Accounts,** which may include local or domain accounts, are typically used for running processes, such as web servers, database servers, and application servers. These may also include the ability to change passwords.
- **Emergency Accounts,** sometimes referred to as "DRP", "firecall" or "breakglass" accounts. While access to emergency accounts normally requires managerial approval as a security measure, they are typically an inefficient manual process with limited auditability.
- **System or Application Accounts** are characteristically used by devices and systems for running operating system components and owning related files.

16.4.10. Traditional administrative or management solutions are typically based on strong password management. Modern systems, especially in a cloud environment, require a more structured and robust means of access control and management. This should include the use of Multi-Factor Authentication (See Section 16.7 - Multi-factor Authentication) to provide access to Privileged Accounts.

16.4.11. In secure environments, privileged accounts should be reserved for network and system administrators to manage the access to and oversight of sensitive information and resources in support of normal agency or organisational operations.

16.4.12. The characteristics and capability of privileged accounts are described at 16.3.3. It is important to note that systems themselves, as well as human users, may have privileged account access. As such it is important to clearly and individually identify all real persons, systems and devices with privileged account access.

16.4.13. Access accounts or channels may have the following characteristics:

- Regular access channels—protected channels that are subject to standard IT controls;
- Privileged access channels (PACs)— channels that might circumvent regular controls but are deemed necessary and legitimate operational channels for reasons of practicality or cost;
- Unintended channels not demanded by any technical or business requirement and represent a vulnerability.

Attacks on Privileged Accounts

16.4.14. Privileged accounts frequently allow unrestricted access the IT infrastructure, often including data residing on those systems. The very high level of access and capability associated with privileged accounts makes them a prime target for external attackers and malicious insiders. A compromise of a privileged account can be extremely damaging and may even cripple systems, such as in ransomware attacks.

16.4.15. Compromised privileged accounts represent one of the largest security vulnerabilities an organisation can face today. A compromise will allow attackers to take full control of an organisation's IT infrastructure, disable security controls, steal confidential information, commit financial fraud and disrupt operations. Stolen, abused or misused privileged credentials are identified in a very high proportion of successful breaches.

16.4.16. Common attack methods may include:

- Probes and scans;
- endpoint targeting;
- System and design vulnerability exploitation;
- Social engineering (including phishing, email spoofing, etc); and
- Malware implants.

Governance and Control

16.4.17. Privileged Accounts are frequently used to deploy and maintain IT systems and necessarily exist in nearly every connected device, server, database, and application. Privileged Accounts may extend beyond an agency-controlled IT infrastructure to include, for example, employee-managed corporate social media accounts. Most agencies and other organisations can typically have many more privileged accounts than employees, sometimes as many as two or three times the number of employees. It is not unusual for some privileged accounts to be unidentified, overlooked, unmanaged, and therefore unprotected.

16.4.18. Governance ensures that privileged accounts are properly approved, controlled, monitored and decommissioned throughout their entire lifecycle. A PAM Policy defines the roles, policies and mechanisms for access requests, as well as the workflow for privileged access approvals and delivery. Monitoring and auditing ensure that account permissions and usage remain appropriate over time. PAM governance is a fundamental part of IT Governance as it can influence other IT security systems, such as identity and access management systems.

16.4.19. In order to support strong IT Governance, it is vital that security efforts are coordinated and technology investment managed. This includes the integration of PAM into the Information Security Policy, Systems Architecture, IT Security Strategy and Risk Management Plan. The sensitivity of data and operations should be assessed by undertaking an impact assessment.

16.4.20. Underpinning any PAM is the principle of enforcement of least privilege. This is defined as the minimisation of access rights and permissions for users, accounts, applications, systems, devices and computing processes to the absolute minimum necessary in order to perform routine, authorised activities and maintain the safe and secure operation of agency or organisational systems.

16.4.21. Enforcing the principle of least privilege assists agencies in minimising their systems attack surface, supporting audit and compliance though improved visibility. This also can reduce risk, complexity, and costs for agencies.

16.4.22. Provision of unnecessary system privileges or data access rights will magnify the impact of misuse or compromise of that users account and can even be devastating. Account privileges should be established to provide a reasonable but minimal level of system privileges and rights needed in order to support the purpose and role. The granting of elevated or excessive system privileges should be carefully controlled and managed.

16.4.23. Risks associated with access to privileged accounts include:

- Misuse of privileges;
- Increased attacker capability;
- Circumventing established security and oversight controls;
- Severe system disruption or failure; and
- Significant data compromise and/or loss.

16.4.24. The principles of PAM controls are to:

- Establish and maintain an inventory of privileged accounts;
- Assess the risk(s) of each privileged access channel;
- Enforce the principle of least privilege;
- Use two-factor or Multi-Factor Authentication for access to Privileged Accounts;
- Minimise access to only essential activities;
- Minimise the number of privileged access channels;
- Ensure each channel and user can be uniquely identified (prevent or minimise sharing of credentials, particularly with accounts such as "root" or "admin");
- Ensure operational systems have access to compiled code only;
- Ensure source code is created, managed and stored on non-operational systems only;
- Restrict access to source code (deny-by-default);
- Log all access to source code including the detection, evaluation, recording and termination of privileged access channels;
- Ensure all logs are periodically reviewed;
- Ensure strong and strict change control procedures are implemented;
- Ensure the authorisation, activation and deactivation of privileged access channels is strictly enforced; and
- Regularly audit and review PAM controls.

16.4.25. It is also important to define all privileged accounts used by an agency or by other organisations, particularly where outsource arrangements are in place. It is fundamental for robust security to identify and record the business functions, related data, systems and access privileges. This is particularly important for agencies that create, store and process classified data.

16.4.26. Without a comprehensive privileged accounts inventory, agencies and other organisations may overlook "backdoor" accounts which allow users to bypass proper controls and auditing. These may have been created during system development, by malicious insiders or by external attackers. Such unregistered accounts may be undetected for months or even years and can create a means of unauthorised and unmonitored access. Such accounts may also be used to erase activity logs to avoid detection.

16.4.27. A privileged access inventory should include a description of the IT system, information asset, privilege description, users and risk classification. This is essential information for assessing risk, the determining of controls and for identifying and managing use and misuse. Of note are:

- Local or Domain Server Admin accounts;
- Domain Admin accounts that typically control Active Directory users;

- System Admin accounts that manage databases;
- Root accounts that manage Unix/Linux platforms;
- Accounts that run and manage Windows applications, services, and scheduled tasks;
- IIS application pools (.NET applications);
- Networking equipment accounts that give access to firewalls, routers, switches, session border controllers, gateways and other similar devices, whether physical or virtual.

16.4.28. Privileged Access Management systems provide many of the capabilities and controls briefly described above and can facilitate PAM, as well as supporting strong IT Governance.

References

16.4.29. Additional information relating to Privileged Account and access management, including some policy examples, can be found at:

Title	Publisher	Source
ISO/IEC 27001:2019 – Annex A.9.1 – Access Control Policy	ISO/IEC/ Standards NZ	https://www.iso.org
Restricting Administrative Privileges	Australian Cyber Security Centre (ACSC)	https://www.cyber.gov.au/publications/restricting-administrative-privileges
Managing user privileges	NCSC - UK	https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/managing-user-privileges
NIST Special Publication 800-123 - Guide to General Server Security	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf
Capability Framework for Privileged Access Management	ISACA	https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/capability-framework-for-privileged-access-management
Securing privileged access	Microsoft	https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access
Privileged Account Management - Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.	MITRE Corporation	https://attack.mitre.org/mitigations/M1026/
Security Standard - Privileged User Access Controls SS-001 (part 2)	UK Department of Works & Pensions	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/703042/dwp-ss001-part-2-security-standard-privileged-user-access-controls.pdf
Management of Privileged Accounts Policy, ICT Document No. WhoG-118	ACT Government	https://www.cmtedd.act.gov.au/__data/assets/pdf_file/0007/1134880/Management-of-Privileged-Accounts-Policy.pdf

Rationale & Controls

16.4.30. Policy Creation and Implementation

16.4.30.R.01. Rationale

The requirement for an agency security policy is discussed and described in **Chapter 5 – Information Security Documentation**. A fundamental part of any security policy is the inclusion of requirements for the treatment of Privileged Accounts. This is most conveniently contained in a Privileged Access Management (PAM) section within the agency's security policy. A PAM policy is a fundamental component of an agency's IT Governance.

16.4.30.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6835]

Agencies MUST establish a Privileged Access Management (PAM) policy.

16.4.30.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:6836]

Within the context of agency operations, the agency's PAM policy MUST define:

- a privileged account; and
- privileged access.

16.4.30.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:6837]

Agencies MUST manage Privileged Accounts in accordance with the Agency's PAM Policy.

16.4.31. The Principle of Least Privilege

16.4.31.R.01. Rationale

The Principle of Least Privilege is discussed in the **Context** part of this section. This principle stipulates the minimisation of access rights and permissions for users, accounts, applications, systems, devices and computing processes to the absolute minimum necessary in order to

perform routine, authorised activities and maintain the safe and secure operation of agency or organisational systems.

16.4.31.R.02. Rationale

The implementation of the Principle of Least Privilege requires limitations on the number and use of privileged accounts as well as minimising the numbers of users with these privileges.

16.4.31.R.03. Rationale

The use of Privileged Access should also follow the principle of least privilege by ensuring the use of two-factor or Multi-Factor Authentication for access to Privileged Accounts and ensuring that only activity requiring such access is undertaken. Refer to Section 16.7 – Multi-Factor Authentication. User accounts without Privileged Access should be used for all other activities. Refer to Section 16.3 – Privileged User Access.

16.4.31.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6842]

Agencies MUST apply the Principle of Least Privilege when developing and implementing a PrivilegedAccess Management (PAM) policy.

16.4.31.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6843]

Agencies SHOULD use two-factor or Multi-Factor Authentication to allow access to Privileged Accounts

16.4.32. Strong Authentication process

16.4.32.R.01. Rationale

The approval and authorisation process for the granting of privileged access should be based on the requirement to manage and protect agency systems and assets or as an operational necessity only.

16.4.32.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6846]

As part of a Privileged Access Management (PAM) policy, agencies MUST establish and implement a strong approval and authorisation process before any privileged access credentials are issued.

16.4.32.C.02. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:6847]

Privileged Access credentials MUST NOT be issued until approval has been formally granted.

16.4.33. Suspension and Revocation of Privileged Access Credentials

16.4.33.R.01. Rationale

Because Privileged Accounts have high levels of trust associated with the issue of related credentials, any indication that credentials or accounts have been compromised or that credentials have been misused must be immediately investigated. Actions may include the immediate suspension of credentials. Revocation may follow depending on the outcome of the investigation.

16.4.33.R.02. Rationale

The privileged access credentials for staff and other users (such as authorised contractors) should be suspended or revoked as part of exit procedures when staff leave the agency and when other users no longer undertake duties for the agency. This ensures the numbers of credentials are controlled, credentials are revoked when no longer required for operational purposes and that the risk of unauthorised activities and access is minimised.

16.4.33.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6852]

Agencies MUST establish robust credential suspension and revocation procedures as part of the agency'sPrivileged Access Management (PAM) policy.

16.4.34. Privileged Account, Rights and Credential Inventory

16.4.34.R.01. Rationale

Account and credential "sprawl" is a continuing challenge as the number of users constantly changes and the number and variety of devices evolves and grows. The growing use of the Internet of Things (IoT) is a good example of this. A primary tool in the management and containment of sprawl is the creation and maintenance of an inventory of privileged accounts and the access rights and credential associated with those accounts together with a process of continuous discovery. This will assist in curbing privileged account sprawl, identifying potential insider abuse, and exposing external threats and malicious activity.

16.4.34.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6855]

Agencies MUST create and maintain a comprehensive inventory of privileged accounts and the associated access rights and credentials.

16.4.35. Monitoring and Review

16.4.35.R.01. Rationale

Privileged Accounts have high levels of system and data access and are a "high value target" for malicious cyber-attacks and insider misuse. Access to privileged accounts can be extremely damaging to systems and can cause data and privacy breaches as well as data loss.

16.4.35.R.02. Rationale

A key control in the ongoing integrity of privileged accounts and their associated credentials is a robust system of monitoring and review in order to maintain the inventory of privileged accounts and implement a process of continuous discovery to curb privileged account sprawl, identify potential insider abuse, and reveal external threats. This includes continuous data and operations impact assessments.

16.4.35.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6859]

Agencies MUST create, implement and maintain a robust system of continuous discovery, monitoring and review of privileged accounts and the access rights and credentials associated with those accounts.

16.4.35.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:6860]

Privileged account monitoring systems MUST monitor and record:

- individual user activity, including exceptions such as out of hours access;
- activity from unauthorised sources;
- any unusual use patterns; and
- any creation of unauthorised privileges access credentials.

16.4.35.C.03. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:6861]

Agencies MUST protect and limit access to activity and audit logs and records.

16.4.36. Response and Remediation

16.4.36.R.01. Rationale

Because privileged accounts have high levels of system and data access, a rapid response to unusual or anomalous activity is fundamental to the maintenance of the integrity of an agency's systems and data. Any response must take urgent action to protect compromised accounts and systems based on defined policy and breach intelligence. This may include, for example, the immediate suspension of credentials, password rotation or deactivation of credentials.

16.4.36.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:6864]

Agencies MUST develop and implement a response and remediation policy and procedure as part of an agency's Privileged Access Management (PAM) policy.

16.4.37. User Education and Awareness

16.4.37.R.01. Rationale

Privileged Account access may have procedures additional to or that vary from an agency's usual account security and maintenance processes and procedures. As an agency will have established a Privileged Account Management (PAM) policy, this can be conveniently dealt with as a separate or additional component of user training and awareness. Refer also to Section 3.5 - System Users and Section 9.1 - Information Security Awareness and Training.

16.4.37.R.02. Rationale

User training and awareness is also useful to make standard users aware of the characteristics and value of privileged accounts to assist with the detection of anomalous activities where a compromise of an agency system or data may have taken place.

16.4.37.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:6868]

Agencies MUST implement a Privileged Access Management (PAM) policy training module as part of the agency's overall user training and awareness requirement.

16.5. Remote Access

Objective

16.5.1.   Remote access to systems is minimised, secure, controlled, authorised and authenticated.

Context

Scope

16.5.2.   This section covers information relating to the methods used by personnel to access an agency system from a remote location.

Remote access

16.5.3.   Remote access is defined as user access to agency systems originating outside an agency network. It does not include web–based access to DMZ resources. Further information on working off–site can be found in Chapter 21 – Working Off-site. The requirements for using multi–factor authentication are described in the Identification and Authentication section of this chapter.

Remote privileged access

16.5.4.   Remote access by a privileged user to an agency system via a less trusted security domain (for example, the Internet) may present additional risks.   Controls in this section are designed to prevent escalation of user privileges from a compromised remote access account.

16.5.5.   Remote privileged access does **not** include privileged access across disparate physical sites that are within the same security domain or privileged access across remote sites that are connected via trusted infrastructure. Privileged access of this nature faces different threats to those discussed above. Ensuring robust processes and procedures are in place within an agency to monitor and detect the threat of a malicious insider are the most important measure for this scenario.

Encryption

16.5.6.   Cryptography is used to provide confidentiality and preserve integrity of data transmitted over networks where it may be intercepted or examined and is outside the control of the sender and recipient.

16.5.7.   With the increases in speed and computing power and the cost reductions of modern computing, older cryptographic algorithms are increasingly vulnerable. It is vital that recommendations and controls in the NZISM are followed.

16.5.8.   The use of approved cryptographic algorithms to encrypt authentication, session establishment and data for all remote access connections is considered good practice (See Chapter 17 - Cryptography and Chapter 21 - Working Off-Site).

References

16.5.9.   Further references can be found at:

Title	Publisher	Source

Virtual Private Network Capability Package Version 3.1 March 2015	NSA	https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/vpn-cp.pdf
NIST Special Publication 800-46 Revision 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
NIST Special Publication 800-114 Revision 1 User's Guide to Telework and Bring Your Own Device (BYOD) Security	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

Rationale & Controls

16.5.10. Authentication

16.5.10.R.01. Rationale

Authenticating remote system users and devices ensures that only authorised system users and devices are allowed to connect to agency systems.

16.5.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:1973]

Agencies MUST authenticate each remote connection and user prior to permitting access to an agency system.

16.5.10.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1974]

Agencies SHOULD authenticate both the remote system user and device during the authentication process.

16.5.11. Remote privileged access

16.5.11.R.01. Rationale

A compromise of remote access to a system can be limited by preventing the use of remote privileged access from an untrusted domain.

16.5.11.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:1977]

Agencies MUST NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.

16.5.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:1978]

Agencies SHOULD NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.

16.5.12. VPNs

16.5.12.R.01. Rationale

Virtual Private Networks (VPN's) use a tunnelling protocol to create a secure connection over an intermediate (public) network such as the internet. A VPN uses techniques such as encryption, authentication, authorisation and access control to achieve a secure connection. See Chapter 17 for details on cryptographic selection and implementation.

16.5.12.R.02. Rationale

A VPN can connect remote or mobile workers or remote locations to a private (agency) network.

16.5.12.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1982]

Agencies SHOULD establish VPN connections for all remote access connections.

16.6. Event Logging and Auditing

Objective

16.6.1. Information security related events are logged and audited for accountability, incident management, forensic and system monitoring purposes.

Context

Scope

16.6.2. This section covers information on the automatic logging of information relating to network activities. Information regarding manual logging of system management activities can be found in Section 16.3 - Privileged Access. See also Chapter7 - Information Security Incidents.

16.6.3. A security event is a change to normal or expected behaviour of a network, network component, system, device or user. Event logging helps improve the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected.

16.6.4. It is important that sufficient details are recorded in order for the logs to be useful when reviewed or when an investigation is in progress. Retention periods are also important to ensure sufficient log history is available. Conducting audits of event logs is an integral part of the security and maintenance of systems, since they will help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions.

References

16.6.5. Additional information relating to event logging is contained in:

Title	Publisher	Source
ISO/IEC 27001:2013 Monitoring	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
Standard Time for a New Zealand Network	Measurement Standards Laboratory	https://www.measurement.govt.nz/about-us/official-new-zealand-time/about-time/

Rationale & Controls

16.6.6.   Maintaining system management logs

16.6.6.R.01.   Rationale

Having comprehensive information on the operations of a system can assist system administration, support information security and assist incident investigation and management. In some cases forensic investigations will rely on the integrity, continuity and coverage of system logs.

16.6.6.R.02.   Rationale

It will be impractical and costly to store all system logs indefinitely. An agency retention policy may consider:

- Legislative and regulatory requirements;
- Ensure adequate retention for operational support and efficiency;
- Minimise costs and storage requirements; and
- An adequate historical archive is maintained.

Care should be taken to ensure that these considerations are properly balanced.
Some practices dictate retention periods, for example good DNSSEC practice requires log information is stored in log servers for 4 months, then archived and retained for at least 2 years.

16.6.6.C.01.   Control System Classification(s): Top Secret; Compliance: MUST [CID:1997]

Agencies MUST maintain system management logs for the life of a system.

16.6.6.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:1998]

Agencies SHOULD determine a policy for the retention of system management logs.

16.6.7.   Content of system management logs

16.6.7.R.01.   Rationale

Comprehensive system management logs will assist in logging key management activities conducted on systems.

16.6.7.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2001]

A system management log SHOULD record the following minimum information:

- all system start-up and shutdown;
- service, application, component or system failures;
- maintenance activities;
- backup and archival activities;
- system recovery activities; and
- special or out of hours activities.

16.6.8.   Logging requirements

16.6.8.R.01.   Rationale

Event logging can help raise the security posture of a system by increasing the accountability for all system user actions.

16.6.8.R.02.   Rationale

Event logging can increase the chances that malicious behaviour will be detected by logging the actions of a malicious party.

16.6.8.R.03.   Rationale

Well configured event logging allows for easier and more effective auditing and forensic examination if an information security incident occurs.

16.6.8.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:2006]

Agencies MUST develop and document logging requirements covering:

- the logging facility, including:
  - log server availability requirements; and
  - the reliable delivery of log information to the log server;
- the list of events associated with a system or software component to be logged; and
- event log protection and archival requirements.

16.6.9.   Events to be logged

16.6.9.R.01.   Rationale

The events to be logged are key elements in the monitoring of the security posture of systems and contributing to reviews, audits, investigations and incident management.

16.6.9.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2009]

Agencies MUST log, at minimum, the following events for all software components:

- logons;
- failed logon attempts;
- logoffs;
- date and time;
- all privileged operations;
- failed attempts to elevate privileges;
- security related system alerts and failures;
- system user and group additions, deletions and modification to permissions; and
- unauthorised or failed access attempts to systems and files identified as critical to the agency.

16.6.10. Additional events to be logged

16.6.10.R.01. Rationale

The additional events to be logged can be useful for reviewing, auditing or investigating software components of systems.

16.6.10.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2012]

Agencies SHOULD 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 or structure 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 import/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.

16.6.10.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2013]

Agencies SHOULD log, at minimum, the following events for all software components:

- user login;
- all privileged operations;

- failed attempts to elevate privileges;
- security related system alerts and failures;
- system user and group additions, deletions and modification to permissions; and
- unauthorised or failed access attempts to systems and files identified as critical to the agency.

16.6.11. Event log facility

16.6.11.R.01. Rationale

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. An authoritative external time source, a local **Time Source Master Clock or server or** Co-ordinated Universal Time (UTC) is essential for the time-stamping of events and later inspection or forensic examination. The NZ Interoperability Framework (e-GIF) recognises the time standard for New Zealand as UTC (MSL), with Network Time Protocol (NTP) v.4 as the delivery method over the Internet.

16.6.11.R.02. Rationale

New Zealand standard time is maintained by the Measurement Standards Laboratory of New Zealand (MSL), a part of Industrial Research Limited (IRL). New Zealand standard time is based on UTC, a worldwide open standard used by all modern computer operating systems. UTC (MSL) is kept within 200 nanoseconds of the international atomic time scale maintained by the Bureau International des Poids et Mesures (BIPM) in Paris.

16.6.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2017]

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 user(s) or processes;
- event description;
- success or failure of the event;
- event source (e.g. application name); and
- IT equipment location/identification.

16.6.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2018]

Agencies SHOULD establish an authoritative time source.

16.6.11.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2019]

Agencies SHOULD synchronise all logging and audit trails with the time source to allow accurate time stamping of events.

16.6.12. Event log protection

16.6.12.R.01. Rationale

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.

16.6.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2022]

Event logs MUST be protected from:

- modification and unauthorised access; and
- whole or partial loss within the defined retention period.

16.6.12.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2023]

Agencies MUST configure systems to save event logs to separate secure servers as soon as possible after each event occurs.

16.6.12.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2024]

Agencies SHOULD ensure that:

- systems are configured to save event logs to a separate secure log server; and
- event log data is archived in a manner that maintains its integrity.

16.6.13. Event log archives

16.6.13.R.01. Rationale

It is important that agencies determine the appropriate length of time to retain DNS, proxy, event systems and other operational logs. Logs are an important information source in reviews, audits and investigations ideally these should be retained for the life of the system or longer.

16.6.13.R.02. Rationale

The Archives, Culture, and Heritage Reform Act 2000, the Public Records Act 2005 and the Official Information Act 1982 may determine or influence the length of time that logs need to be retained and if they should be archived.

16.6.13.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2028]

Event logs MUST be archived and retained for an appropriate period as determined by the agency.

16.6.13.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:2029]

Disposal or archiving of DNS, proxy, event, systems and other operational logs MUST be in accordance with the provisions of the relevant legislation.

16.6.13.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:2030]

> Agencies SHOULD seek advice and determine if their logs are subject to legislation.

16.6.13.C.04. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:2031]

> Agencies SHOULD retain DNS, proxy and event logs for at least 18 months.

16.6.14. Event log auditing

16.6.14.R.01. Rationale

> Conducting audits of event logs is seen as an integral part of the maintenance of systems, as they will assist in the detection and attribution of any violations of agency security policy, including information security incidents, breaches and intrusions.

16.6.14.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2034]

> 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; and
> - roles and specific responsibilities.

16.7. Multi-Factor Authentication

Objective

16.7.1. To ensure authentication systems incorporate Multi-Factor Authentication mechanisms to secure Privileged Accounts and in accordance with the Agency's Privileged Access Management (PAM) policy.

Context

Scope

16.7.2. This section provides information and guidance on the establishment and operation of Multi-Factor Authentication (MFA). It is a critical component of robust Identity and Access Management (IAM), particularly where remote access workforces are required or exist.

16.7.3. Reference to other chapters and sections in this document is essential. In particular:

- Chapter 7 – Information Security Incidents;
- Section 9.1 – Information Security Awareness and Training ;
- Section 16.1 – Identification, Authentication and Passwords;
- Section 16.2 – System Access and Passwords;
- Section 16.3 – Privileged User Access;
- Section 16.4 – Privileged Access Management; and
- Chapter 17 - Cryptography.

Background

16.7.4. Authentication is a key element of security that provides confirmation of the identity of all parties to a transaction. In this context a transaction may include browsing, financial operations and all types of data access, creation, copying and deletion.

16.7.5. Multi-Factor Authentication (MFA) is a security system that verifies a user's identity by requiring multiple credentials, which may be of the same factor or type. Initial authentication often requires a username and password followed by a requirement for other (additional) credentials. It is important to recognise that MFA authentication is not necessarily the same as Two-Factor Authentication or Dual-Factor Authentication. MFA can enable, for example, valid users' access to permit credential reset, even if they are using a username and password that may have been compromised.

16.7.6. Multi-Factor Authentication (MFA) is a strong defence and deterrent against many credential attacks, including brute-force, credential stuffing and password spraying attacks. It also defends against social engineering attacks seeking user credentials.

16.7.7. Multi-Factor Authentication (MFA) incorporates Two-Factor Authentication (2FA), which is also briefly discussed in Section 16.1 – Identification, Authentication and Passwords. 2FA requires two elements from any of the three factors of authentication and with the second factor from a different group to the first factor selected. These factors or groups are:

1. Something you have (preferably NOT the device itself but a SEPARATE authentication device such as a token, RFID card or smartcard). This is also known as the **possession or ownership factor**;

2. Something you know such as a PIN, One-Time Password (OTP), reusable password, pattern or other component of a standard authentication mechanism. This is also described as the **knowledge factor**;

3. Something you are (physical characteristics or biometrics of various types). This is also described as the **inherence factor**.

16.7.8. MFA is frequently used where the assurance provided by username and password is inadequate. Additional authenticators increase attack resistance and reduce risk of unauthorised access. Additional authentication also assists in managing Privileged Access (refer to Section 16.4 – Privileged Access Management).

16.7.9. MFA is most effective when knowledge, possession, and inherence authentication factors are used as compensating factors for other authentication weaknesses. This is discussed in more detail in 16.7.16 below. Using MFA increases attack resistance by increasing the difficulty of obtaining all necessary authenticators.

16.7.10. It is important to use a variety of factors to strengthen attack resistance in order to increase confidence levels in the chosen authentication system. For example, using a second factor from the knowledge group is less effective as passwords are inherently part of the knowledge group. Knowledge groups are most exposed to attack and compromise through social engineering.

16.7.11. To maximise the effectiveness and security of any Multi-Factor Authentication construct, the authentication service should be dedicated, hardened and isolated within the network's security architecture.

SMS

16.7.12. There are several known vulnerabilities in SMS which may make it unsuitable and unsafe for authentication purposes. Vulnerabilities include:

- Hackers have been able to mislead and persuade carriers and service providers into porting a phone number to a new device through a SIM swap. This can often be achieved with minimal personal information such as your phone number, date of birth, full name, the last four digits of your bank card access number, bank account number, mobile device number, Social Security number or similar information. Users often store bank cards with their mobile device so if the device is stolen or simply accessed temporarily, this data can also be accessed. Once the phone number has been redirected, physical access to your device is no longer required. Any SMS codes are then subject to compromise.
- If text messages are synched with or duplicated on a laptop, tablet or other personal device, then SMS are vulnerable if the device used by another person or if the device is stolen.
- There are vulnerabilities in mobile telecommunication infrastructure in what's described as a SS7 (Signalling System 7) attack. An SS7 attack is an exploit that takes advantage of a weakness in the design of SS7 which can enable data theft, eavesdropping, text interception and location tracking. SS7 is a protocol dating from the mid-1970's and almost all telecommunication service providers have now implemented security measures to counter SS7 exploits. Social engineering remains a risk.

Key Benefits

16.7.13. The principal benefits of MFA include:

- Strengthened security and credential protection;
- Streamlined user access;
- Reduced administrative overhead;
- Increased security visibility; and
- Improved compliance.

Adaptive Authentication

16.7.14. **Adaptive Authentication** varies the level or degree of authentication required where an unusual authentication request occurs. For example, out of normal hours, from an unusual geolocation, from an unrecognised device, from an unrecognised IP address and so on. When an unusual authentication request is received, Adaptive Authentication may request additional credentials such as a one-time code provided to a known mobile phone number. Some **risk factors** that may trigger Adaptive Authentication include:

- The location of the access request such as such as a café, airport or home;
- The time of the access request such as like late at night, over weekends or during normal working hours;
- The type of device, such as a smartphone, tablet, laptop or unrecognised device;
- The type of connection, for example, a public network such as the internet, or a VPN or some other private network; and
- A request for access to privileged accounts.

16.7.15. Adaptive authentication includes what is sometimes described as transaction identification where known characteristics are compared to the transaction or access request. For example a known location or common access request. If known characteristics do not match then additional authentication steps may be indicated or required.

Client-Side Authentication

16.7.16. Client-side authentication originates from the user's device such as laptop, mobile phone, tablet or home computer. These devices may provide a variety of authentication methods including:

- **Inherence factor/Biometric:**
  - Fingerprint scans;
  - Facial recognition;
  - Voice command/recognition;
  - Iris scans;
  - Keystroke dynamics;

- **Knowledge factor:**
  - PIN codes;
  - Pattern codes;

- **Possession factor:**
  - Geofencing;
  - Bluetooth device proximity/Near field communication (NFC).

16.7.17. It is important to note that some biometric and other measures, for example fingerprints, are susceptible to attacks such as spoofing. To combat these biometric attacks secondary measures are also required, for example pulse-sensing in addition to fingerprint detection in order to ensure the fingerprint presentation is a live person. Clearly not all secondary measures are fully effective in themselves and multiple secondary measures may be required for high risk/high value authorisation requests.

Single-User and Multi-User Authorisation

16.7.18. **Single-User authorisation** involves prompting the account holder to authorise an action being taken on his behalf. For example, single-user authorisation can even prevent fraud as it occurs in a user-friendly manner. Instead of calling the customer to verify the legitimacy of a purchase, credit card companies could request customer authentication for an on-line purchase by sending an authorisation request to the customer through an alternate channel such as a mobile phone.

16.7.19. **Multi-User authorisation** usually requires multiple and separate authentications (usually people) in order to authorise a transaction or event, such as establishing an account. This system supports the "separation of duties" concept common in accounting transactions or other high risk activities. Another example is a password change for a privileged account. Multiuser authorisation may also assess risk indicators and context (e.g. time, location) to select the authentication components and requirements.

Multi-Step Authentication

16.7.20. **Multi-step Authentication** is a design and architectural approach to control access to resources by sequentially using multiple authentication verifiers. Each authentication step grants access to increasingly privileged areas of the system until access to the desired resources is reached (refer also to 16.4 – Privileged Access Management). Multi-Step Authentication can be activated by risk-based "triggers" where risk factors are identified.

16.7.21. Multi-step Authentication may require only one authentication factor or mechanism, so it is important not to confuse Multi-Step Authentication with Multi-Factor Authentication. Multi-Step Authentication may not be as secure as MFA and cannot be an appropriate substitute for MFA. A key risk is repeated use of a single authentication factor.

16.7.22. It is also worth noting, however, that Multi-Step combined with Multi-Factor Authentication is a strong architectural security construct, particularly when separate authentication factors are required at each step when accessing privileged accounts.

Perfect Forward Secrecy

16.7.23. In addition to the encryption protocols and algorithms discussed in Chapter 17 - Cryptography, the concept of **Perfect Forward Secrecy (PFS)**, often simplified to Forward Secrecy, should also be incorporated into any authentication mechanism design.

16.7.24. **Forward Secrecy** is a property of secure communication protocols that is intended to prevent a compromised encryption key from being used to decrypt previously encrypted traffic. Clearly a compromised key must be immediately replaced in order to maintain the integrity of communications. This mechanism is described as a "**rolling secrets**" technique and is designed to prevent device spoofing and the cloning of mobile clients.

16.7.25. A **"rolling secret"** key is located on the client device. The client receives two encrypted packages. The first contains another private key and is decrypted by the current private key held on the client device. The new key is used to decrypt the second package and the new private key replaces the existing private key, which is then discarded. The new key is used to encrypt traffic to the authentication server. With each cycle the client replaces the old key with the new key.

Cryptography

16.7.26. The use of encryption is a fundamental component is the security of a Multi-Factor Authentication mechanism. It is essential that only approved cryptographic protocols and algorithms are used, refer to Chapter 17 – Cryptography.

Risk Analysis

16.7.27. The design of Multi-Factor Authentication should start with a risk review in order to identify any existing and new risks from changing environments, user populations and threat landscapes. Some early steps will include:

- Review business drivers, existing identity infrastructure, enterprise applications, core platform infrastructure and development plans for each of these;
- Ensure any plans for cloud and related services are reviewed and incorporated;
- Identify authentication use cases including employees and contractors, consumers, customers, partners, and suppliers. For Digital Government this may also include the General Public for some systems;
- Develop baseline requirements;
- Undertake a threat analysis for each use case; and

Select control mechanisms to manage identified risks.

16.7.28. This risk analysis will inform and direct the development of an authentication architecture to provide robust but usable security for each use case. Some key questions include:

- How will users access the system or application?
- At what stage will users be authenticated?
- What authentication factors will provide the appropriate level of authentication and security?
- Is the level of authentication appropriate to secure and protect the systems, data and other related assets? and
- Is there sufficient capacity to service anticipated workloads?

Governance and Control

16.7.29. Good governance processes assist in identifying potential risks to your systems, data, employees, partners and contractors and reduces the risk of a breach or failure to comply with legislation and regulation. Good governance processes support the fulfilment of fiduciary duties of senior and executive management.

16.7.30. Technology governance must demonstrate effective control, security, effectiveness and clear accountability. Identity Access Management and Authentication are fundamental components in protecting agency systems, data and technology assets and underpinning technology governance structures.

16.7.31. There are also a number of national and international legislative and regulatory requirements and accepted international standards which may influence aspects of governance, particularly in relation to data protection and privacy. While not an exhaustive list, these include:

- New Zealand's Privacy Act;
- New Zealand's Public Records Act;
- The European Union's Payment Services Directive (PSD);
- The EU's General Data Protection Regulation (GDPR);
- ISO/IEC 27701:2019 - Security techniques. An Extension to ISO/IEC 27001 and ISO 27002 for privacy information management, particularly GDPR;
- The US Health Insurance Portability and Accountability Act (HIPAA);
- The Payment Card Industry Data Security Standard (PCI DSS).

References

16.7.32. Additional information relating to event logging is contained in:

Title	Publisher	Source
ISO/IEC 27001:2019 – Annex A.9.1 – Access Control Policy	ISO/IEC/ Standards NZ	https://www.iso.org
ISO/IEC 27701:2019 - Security techniques - Extension to ISO/IEC 27001 and ISO 27002 for privacy information management - requirements and guidelines Standard.	ISO/IEC/ Standards NZ	https://www.iso.org
NIST Digital Identity Guidelines (Four Documents)	NIST	https://pages.nist.gov/800-63-3/
NIST Special Publication 800-123 – Guide to General Server Security	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf
NIST Special Publication 800-140E, March 2020 - CMVP Approved Authentication Mechanisms	NIST	https://csrc.nist.gov/CSRC/media/Publications/sp/800-140e/draft/documents/sp800-140e-draft.pdf
NIST Special Publication 1800-17 Multifactor Authentication for E-Commerce	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf
NIST SP 800-95 Guide to Secure Web Services	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf
OAuth 2.0	IETF OAuth Working Group.	https://oauth.net/2/
RFC 6819: OAuth 2.0 Threat Model and Security Considerations	IETF	https://tools.ietf.org/html/rfc6819
RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage	IETF	https://tools.ietf.org/html/rfc6750
RFC 8252 - OAuth 2.0 for Native Apps	IETF	https://tools.ietf.org/html/rfc8252
Authentication Standards	NZ Govt	https://www.digital.govt.nz/standards-and-guidance/identity/identification-management/identification-management-standards/standards-to-be-superseded/authentication-standards/
Implementing Multi-Factor Authentication	ASD	https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication
Cloud security guidance - Identity and authentication	NCSC UK	https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles/identity-and-authentication
Multi-Factor Authentication Version: 1.0 Date: February 2017 Author:	PCI Security Standards Council	https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf
An Architecture for Implementing Enterprise Multifactor Authentication with Open Source Tools	SANS	https://www.sans.org/reading-room/whitepapers/authentication/architecture-implementing-enterprise-multifactor-authentication-open-source-tools-34455
Fast Identity Online Alliance – Draft Reference Architecture	FIDO Alliance	http://fidoalliance.org/assets/downloads/DraftD-FIDO-Refarch-00.pdf
FIDO Specifications Overview	FIDO Alliance	https://fidoalliance.org/specifications/
Azure Multi-Factor Authentication	Microsoft	https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks
OWASP Cheat Sheet Series – Multifactor Authentication Cheat Sheet	OWASP	https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html
A Step by Step Guide to SS7 Attacks	FirstPoint	https://www.firstpoint-mg.com/blog/ss7-attack-guide/

Rationale & Controls

16.7.33. Risk Analysis

The requirement for an agency information security policy is discussed and described in **Chapter 5 – Information Security Documentation**. An essential part of any security policy is the assessment of risk and the inclusion of requirements for securing access to systems, applications and data.

16.7.33.R.02. Rationale

A risk analysis is fundamental to the design, implementation and maintenance of Multi-Factor Authentication (MFA) processes and will inform and direct the development of requirements and an authentication architecture to provide robust but usable security.

16.7.33.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6948]

Agencies MUST undertake a risk analysis before designing and implementing MFA.

16.7.34. System Architecture and Security Controls

16.7.34.R.01. Rationale

Security controls should support security while enabling authorised user access. The system architecture should be sufficiently comprehensive to support this objective.

16.7.34.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6952]

The design of an agency's MFA SHOULD include consideration of:

- Risk Identification;
- Level of security and access control appropriate for each aspect of an agency's information systems (data, devices, equipment, storage, cloud, etc.)
- A formal authorisation process for user system access and entitlements;
- Logging, monitoring and reporting of activity;
- Review of logs for orphaned accounts and inappropriate user access;
- Identification of error and anomalies which may indicate inappropriate or malicious activity;
- Incident response;
- Remediation of errors;
- Suspension and/or revocation of access rights where policy violations occur;
- Capacity planning.

16.7.34.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6953]

Where an agency has implemented MFA they SHOULD:

- Require MFA for administrative or other high privileged users; and
- Implement a secure, multi-factor process to allow users to reset their normal usage user credentials.

16.7.35. Integration with Policy

16.7.35.R.01. Rationale

The requirement for an agency information security policy is discussed and described in **Chapter 5 – Information Security Documentation**. Privileged Access Management policy is discussed in **Section 16.4** - **Privileged Access Management**.

16.7.35.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:6956]

The design of an agency's MFA system SHOULD be integrated with the agency's Information Security Policy and the agency's Privileged Access Management (PAM) Policy.

16.7.36. User Training

16.7.36.R.01. Rationale

It is important that users understand and have continued awareness of risks and threats to authentication credentials, in order to maintain the integrity of the credentials and to maintain the security of the systems being accessed.

16.7.36.R.02. Rationale

MFA introduces some complexity and may require the use of specific devices, hardware or applications. Training is essential if additional overhead through increased support is not to be introduced.

16.7.36.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:6960]

When agencies implement MFA they MUST ensure users have an understanding of the risks, and include appropriate usage and safeguards for MFA in the agency's user training and awareness programmes.

17. Cryptography

17.1. Cryptographic Fundamentals

Objective

17.1.1. Cryptographic products, algorithms and protocols are approved by the GCSB for suitability before being used and that cryptographic implementations by agencies are adequate for the protection of data and communications.

Scope

17.1.2. This section covers information on 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 Section 17.2 - Approved Cryptographic Algorithms and Section 17.3 - Approved Cryptographic Protocols.

Purpose of cryptography

17.1.3. Encryption is primarily used to provide confidentiality protecting against the risk of information being exploited by an attacker. More broadly, cryptography can also provide authentication, non-repudiation and integrity. Cryptography is also used in the establishment of secure connectivity, such as IPSEC VPNs.

17.1.4. The use of approved encryption will generally reduce the likelihood of an unauthorised party gaining access to the information contained within the encrypted data.

17.1.5. Cryptography is an important control for data protection and the encryption selected will depend on the classification of the data. Note that classification, in itself, provides no protection but is merely indicative of the degree of protection and care in handling required for that level of classification.

17.1.6. 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.

17.1.7. With the increases in speed and computing power and the cost reductions of modern computing, older cryptographic algorithms are increasingly vulnerable. It is vital that recommendations and controls in the NZISM are followed.

Using encryption

17.1.8. Encryption of data at rest can be used to reduce the physical protection of storage and handling requirements of the media or systems.

17.1.9. Encryption of data in transit can be used to provide protection for information being communicated over insecure mediums and hence reduce the security requirements of the communication process.

17.1.10. When agencies use encryption for data at rest or in transit, they are **not** reducing the **classification** of the information. When encryption is used the potential risk of disclosure of the information is reduced, and as such the protection requirements for a lower classification may be considered to be more appropriate to that information.

17.1.11. As the classification of the information **does not** change when encrypted, agencies cannot use the lowered storage, physical transfer or security requirements as a baseline to further lower requirements with an additional cryptographic product.

17.1.12. In general terms, the level of assurance of specific encryption protocols and algorithms is defined in terms of Common Criteria, Protection Profiles or, in some cases, approved cryptographic evaluations. It is important to note that evaluations of cryptographic protocols and algorithms are **NOT** universally conducted when security products are evaluated, relying rather on previous approved evaluations of cryptographic protocols and algorithms.

Risk Assessments

17.1.13. Encryption algorithms create data transformations that are designed to be difficult to easily reverse by unauthorised users. Today's software will usually provide several algorithmic options, including some older algorithms provided for backward compatibility with older (legacy) systems. In many cases the older algorithms may be deprecated, are considered time-expired and are not fit for purpose in modern systems.

17.1.14. In all cases a comprehensive risk assessment should be undertaken before configurations are selected. Some general principles to be considered are:

- Long, complex passwords are stronger than short passwords;
- Long keys generally provide stronger encryption than short keys;
- Asymmetric encryption is slower than symmetric encryption;
- Symmetric encryption is generally recommended when the key is stored locally only;
- Asymmetric encryption is recommended when keys need to be shared across communication channels;
- If you are encrypting **very large** volumes of data, encrypting the data using a symmetric key, and encrypting the symmetric key with an asymmetric key **may be** more operationally effective;
- Normally encrypted data cannot be compressed, but compressed data can be encrypted. Data should be compressed before encryption.
- Any risk assessment should include consideration of key management - refer to 17.9 Key Management

17.1.15. It is important to note that the NZISM prescribes approved algorithms and protocols and users must select combinations from these lists.

Transitioning Cryptographic Algorithms and Protocols

17.1.16. It is important to use algorithms that adequately protect sensitive information. It is also important to recognise that all cryptographic algorithms and protocols have a finite life. Challenges are posed by new cryptanalysis techniques and methods, the increasing power of classical computing technology, and the continuing work on the development of quantum computers. In addition, there is an active field of work that continuously seeks to compromise algorithms and protocols currently in use.

17.1.17. Planning for changes in the use of cryptography because of algorithm breaks, the availability of more powerful computing techniques or new technologies is an important consideration for agencies. Awareness of retirement or deprecation of algorithms and associated protocols is essential.

Retiring RSA

17.1.18. RSA was announced in 1976 so it is now over 40 years old. Several flaws and attacks have been identified since creation, each of which required specific mitigations, careful implementation and management. Unfortunately there is ample evidence that implementers continue to have difficulties in securely implementing, using and managing RSA.

17.1.19. To counter identified threats from shorter RSA key lengths, longer key lengths have been specified in the NZISM since 2010. Subsequently it was specified in the NZISM that RSA was approved for use in **legacy systems only**.

17.1.20. This approach was selected to allow agencies to plan the retirement of legacy systems and ensure replacement systems were using only approved algorithms and protocols.

17.1.21. There are several indicators that RSA will be deprecated in the next few years. For example TLS 1.3 deprecates RSA in favour of elliptic curve cryptography. The most recent guidance from NIST is also indicative of impending deprecation of RSA.

17.1.22. It is, therefore essential that agencies are aware of these changes and plan the retirement of RSA from their systems as part of their ongoing operational management.

Product specific cryptographic requirements

17.1.23. This section provides requirements for the use of cryptography to protect classified information. Requirements, additional to those in this Manual, can exist in consumer guides for products once they have completed an approved evaluation. Vendor specifications supplement this manual and where conflict in controls occurs the product specific requirements take precedence. Any policy or compliance conflicts are to be incorporated into the risk assessment.

Exceptions for using cryptographic products

17.1.24. Where Agencies implement a product that uses an Approved Cryptographic Algorithm or Approved Cryptographic Protocol to provide protection of unclassified data at rest or in transit, that product does not require a separate, approved evaluation. Correct implementation of the cryptographic protocol is fundamental to the proper operation of the Approved Cryptographic Algorithm or Approved Cryptographic Protocol and is part of the checking conducted during system certification.

Federal Information Processing Standard 140

17.1.25. The FIPS 140 is a United States standard for the validation of both hardware and software cryptographic modules.

17.1.26. 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.

17.1.27. FIPS 140 is not a substitute for an approved evaluation 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.

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

17.1.29. The GCSB will review the FIPS 140 validation report to confirm compliance with New Zealand National Cryptographic Policy.

New Zealand National Policy for High Assurance Cryptographic Equipment and Key Management

17.1.30. The New Zealand National Standard for High Assurance Cryptographic Equipment (HACE) and related key management is contained in the New Zealand Communications Security Standard No. 301 – Safeguarding of Communications Security (COMSEC) Material. This prescribes national doctrine for the safeguarding of COMSEC materials. New Zealand Communications Security Standard No. 301 – Safeguarding of Communications Security (COMSEC) Material, replaces New Zealand Communications Security Standard No. 300 – Control of COMSEC Material which is now withdrawn. Note NZCSI 301 is a **RESTRICTED** document.

Protection of RESTRICTED/SENSITIVE information in transit over public systems

17.1.31. The physical requirements for protection of information classified RESTRICTED/SENSITIVE are provided by the classification system and PSR guidance.

17.1.32. Where such information is generated and held on information systems (any computer device, including laptops, mobile phones, tablets, desktop and networked systems), the requirements of the NZISM apply. Of particular note is the requirement to encrypt RESTRICTED/SENSITIVE data when in transit over public systems, including any Internet connection, public network or any other network NOT directly controlled by the agency.

Encryption and Key Management

17.1.33. Encryption is necessary to protect the information while in transit and while NOT under the direct control of the agency. The use of encryption (also including data encryption, use of a VPN or some other form of protection using cryptography) must also consider cryptographic key management and the retention of control of key management. Where cloud services are used it is essential that the protection of data at rest is also considered.

17.1.34. Where agencies make use of VPN/ MPLS services provided by an ISP, Telco or other service provider, the control and management of the cryptographic key is fundamental to the integrity and security of the encrypted data.

17.1.35. If your encryption keys are compromised, then any authentication and encryption mechanisms, no matter how robust or comprehensive, are futile. Further risks include the loss of access to encrypted data and the potential to expose all data and systems if keys are maliciously or accidentally replaced.

17.1.36. The selection of the cryptographic protocol and algorithm is described in the NZISM, Chapter 17 and specified in 17.1.48.C.02. It is essential that agencies select and use only approved cryptographic algorithms and protocols and apply the cryptographic key management requirements of the NZISM, see section 17.9 - Key Management.

Direct Control / Agency Control

17.1.37. In relation to the NZISM, *Direct Control* is the immediate and continuous physical and logical control, responsibility for, protection and operation of agency information systems and data. In the NZISM, *Agency Control* is synonymous with *Direct Control.*

Non-Agency Control

17.1.38. Where agencies outsource the management of data centres it follows that they do NOT have direct control over the data centre and related gateways. In other cases the operation of systems within an agency are also outsourced. In such cases encryption MUST be applied at the transmitting device as this is the logical point at which direct agency control ceases. In large agencies, this is likely to be impractical and creates a significant key management overhead. Encryption for routine traffic originating at the transmitting device is therefore likely to occur only in exceptional cases or where special protection is required.

17.1.39. The determination of when and where a communication/transmission leaves direct agency control will depend on a number of factors including:

- The scope and extent of outsourcing and information systems support agreements with service providers;
- Service agreements with ISP's, Telcos and other communication service providers;

- The agency's system architecture and security architecture. In particular the boundary where direct agency control ceases. In traditional network architectures this was described as the "gateway";
- Key management and control of the application of keys when encrypting/decrypting;
- The use of Hardware Security Modules (HSM's- refer to section 17.10).

VPN connection Security

17.1.40. The types of encryption, protocols, and cryptographic algorithms applied in the establishment and maintenance of a VPN connection are fundamental to the security and integrity of the connection.

17.1.41. Key aspects of VPN security include:

- The encryption algorithm and protocol used;
- Cryptographic key length;
- The authentication protocol
- Key Exchange protocol;
- Selection of VPN protocol;
- VPN monitoring and "kill switch" to deter IP leakage   and snooping;
- Cryptographic key management.

17.1.42. It is important to understand that a variety of VPN services can use a variety of mechanisms. Agencies should also consider the service provider's use of hash authentication, perfect forward secrecy, and the difference in encryption settings on both the data and control channels. The NZISM specifies the cryptographic protocols and cryptographic algorithms that should be used (see sections 17.2 – Approved Cryptographic Algorithms and 17.3 – Approved Cryptographic Protocols) and agencies must ensure the VPN connection conforms with these requirements.

References

17.1.43. Further references can be found at:

Title	Publisher	Source
New Zealand Communications Security Instruction No. 301 - Safeguarding of Communications Security (COMSEC) Material. NZCSI 301 replaces NZCSI 300.	GCSB	Contact the GCSB RESTRICTED document available on application to authorised personnel
New Zealand Communications Security Standard No. 500 - Policy	GCSB	Contact the GCSB RESTRICTED document available on application to authorised personnel
FIPS140-2	NIST	http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS140-3 DRAFT	NIST	http://www.csrc.nist.gov/publications/drafts/fips140-3/FIPS_140-3_sections_submitted_for_comments.pdf
NIST Special Publication 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
NIST Special Publication 800-56B Revision 1 - Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, September 2014	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf
NIST 800-175A - Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies, August 2016	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf
NIST 800-175B - Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, March 2020	NIST	https://csrc.nist.gov/publications/detail/sp/800-175B/rev-1/final
SP 800-57 Part 1, Recommendation for Key Management: Part 1: General (Revision4), Jan 2016	NIST	http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization, Aug 2005	NIST	http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf
SP 800-57 Part 3, Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance, Jan, 2015	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

FIPS PUB 186-4 Digital Signature Standard (DSS) July 2013	NIST	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
SP 800-131A Rev. 2 (DRAFT) Transitioning the Use of Cryptographic Algorithms and Key Lengths – July 2018	NIST	https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/draft
SP 800-56B Rev. 1 - Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography - September 2014	NIST	https://csrc.nist.gov/publications/detail/sp/800-56b/rev-1/final
Handling requirements for protectively marked information and equipment	PSR	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/information-security/security-classification-system-and-handling-requirements/handling-requirements-for-protectively-marked-information-and-equipment/
Virtual Private Network Capability Package Version 3.1 March 2015	NSA	https://www.nsa.gov/ia/_files/VPN_CP_3_1.pdf
Suite B Implementer's Guide to NIST SP 800-56A, July 28, 2009	NSA	http://docplayer.net/204368-Suite-b-implementer-s-guide-to-nist-sp-800-56a-july-28-2009.html
Guidelines on Cryptographic Algorithms Usage and Key Management - EPC342-08 Version 8.0 18 December 2018	European Payments Council	https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/guidelines-cryptographic-algorithms-usage-and-key-management-0
Choose an Encryption Algorithm	Microsoft	https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-2017
Transport Layer Protection Cheat Sheet	OWASP	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
Guide to Cryptography	OWASP	https://www.owasp.org/index.php/Guide_to_Cryptography
New Directions in Cryptography - IEEE Transactions on Information Theory Vol IT22 November 1976	Diffie, Hellman	https://ee.stanford.edu/~hellman/publications/24.pdf
Transport Layer Security (tls)	IETF	https://datatracker.ietf.org/wg/tls/documents/
TLS 1.3	IETF	http://ietf.org/blog/tls13/
The Transport Layer Security (TLS) Protocol Version 1.3 March 2018	IETF	https://tlswg.github.io/tls13-spec/draft-ietf-tls-tls13.html
RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP	IETF	https://tools.ietf.org/html/rfc2407
RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)	IETF	https://tools.ietf.org/html/rfc2408
RFC 2409, The Internet Key Exchange (IKE)	IETF	https://tools.ietf.org/html/rfc2409

Rationale & Controls

17.1.44. Using cryptographic products

17.1.44.R.01. Rationale

No real-world product can ever be guaranteed to be free of vulnerabilities. The best that can be done is to increase the level of assurance in a product to a point that represents satisfactory risk management.

17.1.44.R.02. Rationale

Refer to Chapter 12 - Product Security for a discussion on product evaluation and assurance.

17.1.44.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2070]

Agencies using cryptographic functionality within a product for the protection of classified information MUST ensure that the product has completed a cryptographic evaluation recognised by the GCSB.

17.1.45. Data recovery

17.1.45.R.01. Rationale

It is important for continuity and operational stability that cryptographic products provide a means of data recovery to allow for the recovery of data in circumstances such as where the encryption key is unavailable due to loss, damage or failure. This includes production, storage,

backup and virtual systems. This is sometimes described as "key escrow".

17.1.45.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2074]

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.

17.1.45.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2075]

Cryptographic products SHOULD 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.

17.1.46. Reducing storage and physical transfer requirements

17.1.46.R.01. Rationale

When encryption is applied to media or media residing within IT equipment it provides an additional layer of defence. Whilst such measures do not reduce or alter the classification of the information itself, physical storage, handling and transfer requirements may be reduced to those of a lesser classification for the media or equipment (but not the data itself).

17.1.46.R.02. Rationale

Approved Cryptographic Algorithms are discussed in section 17.2.

17.1.46.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2079]

Encryption used to reduce storage or physical handling protection requirements MUST be an approved cryptographic algorithm in an EAL2 (or higher) encryption product.

17.1.46.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2080]

If an agency wishes to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they MUST encrypt the classified information using High Assurance Cryptographic Equipment (HACE). It is important to note that the classification of the information itself remains unchanged.

17.1.46.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2081]

If an agency wishes to use encryption to reduce the storage, handling or physical transfer requirements for IT equipment or media that contains classified information, they MUST use:

- full disk encryption; or
- partial disk encryption where the access control will allow writing only to the encrypted partition holding the classified information.

17.1.46.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2082]

If an agency wishes to use encryption to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they SHOULD use:

- full disk encryption; or
- partial disk encryption where the access control will only allow writing to the encrypted partition holding the classified information.

17.1.47. Encrypting NZEO information at rest

17.1.47.R.01. Rationale

NZEO information is particularly sensitive and it requires additional protection in the form of encryption, when at rest. This includes production, storage, backup and virtual systems.

17.1.47.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2085]

Agencies MUST use an Approved Cryptographic Algorithm to protect NZEO information when at rest on a system.

17.1.48. Information and Systems Protection

17.1.48.R.01. Rationale

When encryption is applied to information being communicated over networks, less assurance is required for the physical protection of the communications infrastructure. In some cases, no physical security can be applied to the communications infrastructure such as public infrastructure, the Internet or non-agency controlled infrastructure. In other cases no direct assurance can be obtained and reliance is placed on third party reviews and reporting. In such cases encryption of information is the only practical mechanism to provide sufficient assurance that the agency information systems are adequately protected.

17.1.48.R.02. Rationale

Data duplication for backups or data replication between data centres requires the same level of protection as other parts of the agency's infrastructure. This includes outsourced services.

17.1.48.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:2089]

Agencies MUST use HGCE if they wish to communicate or pass information over UNCLASSIFIED, insecure or unprotected networks.

17.1.48.C.02. Control System Classification(s): Restricted/Sensitive; Compliance: MUST [CID:2090]

Information or systems classified RESTRICTED or SENSITIVE MUST be encrypted with an approved encryption algorithm and protocol if information is transmitted or systems are communicating over any insecure or unprotected network such as the Internet, public infrastructure or non-agency controlled networks.

17.1.48.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:2091]

Agencies MUST encrypt agency data using an approved algorithm and protocol when data is transmitted between data centres over insecure or

unprotected networks such as the Internet, public infrastructure or non-agency controlled networks.

17.1.48.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2092]

Agencies SHOULD use an approved encryption product if they wish to communicate over insecure or unprotected networks such as the Internet, public networks or non-agency controlled networks.

17.1.49. IT equipment using Encryption

17.1.49.R.01. Rationale

In general terms, when IT equipment employing encryption functionality is turned on and authenticated all information becomes accessible to the system user. At such a time the IT equipment will need to be handled in accordance with the highest classification of information on the system. Special technology architectures and implementations exist where accessibility continues to be limited when first powered on. Agencies should consult the GCSB for further advice on special architectures and implementations.

17.1.49.R.02. Rationale

The classification of the equipment when powered off will depend on the equipment type, cryptographic algorithms and protocols used and whether cryptographic key has been removed. Agencies should consult the GCSB for further advice on treatment of specific software, systems and IT equipment.

17.1.49.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2096]

When IT equipment storing encrypted information is turned on and authenticated, it MUST be treated as per the original classification of the information.

17.1.49.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:2097]

Agencies MUST consult the GCSB for further advice on the powered off status and treatment of specific software, systems and IT equipment.

17.1.50. Encrypting NZEO information in transit

17.1.50.R.01. Rationale

NZEO information is particularly sensitive and requires additional protection. It must be encrypted when in transit.

17.1.50.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2100]

In addition to any encryption already in place for communication mediums, agencies MUST use an Approved Cryptographic Protocol and Algorithm to protect NZEO information when in transit.

17.1.51. Key Refresh and Retirement

17.1.51.R.01. Rationale

All cryptographic keys have a limited useful life after which the key should be replaced or retired. Typically the useful life of the cryptographic key (cryptoperiod) is use, product and situation dependant. Product guidance is the best source of information on establishing cryptoperiods for individual products. A more practical control is the use of data, disk or volume encryption where key changes are more easily managed. Selection of cryptoperiods should be based on a risk assessment. Refer also to section 17.9 – Key Management.

17.1.51.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2103]

Agencies SHOULD establish cryptoperiods for all keys and cryptographic implementations in their systems and operations.

17.1.51.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2104]

Agencies SHOULD use risk assessment techniques and guidance to establish cryptoperiods.

17.1.51.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:2105]

Agencies MUST consult with the GCSB for the key management requirements for HGCE.

17.2. Approved Cryptographic Algorithms

Objective

17.2.1. Information is protected by a properly implemented, Approved Cryptographic Algorithm.

Context

Scope

17.2.2. This section covers cryptographic algorithms that the GCSB recognises as being approved for use within government. Implementations of the algorithms in this section need to have successfully completed an approved cryptographic evaluation before they can be approved to protect information. Correct implementations of cryptographic protocols are checked during system certification.

17.2.3. High grade cryptographic algorithms are not covered in this section.

Approved cryptographic algorithms

17.2.4. 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 government, 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 considered to be feasible with current technologies and capabilities.

17.2.5. 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 security vulnerability.

17.2.6. The approved cryptographic algorithms fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms. Collectively these were known as SUITE B and were first promulgated in 2006.

17.2.7. Suite B was superseded by the Commercial National Security Algorithm Suite in August 2015 and later supplemented by the Commercial Solutions for Classified (CSFC) Programme.

17.2.8. The approved asymmetric/public key algorithms are:

- ECDH for agreeing on encryption session keys;
- ECDSA for digital signatures;
- DH for agreeing on encryption session keys for legacy systems only;
- DSA for digital signatures for legacy systems only;
- RSA for digital signatures and passing encryption session keys or similar keys for legacy systems only.

17.2.9. The approved hashing algorithms are:

- Secure Hashing Algorithm 2 (i.e. SHA-384 and SHA-512); and
- Secure Hashing Algorithm 1 (i.e. SHA-1) for legacy systems only.

17.2.10. The approved symmetric encryption algorithms are:

- AES using key lengths of 256 bits; and
- 3DES for legacy systems only.

17.2.11. SHA-1, 3DES, DH, DSA and RSA MUST NOT be used for new implementations but are approved only for current legacy systems already running these algorithms. It is important to note that the use of these older cryptographic algorithms has been deprecated in several countries including Australia and the US.

17.2.12. Summary Table

Function	Cryptographic algorithm or protocol	Applicable standards	Minimum
Encryption	Advanced Encryption Standard (AES)	FIPS 197	256-bit key
Hashing	Secure Hash Algorithm (SHA)	FIPS 180-4	SHA-384
Digital signature	Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-3 ANSI X9.62	NIST P-384
Key exchange	Elliptic Curve Diffie-Hellman (ECDH)	SP 800-56AANSI X9.63	NIST P-384

Salting

17.2.13. Salting is a technique of further modifying a hash by adding a value or character string to the start or end of a password. This improves the resistance of the hash to brute-force attacks. To further improve resistance the salt should be cryptographically strong and randomly generated as unique for each password.

17.2.14. The effectiveness of salts is reduced if implemented poorly. Common implementation errors are salts that are too short and the reuse of salts. To implemement credential-specific salts the following principles should be followed:

- Generation of a unique salt when a stored credential is created;
- Generate salts as cryptographically strong random data;
- Use a 32 or 64 bit salt as storage and system constraints permit;
- Implement a security schema that is not dependent on hiding, splitting or otherwise obfuscating the salt; and
- Do NOT apply salts per user or on a system wide basis.

References

17.2.15. The following references are provided for the approved asymmetric/public key algorithms, hashing algorithms and encryption algorithms. Note that Federal Information Processing Standards (FIPS) are standards and guidelines that are developed by the US National Institute of Standards and Technology (NIST) for US Federal computer systems.

Topic	Publisher	Reference
DH	IEEE	W. Diffie and M. E. Hellman, 'New Directions in Cryptography', IEEE Transactions on Information Theory, vol. 22, is. 6, pp. 644-654, November 1976
DSA Digital Signature Algorithm	NIST	FIPS 186-4 Digital Signature Standard (DSS) http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
AES Advanced Encryption Standard	NIST	FIPS 197 http://www.nist.gov/customcf/get_pdf.cfm?pub_id=901427

RFC 8492 Secure Password Ciphersuites for Transport Layer Security (TLS) FEB 2019	IETF	https://tools.ietf.org/html/rfc8492
RSA	RSA Laboratories	Public Key Cryptography Standards #1
RFC 6944 Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status	Internet Engineering Task Force (IETF)	https://tools.ietf.org/pdf/rfc6944.pdf
NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management - Part 1: General	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
NIST Special Publication 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	NIST	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf
NIST Special Publication 800-57 Part 3 Revision 1 Recommendation for Key Management Part 3: Application-Specific Key Management Guidance	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0	IETF	https://tools.ietf.org/pdf/rfc2898.pdf
RFC 8018 PKCS #5: Password-Based Cryptography Specification Version 2.1	IETF	https://tools.ietf.org/pdf/rfc8018.pdf
NIST Special Publication 800-63-3 series - Digital Identity Guidelines	NIST	https://pages.nist.gov/800-63-3/
NIST Special Publication 800-106 Randomized Hashing for Digital Signatures	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-106.pdf
NIST Special Publication 800-107 Revision 1 Recommendation for Applications Using Approved Hash Algorithms	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf
NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Application	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf
ECDH	NIST	NIST Special Publication 800-56A (Revision 2), May 2013 - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf Also ANSI X9.63 and ANSI X9.42
SHA	NIST Standards Australia	FIPS PUB 180-4 - Secure Hash Standard (SHS) http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf Also Australian Standard AS 2805.13.3 https://infostore.saiglobal.com/store/
3DES	NIST ANSI Standards Australia	NIST Special Publication 800-67 Revision 1 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher FIPS PUB 46-3 Data Encryption Standard (DES) (withdrawn) ANSI X9.52-1998 Triple Data Encryption Algorithm Modes of Operation (withdrawn) Also Australian Standard AS 2805.5.4 https://infostore.saiglobal.com/store/
Cryptography Management	NIST	Recommendation for Key Derivation through Extraction then Expansion, September 2010. http://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf FIPS 140-3 - Security Requirements for Cryptographic Modules.
AES	NIST	NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

AES	NIST	The Galois/Counter Mode of Operation (GCM) http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf
AES	NIST	NIST Advanced Encryption Standard Algorithm Validation List - http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html
AES-CBC	NIST	Cipher Block Chaining (CBC) see NIST Special Publication 800-38A, Recommendations for Block Cipher Modes of Operation – Methods and Techniques http://csrc.nist.gov/publications/PubsSPs.html
AES-CBC Algorithm	IETF	See RFC 3602. http://www.rfc-editor.org/rfc/rfc3602.txt
AES in TLS	IETF	See RFC 5288 http://www.rfc-editor.org/rfc/rfc5288.txt
Commercial National Security Algorithm (CNSA) Suite, January 2016	NSA	https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm
Commercial National Security Algorithm (CNSA) Suite Factsheet	NSA	https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/commercial-national-security-algorithm-suite-factsheet.cfm
Commercial Solutions for Classified (CSfC) FAQ 2018	NSA	https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/csfc-faqs.pdf
FIPS PUB 180-4, Secure Hash Standard, August 2015	NIST	https://csrc.nist.gov/publications/detail/fips/180/4/final

Rationale & Controls

17.2.16. Using Approved Cryptographic Algorithms

17.2.16.R.01. Rationale

Inappropriate configuration of a product using an Approved Cryptographic Algorithm can inadvertently select relatively weak implementations of the cryptographic algorithms. In combination with an assumed level of security confidence, this can represent a significant security risk.

17.2.16.R.02. Rationale

When configuring unevaluated products that implement an Approved Cryptographic Algorithm, agencies should disable any non-approved algorithms. A less effective control is to advise advising system users not to use them via a policy. Correct implementation of cryptographic protocols and disabling of unapproved algorithms is checked during system certification.

17.2.16.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2128]

Agencies using an unevaluated product that implements an Approved Cryptographic Algorithm MUST ensure that only Approved Cryptographic Algorithms can be used.

17.2.17. Approved asymmetric/public key algorithms

17.2.17.R.01. Rationale

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.

17.2.17.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2131]

Agencies SHOULD use ECDH and ECDSA for all new systems, version upgrades and major system modifications.

17.2.18. Using DH (Legacy systems ONLY)

17.2.18.R.01. Rationale

A modulus of at least 4096 bits for DH is now considered good practice by the cryptographic community.

17.2.18.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2134]

Agencies using DH, for the approved use of agreeing on encryption session keys, MUST use a modulus of at least 4096 bits.

17.2.19. Legacy Equipment using DH

17.2.19.R.01. Rationale

If a network device is NOT able to support the required cryptographic protocol, algorithm and key length, the system will be at risk of a cryptographic compromise. In such cases, the longest feasible key length must be implemented and the legacy device scheduled for replacement as a matter of urgency.

17.2.19.C.01. Control

       Legacy devices which are NOT capable of implementing required key lengths MUST be reconfigured with the longest feasible key length as a matter of urgency.

17.2.19.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2138]

       Legacy devices which are NOT capable of implementing required key lengths MUST be scheduled for replacement as a matter of urgency.

17.2.20. Using DSA (Legacy systems ONLY)

17.2.20.R.01. Rationale

       A modulus of at least 1024 bits for DSA is considered good practice by the cryptographic community.

17.2.20.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2141]

       Agencies using DSA, for the approved use of digital signatures, MUST use a modulus of at least 1024 bits.

17.2.21. Using ECDH

17.2.21.R.01. Rationale

       A field/key size of at least 384 bits for ECDH is now considered good practice by the cryptographic community.

17.2.21.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2144]

       Agencies using ECDH, for the approved use of agreeing on encryption session keys, MUST implement the curve P-384 (prime moduli).

17.2.21.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2145]

       All VPN's using an ECDH key length less than 384 MUST replace all Pre-Shared Keys with keys of at least 384 bits, as soon as possible.

17.2.22. Using ECDSA

17.2.22.R.01. Rationale

       A field/key size of at least 160 bits for ECDSA is considered good practice by the cryptographic community. Not all legacy systems support a modulus of this length, in which case significant risk is being carried.

17.2.22.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2148]

       Agencies using ECDSA, for the approved use of digital signatures, MUST implement the curve P-384 (prime moduli).

17.2.23. Using RSA (Legacy systems ONLY)

17.2.23.R.01. Rationale

       A modulus of at least 2048 bits for RSA is considered good practice by the cryptographic community.

17.2.23.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2151]

       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 2048 bits.

17.2.23.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2152]

       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.

17.2.24. Approved hashing algorithms

17.2.24.R.01. Rationale

       Recent research conducted by 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.

17.2.24.R.02. Rationale

       The use of SHA-1 is permitted ONLY in legacy systems where no other option exists.

17.2.24.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2155]

       Agencies MUST use the SHA-2 family before using SHA-1.

17.2.24.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:5905]

       Agencies SHOULD use a minimum of SHA-384.

17.2.25. Salts

17.2.25.R.01. Rationale

       The use of salts strengthens the resistance of hash values to a variety of attacks, including brute-force, rainbow table, dictionary and lookup table attacks.

17.2.25.R.02. Rationale

       Key derivation functions use a password, a salt, then generate a password hash. Their purpose is to make password guessing by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high and prohibitive.

17.2.25.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:6560]

Memorised secrets such as passwords MUST be stored in a form that is resistant to offline attacks.

17.2.25.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:6561]

Memorised secrets such as passwords SHOULD be salted and hashed using a suitable one-way key derivation function. See 17.2.24.

17.2.25.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:6562]

The salt SHOULD be at least 32 bits in length, be chosen arbitrarily, and each instance is unique so as to minimise salt value collisions among stored hashes.

17.2.26. Approved symmetric encryption algorithms

17.2.26.R.01. Rationale

The use of Electronic Code Book (ECB) 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.

17.2.26.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:2158]

Agencies using AES or 3DES SHOULD NOT use Electronic Code Book Mode (ECB).

17.2.27. Using 3DES (Legacy systems ONLY)

17.2.27.R.01. Rationale

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.

17.2.27.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:2161]

3DES MUST use either two distinct keys in the order key 1, key 2, key 1 or three distinct keys.

17.2.28. Using the Advanced Encryption Standard

17.2.28.R.01. Rationale

AES can operate in several modes. The Galois/Counter Mode (GCM) is the preferred AES mode, selected for its efficiency and performance.

17.2.28.R.02. Rationale

Galois/Counter Mode (GCM) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption. It can be implemented in hardware to achieve high speeds with low cost and low latency. Software implementations of GCM can achieve excellent performance by using table-driven field operations. It uses mechanisms that are supported by a well-understood theoretical foundation with security is based on the security of the block cipher.

17.2.28.R.03. Rationale

The two functions that comprise AES/GCM are described as authenticated encryption and authenticated decryption. The authenticated encryption function encrypts the data and computes an authentication tag. The authenticated decryption function decrypts the data, contingent on the verification of the tag.

17.2.28.R.04. Rationale

Implementation of AES may restrict the data to be encrypted to the non-confidential data. This variant of GCM is called GMAC. For GMAC, the authenticated encryption and decryption functions become the functions for generating and verifying an authentication tag on the non-confidential data.

17.2.28.R.05. Rationale

Refer to NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC for detailed application independent information. RFC 4106 and RFC 6379 describe the use of GCM in IPsec Encapsulating Security Payload (ESP). RFC 5288 describes the use of GCM in Transport Layer Security (TLS).

17.2.28.R.06. Rationale

The Cipher Block Chaining (CBC) mode is approved for use in IKEv2. NIST Special Publication 800-38A - Recommendations for Block Cipher Modes of Operation – Methods and Techniques, contains an application independent description of CBC. The AES-CBC cipher algorithm standard is defined in RFC 3602.

17.2.28.R.07. Rationale

Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) mode and Galois/Counter Mode Protocol (GCMP) are both approved for use in Wireless LAN Access Systems implementing the IEEE 802.11ac standard.

17.2.28.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:2170]

AES implementations for symmetric encryption of data SHOULD use the Galois/Counter Mode (GCM).

17.3. Approved Cryptographic Protocols

Objective

17.3.1. Classified information in transit is protected by an Approved Cryptographic Protocol implementing an Approved Cryptographic Algorithm.

Context

Scope

17.3.2. This section covers information on the cryptographic protocols that the GCSB recognises as being approved for use within government.   Implementations of the protocols in this section need to have successfully completed a GCSB recognised cryptographic evaluation before they can be approved for implementation.

17.3.3. High grade cryptographic protocols are **not** covered in this section.

Approved cryptographic protocols

17.3.4. In general, the GCSB only recognises the use of cryptographic products that have passed a formal evaluation. However, the GCSB may approve the use of some commonly available cryptographic protocols even though their implementations within specific products have not been formally evaluated. This approval is limited to cases where they are used in accordance with the requirements in this manual.

17.3.5. The Approved Cryptographic Protocols are:

- TLS;
- SSH;
- S/MIME;
- OpenPGP Message Format; and
- IPSec.

Rationale & Controls

17.3.6. Using Approved Cryptographic Protocols

17.3.6.R.01.   Rationale

If a product implementing an Approved Cryptographic Protocol has been inappropriately configured, it is possible that relatively weak cryptographic algorithms or implementations could be inadvertently selected. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

17.3.6.R.02.   Rationale

When configuring unevaluated products that implement an Approved Cryptographic Protocol, agencies can ensure that only the Approved Cryptographic Algorithm can be used by disabling the unapproved algorithms within the products (which is preferred). Alternatively a policy can be put in place to advise system users not to use the non-approved algorithms.

17.3.6.R.03.   Rationale

While many Approved Cryptographic Protocols support authentication, agencies should be aware that these authentication mechanisms are not foolproof. To be effective, these mechanisms MUST 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; and
- using a legitimate identity registration scheme.

17.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:2520]

Agencies using a product that implements an Approved Cryptographic Protocol MUST ensure that only Approved Cryptographic Protocols can be used.

17.4. Transport Layer Security

Objective

17.4.1. Transport Layer Security is implemented correctly as an approved protocol.

Context

Scope

17.4.2. This section covers the conditions under which TLS can be used as an approved cryptographic protocols. Additionally, as File Transfer Protocol over SSL is built on SSL/TLS, it is also considered within scope.

17.4.3. When using a product that implements TLS, requirements for using approved cryptographic protocols will also need to be referenced in the Section 17.3 - Approved Cryptographic Protocols.

17.4.4. Further information on handling TLS traffic through gateways can be found in Section 14.3 - Web Applications.

Background

17.4.5. **Secure Sockets Layer (SSL)**, and **Transport Layer Security (TLS)** are cryptographic protocols designed to provide communication security when using the Internet. They use X.509 certificates and asymmetric cryptography for authentication purposes. This generates a session key. This session key is then used to encrypt data between the parties.

17.4.6. Encryption with the session key provides data and message confidentiality, and message authentication codes for message integrity.

17.4.7. Several versions of the SSL and TLS protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP).

17.4.8. Although common usage has been to use the terms TLS and SSL interchangeably, they are distinct protocols.

17.4.9. TLS is an Internet Engineering Task Force (IETF) protocol, first defined in 1999, updated in RFC 5246 (August 2008) and RFC 6176 (March 2011). It is based on the earlier SSL specifications (1994, 1995, 1996) developed by Netscape Communications for adding the HTTPS protocol to their Navigator

web browser. A draft of TLS 1.3 was released in October 2014, with a definitive version issued in 2018.

17.4.10. Microsoft announced in October 2014 that that it will disable Secure Sockets Layer (SSL) 3.0 support in its Internet Explorer browser and in its Online Services, from Dec. 1, 2014.

SSL 3.0 Vulnerability

17.4.11. A design vulnerability has been found in the way SSL 3.0 handles block cipher mode padding. The Padding Oracle On Downgraded Legacy Encryption (POODLE) attack demonstrates how an attacker can exploit this vulnerability to decrypt and extract information from an encrypted transaction.

17.4.12. The POODLE attack demonstrates this vulnerability using web browsers and web servers, which is one of the most likely exploitation scenarios. All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable.

SSL Superseded

17.4.13. SSL is now superseded by TLS, with the latest version being TLS 1.3 which was released in August 2018. This is largely because of security flaws in the older SSL protocols.

17.4.14. Accordingly SSL is no longer an approved cryptographic protocol and it SHOULD be replaced by TLS.

References

17.4.15. Further information on SSL and TLS can be found at:

Title	Publisher	Source
The SSL 3.0 specification	IETF	https://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00
The TLS 1.2 specification	IETF	https://tools.ietf.org/html/rfc5246
The SSL 2.0 prohibition	IETF	https://tools.ietf.org/html/rfc6176
The Transport Layer Security (TLS) Protocol Version 1.3	IETF	https://tools.ietf.org/html/rfc8446
Vulnerability Summary for CVE-2014-3566	NIST	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
Alert (TA14-290A) - SSL 3.0 Protocol Vulnerability and POODLE Attack	US-CERT	https://www.us-cert.gov/ncas/alerts/TA14-290A
This POODLE Bites: Exploiting The SSL 3.0 Fallback	Google September 2014	http://www.openssl.org/~bodo/ssl-poodle.pdf

Rationale & Controls

17.4.16. Using TLS

17.4.16.R.01. Rationale

Whilst version 1.0 of SSL was never released, 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 1.3 which was released in August 2018. SSL is no longer an approved cryptographic protocol.

17.4.16.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2598]

Agencies SHOULD use the current version of TLS (version 1.3).

17.4.16.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:2600]

Agencies SHOULD NOT use any version of SSL.

17.5. Secure Shell

Objective

17.5.1. Secure Shell (SSH) is implemented correctly as an Approved Cryptographic Protocol.

References

17.5.2. Further references can be found at:

Title	Publisher	Source
Further information on SSH can be found in the SSH specification	IETF	http://tools.ietf.org/html/rfc4252
Further information on Open SSH	Open SSH	http://www.openssh.org
OpenSSH 7.3	Open SSH	http://www.openssh.com/txt/release-7.3

Context

Scope

17.5.3. SSH is software based on the Secure Shell protocol and enables a connection to a remote system.

17.5.4. This section covers information on the conditions under which commercial and open-source implementations of SSH can be used as an approved cryptographic protocol. Additionally, secure copy and Secure File Transfer Protocol use SSH and are therefore also covered by this section.

17.5.5. When using a product that implements SSH, requirements for using approved cryptographic protocols will also need to be referenced from the Section 17. 3 - Approved Cryptographic Protocols.

Rationale & Controls

17.5.6. Using SSH

17.5.6.R.01. Rationale

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.

17.5.6.R.02. Rationale

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.

17.5.6.R.03. Rationale

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 classified information.

17.5.6.R.04. Rationale

Host-based authentication requires no credentials (password, public key etc.) to authenticate although in some cases a host key can be used. This renders SSH vulnerable to an IP spoofing attack.

17.5.6.R.05. Rationale

An attacker who gains access to a system with system administrator privileges will have the ability to not only access classified information but to control that system completely. Given the clearly more serious consequences of this, system administrator login or administrator privilege escalation SHOULD NOT be permitted.

17.5.6.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2647]

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

17.5.7. Authentication mechanisms

17.5.7.R.01. Rationale

Public key-based systems have greater potential for strong authentication, put simply, people are not able to remember particularly strong passwords. Password-based authentication schemes are also more susceptible to interception than public key-based authentication schemes.

17.5.7.R.02. Rationale

Passwords are more susceptible to guessing attacks, so if passwords are used in a system then countermeasures should be put into place to reduce the chance of a successful brute force attack.

17.5.7.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2672]

Agencies SHOULD use public key-based authentication before using password-based authentication.

17.5.7.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2673]

Agencies that allow password authentication SHOULD use techniques to block brute force attacks against the password.

17.5.8. Automated remote access

17.5.8.R.01. Rationale

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.

17.5.8.R.02. Rationale

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.

17.5.8.R.03. Rationale

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.

17.5.8.R.04. Rationale

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.

17.5.8.R.05. Rationale

Allowing console access permits every user who logs into the console to run programs that are normally restricted to the root user.

17.5.8.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2725]

Agencies SHOULD use parameter checking when using the 'forced command' option.

17.5.8.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2726]

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; and
- console access.

17.5.8.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2727]

Agencies that use remote access without the use of a password SHOULD use the 'forced command' option to specify what command is executed.

17.5.9. SSH-agent

17.5.9.R.01. Rationale

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. Screenlocks and expiring key caches ensure that the user's private key is not left unlocked for long periods of time.

17.5.9.R.02. Rationale

Agent credential forwarding is required when multiple SSH connections are chained to allow each system in the chain to authenticate the user.

17.5.9.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2737]

Agencies that use SSH-agent or other similar key caching programs SHOULD:

- only use the software on workstation and servers with screenlocks;
- ensure that the key cache expires within four hours of inactivity; and
- ensure that agent credential forwarding is used when multiple SSH traversal is needed.

17.5.10. SSH-Versions

17.5.10.R.01. Rationale

Older versions contain known vulnerabilities which are regularly addressed or corrected by newer versions.

17.5.10.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2740]

Agencies SHOULD ensure that the latest implementation of SSH software is being used. Older versions contain known vulnerabilities.

17.6. Secure Multipurpose Internet Mail Extension

Objective

17.6.1. Secure Multipurpose Internal Mail Extension (S/MIME) is implemented correctly as an approved cryptographic protocol.

Context

Scope

17.6.2. This section covers information on the conditions under which S/MIME can be used as an approved cryptographic protocol.

17.6.3. When using a product that implements S/MIME, requirements for using approved cryptographic protocols will also need to be referenced from Section 17.3 - Approved Cryptographic Protocols.

17.6.4. Information relating to the development of password selection policies and password requirements can be found in Section 16.1 - Identification and Authentication.

References

17.6.5. Further information on S/MIME can be found at:

Title	Publisher	Source
Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	IETF	https://tools.ietf.org/html/rfc5751 https://datatracker.ietf.org/wg/smime
NIST SP800-57, Recommendations for Key Management	NIST	http://csrc.nist.gov/publications/PubsSPs.html

Rationale & Controls

17.6.6. Decommissioning

17.6.6.R.01. Rationale

Decommissioning MUST ensure any remanent cryptographic data is destroyed or unrecoverable.

17.6.6.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:2769]

Decommissioning of faulty or redundant equipment MUST comply with media sanitisation requirements described in Chapter 12 – Product Security.

17.6.7. Using S/MIME

17.6.7.R.01. Rationale

S/MIME 2.0 used 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 Taskforce (IETF) standard.

17.6.7.R.02. Rationale

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.

17.6.7.R.03. Rationale

Improper decommissioning and sanitisation presents opportunities for harvesting Private Keys. Products that hosted multiple Private Keys for the management of multiple identities should be considered points of aggregation with an increased "target value". Where cloud based computing services have been employed, media sanitisation may be problematic and require the revocation and re-issue of new keys.

17.6.7.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:2780]

Agencies MUST NOT allow versions of S/MIME earlier than 3.0 to be used.

17.7. OpenPGP Message Format

Objective

17.7.1. OpenPGP Message Format is implemented correctly as an Approved Cryptographic Protocol.

Context

Scope

17.7.2. This section covers information on the conditions under which the OpenPGP Message Format can be used as an approved cryptographic protocol. It applies to the protocol as specified in IETF's RFC 2440 and RFC 4880, which supercedes RFC 2440.

17.7.3. When using a product that implements the OpenPGP Message Format, requirements for using approved cryptographic protocols will also need to be referenced from the Section 17.3 - Approved Cryptographic Protocols.

17.7.4. Information relating to the development of password selection policies and password requirements can be found in the Section 16.1 - Identification and Authentication.

References

17.7.5. Further information on the OpenPGP Message Format can be found at:

Title	Publisher	Source
OpenPGP Message Format specification	IETF	http://tools.ietf.org/html/rfc4880

Rationale & Controls

17.7.6. Using OpenPGP Message Format

17.7.6.R.01. Rationale

If the private certificate and associated key used for encrypting messages is suspected of being compromised i.e. 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 as third parties could intercept the message and decrypt it using the private key.

17.7.6.C.01.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:2806]

Agencies MUST immediately revoke key pairs when a private certificate is suspected of being compromised or leaves the control of the agency.

17.8. Internet Protocol Security (IPSec)

Objective

17.8.1. Internet Protocol Security (IPSec) is correctly implemented.

Context

Scope

17.8.2. This section covers information on the conditions under which IPSec can be used as an Approved Cryptographic Protocol.

17.8.3. When using a product that implements IPSec, requirements for using approved cryptographic protocols will also need to be referenced from Section 17.3 Approved Cryptographic Protocols.

Modes of operation

17.8.4. IPSec can be operated in two modes: transport mode or tunnel mode.

Cryptographic algorithms

17.8.5. Most IPSec implementations can accommodate a number of cryptographic algorithms for encrypting data when the Encapsulating Security Payload (ESP) protocol is used. These include 3DES and AES.

Key exchange

17.8.6. Most IPSec implementations facilitate 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

17.8.7. Most IPSec implementations can select from a number of methods for authentication as part of ISAKMP. These can include digital certificates, encrypted nonces or pre-shared keys. All these methods are considered suitable for use.

ISAKMP modes

17.8.8. ISAKMP uses two modes to exchange information as part of IKE. These are main mode and aggressive mode.

References

17.8.9. Further information on IPSec can be found at:

Title	Publisher	Source
Security Architecture for the IP overview	IETF	http://tools.ietf.org/html/rfc2401
NIST 800-77, Rev 1, Guide to IPSec VPNs, June 2020	NIST	https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final

Rationale & Controls

17.8.10. Mode of operation

17.8.10.R.01. Rationale

The tunnel mode of operation provides full encapsulation of IP packets whilst the transport mode of operation only encapsulates the payload of the IP packet.

17.8.10.C.01.   Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2842]

Agencies SHOULD use tunnel mode for IPSec connections.

17.8.10.C.02.   Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2843]

Agencies choosing to use transport mode SHOULD additionally use an IP tunnel for IPSec connections.

17.8.11. Protocol

17.8.11.R.01. Rationale

In order to provide a secure VPN style connection both authentication and encryption are needed. ESP is the only way of providing encryption yet Authentication Header (AH) and ESP can provide authentication for the entire IP packet and the payload respectively. ESP is generally preferred for authentication though as AH has inherent network address translation limitations.

17.8.11.R.02. Rationale

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.

17.8.11.C.01.   Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:2847]

Agencies SHOULD use the ESP protocol for IPSec connections.

17.8.12. ISAKMP modes

17.8.12.R.01. Rationale

Using main mode instead of aggressive mode provides greater security since all exchanges are protected.

17.8.12.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2850]

Agencies using ISAKMP SHOULD disable aggressive mode for IKE.

17.8.13. Security association lifetimes

17.8.13.R.01. Rationale

Using a secure association lifetime of four hours or 14400 seconds provides a balance between security and usability.

17.8.13.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2853]

Agencies SHOULD use a security association lifetime of four hours or 14400 seconds, or less.

17.8.14. HMAC algorithms

17.8.14.R.01. Rationale

MD5 and SHA-1 are no longer approved Cryptographic Protocols. The approved algorithms that can be used with HMAC are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512.

17.8.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2856]

Agencies SHOULD use HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 as the HMAC algorithm.

17.8.15. DH groups

17.8.15.R.01. Rationale

Using a larger DH group provides more entropy for the key exchange.

17.8.15.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2859]

Agencies SHOULD use the largest modulus size available for the DH exchange.

17.8.16. Perfect Forward Secrecy

17.8.16.R.01. Rationale

Using Perfect Forward Secrecy reduces the impact of the compromise of a security association.

17.8.16.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2862]

Agencies SHOULD use Perfect Forward Secrecy for IPSec connections.

17.8.17. IKE Extended Authentication

17.8.17.R.01. Rationale

XAUTH using IKEv1 has documented vulnerabilities associated with its use.

17.8.17.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:2865]

Agencies SHOULD disable the use of XAUTH for IPSec connections using IKEv1.

17.9. Key Management

Objective

17.9.1. Cryptographic keying material is protected by key management procedures.

Context

Scope

17.9.2. This section covers information relating to the general management of cryptographic system material. Because there is a wide variety of cryptographic systems and technologies available, and there are varied security risks for each, detailed key management guidance is not provided in this manual.

17.9.3. If HGCP or HGCE is being used, agencies are advised to consult the respective NZCSI national standards for the respective equipment.

17.9.4. In a cloud enviroment it is possible to outsource the control of cryptographic key to the cloud service provider, Hold Your Own Keys (HYOK) and Bring Your Own Keys (BYOK). It is important to note that there is little distinction between HYOK and BYOK.

17.9.5. Hold Your Own Keys (HYOK) generally refers to the management of keys by the agency or organisation where keys may be generated by the agency or by a third party such as a National Authority or a Certificate Authority. The agency retains full control of the management of keys.

17.9.6. Bring Your Own Keys (BYOK) also refers to the management of keys by the agency or organisation. In this case keys are provided to the cloud service (or other service) providers for use on outsourced services related to that agency. In such cases, the agency relinquishes some elements of control of the use, storage and protection of the keys.

Applicability for cryptographic systems

17.9.7. In general, the requirements specified in this manual for systems apply equally to cryptographic systems. Where the requirements for cryptographic systems are different, the variations are contained in this section, and take precedence over requirements specified elsewhere in this manual.

Background

17.9.8. Encryption is an unparalleled technology for the protection of information but it relies on the strength of the algorithm, the strength of the key and, most importantly, strong key management.

17.9.9. All encryption has four important characteristics:

- The data to be protected;
- The algorithm used to encrypt the data;
- The protocol used to apply the algorithm; and
- The encryption key.

17.9.10. In almost all cases the algorithm is in the public domain and is not a secret. When an encryption algorithm is publically available, security rests entirely on the secrecy of the encryption key. It is also true that the effectiveness of most encryption systems depends on the secrecy of the encryption key.   Approved Cryptographic Algorithms are described in Section 17.2. and Approved Cryptographic Protocols (applying the algorithms) are described in Section 17.3. These sections also specify key strengths to resist attempts to compromise the key through cryptanalysis.

17.9.11. While any algorithm can, theoretically, be broken through cryptanalysis, this may require the use of vast computing power and other resources, making this approach infeasible. If, however, the encryption key is compromised, there is no need to attack the algorithm itself. Attacks on encryption systems will always target the weakest point, the protection of the key. Attempts to compromise keys and key management are more likely and more efficient than attacks on the algorithm itself. This is why strong key management is vital in order to protect the encryption key and keep the key secure and secret. When key management fails, cryptographic security is compromised.

17.9.12. In today's Internet-connected world, almost all Internet security protocols use cryptography for authentication, integrity, confidentiality and non-repudiation. It is vital that good key management is implemented if these security protocols are to be protected, considered reliable and provide required levels of assurance to organisations and users.

17.9.13. In some cases, trusted third-party key management service providers furnish assistance to agencies in the generation, storage, operation, management and retirement (disposal) of keys associated with the agency.

Key Management

17.9.14. For encryption to be used effectively, the encryption keys must be managed with the same care and security as the data encrypted by those keys for the entire lifetime of those keys.

17.9.15. Key Management encompasses the operations and tasks necessary to create, protect and control the use of cryptographic keys. The process from creation to destruction of the encryption key is described as the key management life cycle.

Key Management Life Cycle

17.9.16. The key management lifecycle covers:

- Key generation;
- Key registration;
- Secure key storage;
- Key distribution and installation;
- Key use;
- Key rotation;
- Key backup (operational, backup and archive);
- Key replacement and reissue;
- Key recovery;
- Key revocation;
- Key suspension;
- Key retirement; and
- Key destruction.

Open Networks

17.9.17. Open networks, by definition, seek to establish arbitrary connections without there necessarily being a pre-existing relationship. Protocols have been developed to manage this requirement through key exchange protocols and through trusted agents, most often a National Authority or Certificate Authority. Again it is important that approved protocols and algorithms, as specified in this document, are used. Refer to sections 17.2 Approved Cryptographic Algorithms and 17.3 Approved Cryptographic Protocols.

Public Key Infrastructure

17.9.18. Public Key Infrastructure was first publically discussed in the early 1970's with some of the first PKI standards from the IETF published in the 1990's. PKI is the system to create, issue, manage and revoke digital certificates and their associated cryptographic keys. PKI has many different applications but typically is used primarily for encrypting and digitally signing data in order to authenticate and protect data in transmission, supporting confidentiality and privacy. It is used extensively in ecommerce, internet banking and secure email as well as being a key element in protecting website traffic.

Risks

17.9.19. There are a number of specific risks related to the management of cryptographic keys. These include:

- Keys exposed to unauthorised persons or applications, potentially compromising the keys or data the encryption is protecting;
- Data breaches;
- Lost or unrecoverable cryptographic keys;
- Software based key management, which provides only limited protection;
- Fragmented key management as new systems are introduced; and
- Poorly documented and understood key management processes and activities increasing the possibility of compromise and potentially increasing compliance costs.

Prioritisation

17.9.20. Prioritisation helps identify and manage requirements for the use and management of cryptography and key management systems. This will determine the extent and complexity of the key management programme. Important aspects to consider are:

- Sensitivity and value of the data. This is summarised by the classification of the data but may not always reflect the values of aggregation, cost of compliance breaches or reputation damage from a breach.
- The volume of data and keys.
- The variety of key types, data formats, algorithms, protocols and sources.
- The speed and frequency of transactions, requirements for data access and availability.

References

17.9.21. The NZCSI and NZCSS series of policy documents should be consulted for additional information on high grade cryptography.

17.9.22. Further information on key management practices can be found in the following references:

Title	Publisher	Description & Source
ISO 11568-1:2005 Banking -- Key management (retail) -- Part 1: Principles	ISO / IEC	Specifies the principles for the management of keys used in cryptosystems implemented within the retail-banking environment. Focused mainly on card transactions and devices. http://www.iso.org
ISO 11568-2:2012 Financial services -- Key management (retail) -- Part 2: Symmetric ciphers, their key management and life cycle	ISO / IEC	http://www.iso.org
ISO 11568-4:2007 Banking -- Key management (retail) -- Part 4: Asymmetric cryptosystems -- Key management and life cycle	ISO / IEC	http://www.iso.org
ISO/IEC 11770-1:2010, Information Technology – Security Techniques – Key Management -- Part 1: Framework	ISO / IEC	This standard describes the concepts of key management and some concept models for key distribution. http://www.iso.org
ISO/IEC 11770-2:2008 Information technology -- Security techniques -- Key management -- Part 2:	ISO / IEC	Mechanisms using symmetric techniques http://www.iso.org
ISO/IEC 11770-3:2015 Information technology -- Security techniques -- Key management -- Part 3:	ISO / IEC	Mechanisms using asymmetric techniques http://www.iso.org
June 2005, RFC 4107, Guidelines for Cryptographic Key Management	IETF	This document specifies an Internet Best Current Practices for the Internet Community https://tools.ietf.org/pdf/rfc4107.pdf
Public Key Cryptography Standards	IETF	Numbered #1 through #15 with some withdrawn (#4) or not completed (#13, #14). A series of Public Key Cryptography Standards. https://tools.ietf.org
RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP	IETF	https://tools.ietf.org/html/rfc2407
RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)	IETF	https://tools.ietf.org/html/rfc2408
RFC 2409, The Internet Key Exchange (IKE)	IETF	https://tools.ietf.org/html/rfc2409
August, 2013: NIST Special Publication (SP) 800-130, A Framework for Designing Cryptographic Key Management Systems.	NIST	This publication contains a description of the topics to be considered and the documentation requirements to be addressed when designing a CKMS. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf
April 2013, Special Publication 800-53 R4, Security and Privacy Controls for Federal Information Systems	NIST	Security and Privacy Controls for Federal Information Systems and Organizations updated 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
December 2014 Special Publication 800-53A, R4 Assessing the Security Controls for Federal Information Systems	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

January, 2016: Revision 4 of Special Publication (SP) 800-57, Part 1, Recommendation for Key Management, Part 1: General.	NIST	This publication contains basic key management guidance, including the security services that may be provided and the key types that may be employed in using cryptographic mechanisms, the functions involved in key management, and the protections and handling required for cryptographic keys. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
SP 800-57 Part 2, Recommendation for Key Management - Part 2: Best Practices for Key Management Organizations	NIST	This recommendation provides guidance for system and application owners for use in identifying appropriate organisational key management infrastructures, establishing organizational key management policies, and specifying organisational key management practices. http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf
January 2015: NIST Special Publication 800-57 Part 3 Revision 1, Recommendation for Key Management Part 1: General	NIST	This document provides guidance on the use of application-specific key management. http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part3.pdf
December 21, 2012: NIST Special Publication (SP) 800-133, Recommendation for Cryptographic Key Generation	NIST	This Recommendation discusses the generation of the keys to be used with approved cryptographic algorithms. http://dx.doi.org/10.6028/NIST.SP.800-133
November, 2015: Special Publication (SP) 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.	NIST	This Recommendation provides the approach for transitioning from the use of one algorithm or key length to another. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
Federal Information Processing Standards Publication FIPS Pub 140-2 Security Requirements For Cryptographic Modules	NIST	This standard includes Annexes A-D and covers physical security as well as key management and design assurance. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
NISTIR 7609 January 2010 Cryptographic Key Management Workshop Summary	NIST	Summary of workshop to develop and enhance key management standards. http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7609.pdf
PCI Data Security Standards	PCI	Requirements and Security Assessment Procedures Version 3.2 April 2016 https://www.pcisecuritystandards.org
Enterprise Key Management Infrastructure (EKMI)	OASIS	Guidance on standardising management of symmetric encryption cryptographic keys across the enterprise https://www.oasis-open.org
Key Management Interoperability Protocol (KMIP)	OASIS	Interoperability standard for enterprise encryption key management https://www.oasis-open.org
Guidelines on Cryptographic Algorithms Usage and Key Management December 2016	European Payments Council	http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/guidelines-on-cryptographic-algorithms-usage-and-key-management/

17.9.23. Further information on key establishment can be found in the following references:

Key Establishment		
June 5, 2013: SP 800-56A Revision 2: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	NIST	The revisions are made on the March 2007 version of this Recommendation. The major revisions are summarized in Appendix D. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

August 27, 2009: SP 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography	NIST	This Recommendation provides the specifications of key establishment schemes that are based on a standard developed by the Accredited Standards Committee (ASC) X9, Inc.: ANS X9.44, Key Establishment using Integer Factorization Cryptography. SP 800-56B provides asymmetric-based key agreement and key transport schemes that are based on the Rivest Shamir Adleman (RSA) algorithm. http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf
December 11, 2011: NIST SP 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion	NIST	This Recommendation specifies techniques for the derivation of keying material from a shared secret established during a key establishment scheme defined in NIST Special Publications 800-56A or 800-56B through an extraction-then-expansion procedure. http://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf
December 2012: NIST has published an ITL Bulletin that summarizes NIST SP 800-133: Recommendation for Cryptographic Key Generation.	NIST	http://csrc.nist.gov/publications/nistbul/itlbul2012_12.pdf http://csrc.nist.gov/groups/ST/toolkit/key_management.html
NIST Special Publication 800-38F, December 2012 - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping	NIST	http://dx.doi.org/10.6028/NIST.SP.800-38F
Public Key Cryptography Standards	IETF	Numbered #1 through #15 with some withdrawn (#4) or not completed (#13, #14). A series of Public Key Cryptography Standards. https://tools.ietf.org

Rationale & Controls

17.9.24. Developing Key Management Plans (KMPs)

17.9.24.R.01. Rationale

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 New Zealand national or allied national. Cryptographic system material is safeguarded by implementing strong personnel, physical, documentation and procedural security measures.

17.9.24.R.02. Rationale

Cryptographic system material is safeguarded by implementing strong key management plan (KMP) encompassing personnel, physical, documentation and procedural security measures.

17.9.24.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3016]

Agencies MUST develop a KMP when they have implemented a cryptographic system using HGCP.

17.9.24.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3017]

The level of detail included in a KMP MUST be consistent with the criticality and classification of the information to be protected.

17.9.24.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3018]

Agencies SHOULD develop a KMP when they have implemented a cryptographic system using commercial grade cryptographic equipment.

17.9.25. Contents of KMPs

17.9.25.R.01. Rationale

When agencies implement the recommended contents for KMPs they will have a good starting point for the protection of cryptographic systems and their material within their agencies.

17.9.25.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3021]

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

Topic	Content
Objectives	• Objectives of the cryptographic system and KMP, including organisational aims. • Refer to relevant NZCSIs.

System description	• The environment. • Maximum classification of information protected. • Topology Diagram(s) and description of the cryptographic system topology including data flows. • The use of keys. • Key algorithm. • Key length. • Key lifetime.
Roles and administrative responsibilities.	Documents roles and responsibilities, including the: • COMSEC Custodian; • Cryptographic systems administrator; • Record keeper; and • Auditor
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 cryptographic system software. • Classification of the cryptographic system documentation.
Information 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 information 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 equipment and media.
References	• Vendor documentation • Related policies.

17.9.26. Accounting

17.9.26.R.01. Rationale

As cryptographic equipment, and the keys they store, provide a significant security function for systems it is important that agencies are able to account for all cryptographic equipment.

17.9.26.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3024]

Agencies MUST be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.

17.9.26.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3025]

Agencies SHOULD be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.

17.9.27. Audits, compliance and inventory checks

17.9.27.R.01. Rationale

Cryptographic system audits are used as a process to account for cryptographic equipment.

17.9.27.C.01. Control

Agencies MUST conduct audits using two personnel with cryptographic system administrator access.

17.9.27.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3029]

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; and
- at least annually.

17.9.27.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3030]

Agencies SHOULD perform audits to:

- account for all cryptographic system material; and
- confirm that agreed security measures documented in the KMP are being followed.

17.9.28. Access register

17.9.28.R.01. Rationale

Access registers can assist in documenting personnel that have privileged access to cryptographic systems along with previous accounting and audit activities for the system.

17.9.28.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3033]

Agencies MUST 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; and
- audit activities.

17.9.29. Cryptographic system administrator access

17.9.29.R.01. Rationale

The cryptographic system administrator is a highly privileged position which involves granting privileged access to a cryptographic system. Therefore extra precautions need to be put in place surrounding the security and vetting of the personnel as well as the access control procedures for individuals designated as cryptographic system administrators.

17.9.29.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3036]

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 Key Management Policy and Plan (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 the GCSB; and
- ensure relevant staff have received appropriate training.

17.9.30. Area security and access control

17.9.30.R.01. Rationale

As cryptographic equipment contains particularly sensitive information additional physical security measures need to be applied to the equipment.

17.9.30.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3039]

Cryptographic system 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.

17.9.30.C.02. Control

Areas in which cryptographic system material is used SHOULD be separated from other areas and designated as a controlled cryptography area.

17.9.31. High Assurance Cryptographic Equipment (HACE)

17.9.31.R.01. Rationale

The NZCSI series of documents provide product specific policy for HACE.

17.9.31.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3043]

Agencies MUST comply with NZCSI when using HACE.

17.9.32. Transporting commercial grade cryptographic equipment & products

17.9.32.R.01. Rationale

Transporting commercial grade cryptographic equipment in a keyed state exposes the equipment to the potential for interception and compromise of the key stored within the equipment. As such when commercial grade cryptographic equipment is transported in a keyed state it needs to be done so according to the requirements for the classification of the key stored in the equipment.

17.9.32.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3048]

Unkeyed commercial grade cryptographic equipment MUST be distributed and managed by a means approved for the transportation and management of government property.

17.9.32.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3050]

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 within the equipment.

17.9.32.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3053]

Agencies SHOULD NOT transport commercial grade cryptographic equipment or products in a keyed state.

17.10. Hardware Security Modules

Objective

17.10.1. Hardware Security Modules are used where additional security of cryptographic functions is desirable.

Context

Scope

17.10.2. This section covers information relating to Hardware Security Modules (HSMs). Detailed key management guidance is provided in Section 17.9 – Key Management.

Hardware Security Module

17.10.3. Hardware Security Modules (HSMs) are defined as a hardware module or appliance which provides cryptographic functions. HSM's can be integrated into a design, installed in a host or be externally connected. HSM's can be packaged as discrete appliances, PCI cards, USB devices, smartcards or other form factors.

17.10.4. Functions include (but are not limited to) encryption, decryption, key generation, signing, hashing and cryptographic acceleration. The appliance usually also offers some level of physical tamper-resistance, has a user interface and a programmable interface for key management, configuration and firmware or software updates.

Usage

17.10.5. HSMs are used in high assurance security solutions that satisfy widely established and emerging standards of due care for cryptographic systems and practices—while also maintaining high levels of operational efficiency. Traditional use of HSMs is within automatic teller machines, electronic fund transfer, and point-of-sale networks. HSMs are also used to secure CA keys in PKI deployments, SSL acceleration and DNSSEC (DNS Security Extensions) implementations.

Physical Security

17.10.6. HSM's usually describe an encapsulated multi-chip module, device, card or appliance, rather than a single chip component or device. The nature of HSM's requires more robust physical security, including tamper resistance, tamper evidence, tamper detection, and tamper response.

Tamper Resistance

17.10.7. Tamper Resistance is designed to limit the ability to physically tamper with, break into or extract useful information from an HSM. Often the boards and components are encased in an epoxy-like resin that will destroy any encapsulated components when drilled, scraped or otherwise physically tampered with.

Tamper Evidence

17.10.8. The HSM is designed so that any attempts at tampering are evident. Many devices use seals and labels designed break or reveal a special message when physical tampering is attempted. Tamper evidence may require a regular inspection or audit mechanism.

17.10.9. HSMs can include features that detect and report tampering attempts. For example, embedding a conductive mesh within the epoxy-like package; internal circuitry monitored the electrical proper-ties of this mesh — properties which physical tamper would disrupt. Devices can also monitor for temperature extremes, radiation extremes, light, air and other unusual conditions.

Tamper Response

17.10.10. HSMs can include defensive features that activate when tampering is detected. For example, cryptographic keys and sensitive data are deleted or zeroised. A trade-off exists between availability and security as an effective tamper response essentially renders the HSM unusable.

References

17.10.11. Further references can be found at:

Title	Publisher	Source
Payment Card Industry (PCI) Hardware Security Module (HSM) - Security Requirements - Version 1.0, April 2009	PCI	https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf
FIPS PUB 140-2 - Effective 15-Nov-2001 - Security Requirements for Cryptographic Modules	NIST	http://csrc.nist.gov/groups/STM/cmvp/standards.html

17.10.12 Hardware Security Modules

17.10.12.R.01. Rationale

Where high assurance or high security is required or high volumes of data are encrypted or decrypted, the use of an HSM should be considered when designing the network and security architectures.

17.10.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3103]

Agencies MUST consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.

17.10.12.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3105]

Agencies MUST follow the product selection guidance in this manual. See Chapter 12 – Product Security.

17.10.12.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3108]

Agencies SHOULD consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.

17.10.12.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3110]

Agencies SHOULD follow the product selection guidance in this manual. See Chapter 12 – Product Security.

18. Network security

18.1. Network Management

Objective

18.1.1.   Any change to the configuration of networks is authorised and controlled through appropriate change management processes to ensure security, functionality and capability is maintained.

Context

Scope

18.1.2.   This section covers information relating to the selection, management and documentation of network infrastructure.

Network diagrams

18.1.3.   An agency's network diagrams should illustrate all network devices including firewalls, IDSs, IPSs, routers, switches, hubs, etc. It does not need to illustrate all IT equipment on the network, such as workstations or printers which can be collectively represented. The inclusion of significant devices such as MFD's and servers can aid interpretation.

Systems Documentation

18.1.4.   Knowledge of systems design, equipment and implementation is a primary objective of those seeking to attack or compromise systems or to steal information. System documentation is a rich source allowing attackers to identify design weaknesses and vulnerabilities. The security of systems documentation is therefore important in preserving the security of systems.

18.1.5.   Detailed network documentation and configuration details can contain information about IP addresses, port numbers, host names, services and protocols, software version numbers, patch status, security enforcing devices and information about information compartments and enclaves containing highly valuable information. This information can be used by a malicious actor to compromise an agency's network.

18.1.6.   This information may be particularly exposed when sent to offshore vendors, consultants and other service providers. Encrypting this data will provide an important protective measure and assist in securing this data and information.

18.1.7.   Reference should also be made to Section 12.7 – Supply Chain.

PSR references

18.1.8.   Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/
PSR content protocols	Management protocol for information security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Supply chain security Understand the information security lifecycle	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/governance/supply-chain-security/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/

Managing specific scenarios	Outsourced ICT facilities Outsourcing, Offshoring and supply chains Communication security Mobile and remote working Physical security for ICT systems Working away from the office	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/outsourced-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/communications-security/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/working-away-from-your-office/

Rationale & Controls

18.1.9.   Classification of Network Documentation

18.1.9.R.01.   Rationale

To provide an appropriate level of protection to systems and network documentation, a number of security aspects should be considered. These include:

- the existence of the system;
- the intended use;
- the classification of the data to be carried or processed by this system;
- the connectivity and agencies connected;
- protection enhancements and modifications; and
- the level of detail included in the documentation.

High level conceptual diagrams and accompanying documentation should also be subject to these considerations

18.1.9.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3170]

Agencies MUST perform a security risk assessment before providing network documentation to a third party, such as a commercial provider or contractor.

18.1.9.C.02.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3172]

Systems documentation and detailed network diagrams MUST be classified at least to the level of classification of the data to be carried on those systems.

18.1.9.C.03.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3174]

Network documentation provided to a third party, such as to a commercial provider or contractor, MUST contain only the information necessary for them to undertake their contractual services and functions, consistent with the need-to-know principle.

18.1.9.C.04.   Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:3176]

Detailed network configuration information MUST NOT be published in tender documentation.

18.1.9.C.05.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3179]

Security aspects SHOULD be considered when determining the classification level of systems and network documentation.

18.1.10. Configuration management

18.1.10.R.01.   Rationale

If the network is not centrally managed, there could be sections of the network that do not comply with the agency's security policies, and thus create a vulnerability.

18.1.10.R.02.   Rationale

Changes should be authorised by a change management process, including 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.

18.1.10.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3188]

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

18.1.10.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3190]

All changes to the configuration SHOULD be documented and approved through a formal change control process.

18.1.10.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3191]

Agencies SHOULD regularly review their network configuration to ensure that it conforms to the documented network configuration.

18.1.10.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3192]

Agencies SHOULD deploy an automated tool that compares the running configuration of network devices against the documented configuration.

18.1.11. Network diagrams

18.1.11.R.01.   Rationale

As most decisions are made on the documentation that illustrates the network, it is important that:

- a network diagram exists;
- the security architecture is recorded;
- the network diagram is an accurate depiction of the network; and
- the network diagram indicates when it was last updated.

18.1.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3195]

For each network an agency manages they MUST have:

- a high-level diagram showing all connections and gateways into the network; and
- a network diagram showing all communications equipment.

18.1.12. Updating network diagrams

18.1.12.R.01. Rationale

Because of the importance of the network diagram and decisions made based upon its contents, it should be updated as changes are made. This will assist system administrators to completely understand and adequately protect the network.

18.1.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3198]

An agency's network diagrams MUST:

- be updated as network changes are made; and
- include a 'Current as at [date]' statement on each page.

18.1.12.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3199]

An agency's network diagrams SHOULD:

- be updated as network changes are made; and
- include a 'Current as at [date]' statement on each page.

18.1.13. Limiting network access

18.1.13.R.01. Rationale

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 against attackers traversing 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.

18.1.13.R.02. Rationale

Although circumventing some network access controls can be trivial, their use is primarily aimed at the protection they provide against accidental connection to another network.

18.1.13.R.03. Rationale

The design of a robust security architecture is fundamental to the security of a system. This may include concepts such as trust zones, application of the principles of separation and segregation through, for example, segmented networks and VPNs and other design techniques.

18.1.13.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3204]

Agencies MUST implement network access controls on all networks.

18.1.13.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3205]

Agencies SHOULD implement network access controls on all networks.

18.1.14. Management traffic

18.1.14.R.01. Rationale

Implementing protection measures specifically for management traffic provides another layer of defence on the network. This also makes it more difficult for an attacker to accurately define their target network.

18.1.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3208]

Agencies SHOULD implement protection measures to minimise the risk of unauthorised access to network management traffic on a network.

18.1.15. Simple Network Management IT Protocol (SNMP)

18.1.15.R.01. Rationale

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices such as switches, routers and wireless access points. Early versions of SNMP were insecure. SNMPv3 uses stronger authentication methods but continues to establish default SNMP community strings and promiscuous access. Encryption may be used as an additional assurance measure but this may create additional workload in investigating faults. An assessment of risk, threats and the agency's requirements may be required to determine an appropriate configuration.

18.1.15.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3211]

Agencies SHOULD NOT use SNMP unless a specific requirement exists.

18.1.15.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3238]

Agencies SHOULD implement SNMPv3 where a specific SNMP requirement exists.

18.1.15.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3239]

Agencies SHOULD change all default community strings in SNMP implementations.

18.1.15.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3240]

SNMP access SHOULD be configured as read-only.

18.2. Wireless Local Area Networks

Objective

18.2.1.   Wireless local area networks are deployed in a secure manner that does not compromise the security of information and systems.

Context

Scope

18.2.2.   This section covers information on 802.11x WLANs. It does not cover other wireless communications. These communication methods are covered in Chapter 11 - Communications Systems and Devices. The description 802.11x refers to all versions and 802.11 standards.

Title	Publisher	Source
802.11 Wi-Fi	IEEE	Wireless LAN Media Access Control and Physical Layer specification. 802.11a,b,g,etc. are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified".
802.15 Wireless Personal Area Networks	IEEE	Communications specification that was approved in early 2002 by the IEEE for wireless personal area networks (WPANs and includes Bluetooth, Ultrs Wideband, Zigbee and Mesh Networks.
802.16 Wireless Metropolitan Area Networks	IEEE	This family of standards covers Fixed and Mobile Broadband Wireless Access methods used to create Wireless Metropolitan Area Networks (WMANs.) Connects Base Stations to the Internet using OFDM in unlicensed (900 MHz, 2.4, 5.8 GHz) or licensed (700 MHz, 2.5 – 3.6 GHz) frequency bands. Products that implement 802.16 standards can undergo WiMAX certification testing.

18.2.3.   Hardware Security Modules (HSMs) are defined as a hardware module or appliance that provides cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The appliance usually also offers some level of physical tamper-resistance and has a user interface and a programmable interface. Refer also to Section 17.10 – Hardware Security Modules.

References

18.2.4.   Further references can be found at:

Title	Publisher	Source
Implementing Network Segmentation and Segregation, June 2020	ASD	https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation
Wi-Fi Alliance certification programs	Wi-Fi Alliance	http://www.wi-fi.org/certification_programs.php
802.11	IEEE	http://standards.ieee.org/findstds/standard/802.11-2012.html
EAP specification	IETF	http://tools.ietf.org/html/rfc5247
EAP-TLS specification	IETF	http://tools.ietf.org/html/rfc5216
EAP-TTLS specification	IETF	http://tools.ietf.org/html/rfc5281
Payment Card Industry (PCI) Hardware Security Module (HSM) - Security Requirements - Version 1.0, April 2009	PCI	https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf
FIPS PUB 140-2 - Effective 15-Nov-2001 - Security Requirements for Cryptographic Modules	NIST	http://csrc.nist.gov/groups/STM/cmvp/standards.html
Extensible Authentication Protocol	Microsoft	https://technet.microsoft.com/en-us/network/bb643147.aspx

Rationale & Controls

18.2.5.   Bridging networks

18.2.5.R.01. Rationale

When connecting devices via Ethernet to an agency's fixed network, agencies need to be aware of the risks posed by active wireless functionality. Devices may automatically connect to any open wireless networks they have previously connected to, which a malicious actor can use to masquerade and establish a connection to the device. This compromised device could then be used as a bridge to access the agency's fixed network. Disabling wireless functionality on devices, preferably by a hardware switch, whenever connected to a fixed network can prevent this from occurring. Additionally, devices do not have to be configured to remember and automatically connect to open wireless networks that they have previously connected to.

18.2.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:3274]

Devices MUST NOT be configured to remember and automatically connect to any wireless networks that they have previously connected to.

18.2.5.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3282]

Wireless auto-connect functionality on devices SHOULD be disabled, preferably by a hardware switch, whenever connected to a fixed network.

18.2.6. Providing wireless communications for public access

18.2.6.R.01. Rationale

To ensure that a wireless network provided for public access cannot be used as a launching platform for attacks against an agency's system it MUST be **separated** from all other systems. Security architectures incorporating segmented networks, DMZ's and other segregation mechanisms are useful in this regard.

18.2.6.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3290]

Agencies deploying a wireless network for public access MUST **separate** it from any other agency networks; including BYOD networks.

18.2.7. Using wireless communications

18.2.7.R.01. Rationale

As the Accreditation Authority for TOP SECRET systems, GCSB has mandated that all agencies considering deploying a wireless TOP SECRET deployment seek approval from GCSB prior to initiating any networking projects.

18.2.7.C.01. Control System Classification(s): Top Secret; Compliance: MUST NOT [CID:3298]

Agencies MUST NOT use wireless networks unless the security of the agency's wireless deployment has been approved by GCSB.

18.2.8. Selecting wireless access point equipment

18.2.8.R.01. Rationale

Wireless access points that have been certified in a Wi-Fi Alliance certification program provide an agency with assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points on a wireless network will limit incompatibility of wireless equipment and incorrect implementation of wireless devices by vendors.

18.2.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3302]

All wireless access points used for government wireless networks MUST be Wi-Fi Alliance certified.

18.2.9. 802.1X Authentication

18.2.9.R.01. Rationale

A number of Extensible Authentication Protocol (EAP) methods, supported by the Wi-Fi Protected Access 2 (WPA2) protocol, are available.

18.2.9.R.02. Rationale

Agencies deploying a secure wireless network can choose WPA2-Enterprise with EAP-Transport Layer Security (EAP-TLS), WPA2-Enterprise with EAP-Tunnelled Transport Layer Security (EAP-TTLS) or WPA2-Enterprise with Protected EAP (PEAP) to perform mutual authentication.

WPA2-Enterprise with EAP-TLS is considered one of the most secure EAP methods. With its inclusion in the initial release of the WPA2 standard, it enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. EAP-TLS uses a public key infrastructure (PKI) to secure communications between devices and a Remote Access Dial In User Service (RADIUS) server through the use of X.509 certificates. While EAP-TLS provides strong mutual authentication, it requires an agency to have established a PKI. This involves either deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses the wireless network. This can introduce additional costs and management overheads but the risk and security management advantages are significant.

The **EAP-TTLS/MSCHAPv2, or simply EAP-TTLS**, method used with WPA2-Enterprise is generally supported through the use of third party software. It has support in multiple operating systems including Microsoft Windows 7, 8, 10 and Server 2012 but does **not** have native support in earlier versions of Microsoft Windows. EAP-TTLS is different to EAP-TLS in that devices do not authenticate to the server when the initial TLS tunnel is created. Only the server authenticates to devices. Once the TLS tunnel has been created, mutual authentication occurs through the use of another EAP method.

An advantage of EAP-TTLS over PEAP is that a username is never transmitted in the clear outside of the TLS tunnel. Another advantage of EAP-TTLS is that it provides support for many legacy EAP methods, while PEAP is generally limited to the use of EAP-MSCHAPv2.

PEAPv0/EAP-MSCHAPv2, or simply PEAP, is the second most widely supported EAP method after EAP-TLS. It enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. PEAP operates in a very similar way to EAP-TTLS by creating a TLS tunnel which is used to protect another EAP method. PEAP differs from EAP-TTLS in that when the EAP-MSCHAPv2 method is used within the TLS tunnel, only the password portion is protected and not the username. This may allow an intruder to capture the username and replay it with a bogus password in order to lockout the user's account, causing a denial of service for that user. While EAP-MSCHAPv2 within PEAP is the most common implementation, Microsoft Windows supports the use of EAP-TLS within PEAP, known as PEAP-EAP-TLS. This approach is very similar in operation to traditional EAP-TLS yet provides increased protection, as parts of the certificate that are not encrypted with EAP-TLS are encrypted with PEAP-EAP-TLS. The downside to PEAP-EAP-TLS is its support is limited to Microsoft products.

18.2.9.R.03. Rationale

Ultimately, an agency's choice in authentication method will often be based on the size of their wireless deployment, their security requirements and any existing authentication infrastructure. If an agency is primarily motivated by security they can implement either PEAP-EAP-TLS or EAP-TLS. If they are primarily motivated by flexibility and legacy support they can implement EAP-TTLS. If they are primarily motivated by simplicity they can implement PEAP with EAP-MSCHAPv2.

18.2.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3319]

WPA2-Enterprise with EAP-TLS, WPA2-Enterprise with PEAP-EAP-TLS, WPA2-Enterprise with EAP-TTLS or WPA2-Enterprise with PEAP MUST be used on wireless networks to perform mutual authentication.

18.2.10. Evaluation of 802.1X authentication implementation

18.2.10.R.01. Rationale

The security of 802.1X authentication is dependent on three main elements and their interaction. These three elements include supplicants (clients) that support the 802.1X authentication protocol, authenticators (wireless access points) that facilitate communication between supplicants and the authentication server, and the authentication server (RADIUS server) that is used for authentication, authorisation and accounting purposes. To provide assurance that these elements have been implemented appropriately, supplicants, authenticators and the authentication server used in wireless networks must have completed an appropriate product evaluation.

18.2.10.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3326]

Supplicants, authenticators and the authentication server used in wireless networks MUST have completed an appropriate product evaluation.

18.2.10.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3329]

Supplicants, authenticators and the authentication server used in wireless networks SHOULD have completed an appropriate product evaluation.

18.2.11. Issuing certificates for authentication

18.2.11.R.01. Rationale

Certificates for authenticating to wireless networks can be issued to either or both devices and users. For assurance, certificates must be generated using a certificate authority product or hardware security module (HSM) that has completed an appropriate product evaluation.

18.2.11.R.02. Rationale

When issuing certificates to devices accessing wireless networks, agencies need to be aware of the risk that these certificates could be stolen by malicious software. Once compromised, the certificate could be used on another device to gain unauthorised access to the wireless network. Agencies also need to be aware that in only issuing a certificate to a device, any actions taken by a user will only be attributable to the device and not a specific user.

18.2.11.R.03. Rationale

When issuing certificates to users accessing wireless networks, they can either be in the form of a certificate that is stored on a device or a certificate that is stored within a smart card. Issuing certificates on smart cards provides increased security, but usually at a higher cost. Security is improved because a user is more likely to notice a missing smart card and alert their local security team, who is then able to revoke the credentials on the RADIUS server. This can minimise the time an intruder has access to a wireless network.

18.2.11.R.04. Rationale

In addition, to reduce the likelihood of a stolen smart card from being used to gain unauthorised access to a wireless network, two-factor authentication can be implemented through the use of Personal Identification Numbers (PINs) on smart cards. This is essential when a smart card grants a user any form of administrative access on a wireless network or attached network resource.

18.2.11.R.05. Rationale

For the highest level of security, unique certificates should be issued for both devices and users. In addition, the certificates for a device and user must not be stored on the same device. Finally, certificates for users accessing wireless networks should be issued on smart cards with access PINs and not stored with a device when not in use.

18.2.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3343]

Agencies MUST generate certificates using a certificate authority product or hardware security module that has completed an appropriate product evaluation.

18.2.11.C.02. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:3346]

The certificates for both a device and user accessing a wireless network MUST NOT be stored on the same device.

18.2.11.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3348]

Agencies SHOULD use unique certificates for both devices and users accessing a wireless network.

18.2.11.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3350]

Certificates for users accessing wireless networks SHOULD be issued on smart cards with access PINs and not stored with a device when not in use.

18.2.11.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3351]

Certificates stored on devices accessing wireless networks SHOULD be protected by implementing full disk encryption on the devices.

18.2.12. Using commercial certification authorities for certificate generation

18.2.12.R.01. Rationale

A security risk exists with EAP-TTLS and PEAP when a commercial certificate authority's certificates are automatically trusted by devices using vendor trusted certificate stores. This trust can be exploited by obtaining certificates from a commercial certificate authority under false

pretences, as devices can be tricked into trusting their signed certificate. This will allow the capture of authentication credentials presented by devices, which in the case of EAP-MSCHAPv2 can be cracked using a brute force attack granting not only network access but most likely Active Directory credentials as well.

To reduce this risk, devices can be configured to:

- validate the server certificate;
- disable any trust for certificates generated by commercial certificate authorities that are not trusted;
- disable the ability to prompt users to authorise net servers or commercial certificate authorities; and
- set devices to enable identity privacy to prevent usernames being sent prior to being authenticated by the RADIUS server.

18.2.12.C.01. Control**System Classification(s): All Classifications; Compliance: MUST** [CID:3354]

Devices MUST be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities.

18.2.12.C.02. Control**System Classification(s): All Classifications; Compliance: SHOULD** [CID:3355]

Devices SHOULD be set to enable identity privacy.

18.2.13. Caching 802.1X authentication outcomes

18.2.13.R.01. Rationale

When 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated. Upon successful authentication of a device, the PMK can be cached to assist with fast roaming between wireless access points. When a device roams away from a wireless access point that it has authenticated to, it will not need to perform a full re-authentication should it roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate a device to other neighbouring wireless access points that the device might roam to. Although requiring full authentication for a device each time it roams between wireless access points is ideal, agencies can chose to use PMK caching and pre-authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

18.2.13.C.01. Control**System Classification(s): All Classifications; Compliance: SHOULD NOT** [CID:3358]

The PMK caching period SHOULD NOT be set to greater than 1440 minutes (24 hours).

18.2.14. Remote Authentication Dial-In User Service (RADIUS) authentication

18.2.14.R.01. Rationale

The RADIUS authentication process that occurs between wireless access points and the RADIUS server is distinct and a separate to the 802.1X authentication process. During the initial configuration of wireless networks using 802.1X authentication, a shared secret is entered into either the wireless access points or the RADIUS server. If configured on the wireless access points, the shared secret is sent to the RADIUS server via the RADIUS protocol, and vice versa if configured on the RADIUS server. This shared secret is used for both RADIUS authentication and confidentiality of RADIUS traffic.

18.2.14.R.02. Rationale

An intruder that is able to gain access to the RADIUS traffic sent between wireless access points and the RADIUS server may be able to perform a brute force or an off-line dictionary attack to recover the shared secret. This in turn allows the intruder to decrypt all communications between wireless access points and the RADIUS server. To mitigate this security risk, communications between wireless access points and a RADIUS server must be encapsulated with an additional layer of encryption using an appropriate encryption product (See Chapter 17 – Cryptography).

18.2.14.C.01. Control**System Classification(s): All Classifications; Compliance: MUST** [CID:3362]

Communications between wireless access points and a RADIUS server MUST be encapsulated with an additional layer of encryption using an approved encryption product (See Chapter 17 – Cryptography).

18.2.15. Encryption

18.2.15.R.01. Rationale

As wireless transmissions are capable of radiating outside of secure areas into unsecure areas they need to be encrypted to the same level as classified information communicated over cabled infrastructure in unsecure areas.

18.2.15.C.01. Control**System Classification(s): All Classifications; Compliance: MUST** [CID:3365]

Agencies using wireless networks MUST ensure that classified information is protected by cryptography that meets the assurance level mandated for the communication of information over unclassified network infrastructure (See Section 17.2, Suite B).

18.2.16. Cipher Block Chaining Message Authentication Code Protocol (CCMP) Encryption

18.2.16.R.01. Rationale

As wireless transmissions are capable of radiating outside of secure areas, agencies cannot rely on the traditional approach of physical security to protect against unauthorised access to sensitive or classified information on wireless networks. Using the AES based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) helps protect the confidentiality and integrity of all wireless network traffic.

18.2.16.C.01. Control**System Classification(s): All Classifications; Compliance: MUST** [CID:3368]

CCMP MUST be used to protect the confidentiality and integrity of all wireless network traffic.

18.2.17. Temporal Key Integrity Protocol (TKIP) and Wireless Encryption Protocol (WEP)

18.2.17.R.01. Rationale

CCMP was introduced in WPA2 to address feasible attacks against the Temporal Integrity Key Protocol (TKIP) used by the Wi-Fi Protected Access (WPA) protocol as well as the original Wireless Encryption Protocol (WEP). A malicious actor seeking to exploit vulnerabilities in TKIP and WEP

can attempt to connect to wireless access points using one of these protocols. By default, wireless access points will attempt to accommodate this request by falling back to a legacy protocol that the device supports. Disabling or removing TKIP and WEP support from wireless access points ensures that wireless access points do not fall back to an insecure encryption protocol.

18.2.17.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3373]

TKIP and WEP support MUST be disabled or removed from wireless access points.

18.2.18. Wired Equivalent Privacy (WEP)

18.2.18.R.01.   Rationale

WEP has serious flaws which allow it to be trivially compromised. A WEP network should be considered equivalent to an unprotected network.

18.2.18.C.01.   Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:3379]

Agencies MUST NOT use WEP for wireless deployments.

18.2.19. Wi-Fi Protected Access (WPA)

18.2.19.R.01.   Rationale

WPA has been superseded by WPA2. Agencies are strongly encouraged to deploy WPA2 wireless networks instead of unsecure, WEP or WPA based wireless networks.

18.2.19.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3386]

Agencies SHOULD NOT use Wi-Fi Protected Access (WPA) for wireless deployments.

18.2.20. Pre-shared keys

18.2.20.R.01.   Rationale

The use of pre-shared keys is poor practice and not recommended for wireless authentication, in common with many authentication and encryption mechanisms, the greater the length of pre-shared keys the greater the security they provide.

18.2.20.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:3391]

Agencies MUST NOT use pre-shared keys for wireless authentication.

18.2.20.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3392]

If pre-shared keys are used, agencies SHOULD use random keys of the maximum allowable length.

18.2.20.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3393]

Agencies SHOULD NOT use pre-shared keys for wireless authentication.

18.2.21. Administrative interfaces for wireless access points

18.2.21.R.01.   Rationale

Administrative interfaces may allow users to modify the configuration and security settings of wireless access points. Often wireless access points by default allow users to access the administrative interface over methods such as fixed network connections, wireless network connections and serial connections directly on the device. Disabling the administrative interface on wireless access points will prevent unauthorised connections.

18.2.21.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3397]

Agencies SHOULD disable the administrative interface on wireless access points for wireless connections.

18.2.22. Protecting management frames on wireless networks

18.2.22.R.01.   Rationale

Effective DoS 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 DoS attacks.

18.2.22.R.02.   Rationale

The current release of the 802.11 standard provides no protection for management frames and therefore does not prevent spoofing or DoS attacks.

18.2.22.R.03.   Rationale

However, 802.11w was ratified in 2009 and specifically addresses the protection of management frames on wireless networks. Wireless access points and devices should be upgraded to support the 802.11w amendment or any later amendment or version that includes a capability for the protection of management frames.

18.2.22.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3408]

Wireless access points and devices SHOULD be upgraded to support a minimum of the 802.11w amendment.

18.2.23. Default service set identifiers (SSIDs)

18.2.23.R.01.   Rationale

All wireless access points are configured with a default Service Set Identifier (SSID). The SSID is commonly used to identify the name of a wireless network to users. As the default SSIDs of wireless access points are well documented on online forums, along with default accounts and passwords, it is important to change the default SSID and default passwords of wireless access points.

18.2.23.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3416]

Agencies MUST change the default SSID of wireless access points.

18.2.23.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:3418]

Agencies MUST rename or remove default accounts and passwords.

18.2.24. Changing the SSID

18.2.24.R.01. Rationale

When changing the default SSID, it is important that it lowers the profile of an agency's wireless network. In doing so, the SSID of a wireless network should not be readily associated with an agency, the location of or within their premises, or the functionality of the network.

18.2.24.R.02. Rationale

This procedure applies to all wireless network assets owned/or managed by the agency, including any guest or other publically accessible networks.

18.2.24.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3505]

The SSID of a wireless network SHOULD NOT be readily associated with an agency, the premises, location or the functionality of the network.

18.2.25. SSID Broadcasting

18.2.25.R.01. Rationale

A common method to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, the SSID is still broadcast in probe requests, probe responses, association requests and re-association requests for the network. Malicious actors can determine the SSID of wireless networks by capturing these requests and responses. By disabling SSID broadcasting agencies will make it more difficult for legitimate users to connect to wireless networks as legacy operating systems have only limited support for hidden SSIDs. Disabling SSID broadcasting infringes the design of the 802.11x standards.

18.2.25.R.02. Rationale

A further risk exists where an intruder can configure a wireless access point to broadcast the same SSID as the hidden SSID used by a legitimate wireless network. In this scenario devices will automatically connect to the wireless access point that is broadcasting the SSID they are configured to use before probing for a wireless access point that accepts the hidden SSID. Once the device is connected to the intruder's wireless access point the intruder can steal authentication credentials from the device to perform a man-in-the-middle attack to capture legitimate wireless network traffic or to later reuse to gain access to the legitimate wireless network.

18.2.25.R.03. Rationale

Disabling SSID broadcasting is not considered to be an effective control and may introduce additional risks.

18.2.25.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3514]

Agencies SHOULD NOT disable SSID broadcasting on wireless networks.

18.2.26. Static addressing

18.2.26.R.01. Rationale

Rogue devices or Access Points (APs) are unauthorised Wireless Access Points operating outside of the control of an agency. Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a network from being assigned a routable IP address. However, some malicious actors will be able to determine IP addresses of legitimate users and use this information to guess or spoof valid IP address ranges for wireless networks. Configuring devices to use static IP addresses introduces a management overhead without any tangible security benefit.

18.2.26.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3520]

Agencies SHOULD use the Dynamic Host Configuration Protocol (DHCP) for assigning IP addresses on wireless networks.

18.2.27. Media Access Control address filtering

18.2.27.R.01. Rationale

Devices that connect to wireless networks have a unique Media Access Control (MAC) address. It is possible to use MAC address filtering on wireless access points to restrict which devices can connect to wireless networks. While this approach will introduce a management overhead of configuring whitelists of approved MAC addresses, it can prevent rogue devices from connecting to wireless networks. However, some malicious actors will be able to determine valid MAC addresses of legitimate users already on wireless networks and use this information to spoof valid MAC addresses and gain access to a network. MAC address filtering introduces a management overhead without any real tangible security benefit.

18.2.27.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3529]

MAC address filtering SHOULD NOT be used as a security mechanism to restrict which devices connect to a wireless network.

18.2.28. Documentation

18.2.28.R.01. Rationale

Wireless device driver and WAP vulnerabilities are very exposed to the threat environment and require specific attention as exploits can gain immediate unauthorised access to the network.

18.2.28.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3533]

Key generation, distribution and rekeying procedures SHOULD be documented in the SecPlan for the wireless network.

18.2.28.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:3534]

Wireless device drivers and their versions SHOULD be documented in the SecPlan for the wireless network.

18.2.29. Non-agency devices connecting to agency controlled wireless networks

18.2.29.R.01. Rationale

As agencies have no control over the security of non-agency devices or knowledge of the security posture of such devices, allowing them to connect to agency controlled wireless networks poses a serious threat. Of particular concern is that non-agency devices may be infected with viruses, malware or other malicious code that could crossover onto the agency network. Furthermore, any non-agency devices connecting to agency controlled wireless networks will take on the classification of the network and will need to be appropriately sanitised and declassified before being released back to their owners.

18.2.29.R.02. Rationale

The practice of Bring Your Own Device (BYOD) is becoming more widespread but introduces a significant number of additional risks to agency systems. Refer to Section 21.4 for guidance on the use of BYOD.

18.2.29.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3583]

Where BYOD has been approved by an agency, any wireless network allowing BYOD connections MUST be segregated from all other agency networks, including any agency wireless networks.

18.2.29.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3586]

Any BYOD devices MUST comply with the policies and configuration described in Section 21.4– BYOD.

18.2.29.C.03. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:3588]

Agencies MUST NOT allow non-agency devices to connect to agency controlled wireless networks not intended or configured for BYOD devices or for public access.

18.2.30. Agency devices connecting to non-agency controlled wireless networks

18.2.30.R.01. Rationale

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.

18.2.30.R.02. Rationale

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.

18.2.30.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3600]

Agencies SHOULD NOT allow agency devices to connect to non-agency controlled wireless networks.

18.2.31. Connecting wireless networks to fixed networks

18.2.31.R.01. Rationale

When an agency has a business requirement to connect a wireless network to a fixed network, it is important that they consider the security risks. While fixed networks can be designed with a certain degree of physical security, wireless networks are often easily accessible outside of the agency's controlled area. Treating connections between wireless networks and fixed networks in the same way agencies would treat connections between fixed networks and the Internet can help protect against an intrusion originating from a wireless network against a fixed network. For example, agencies can implement a gateway to inspect and control the flow of information between the two networks.

18.2.31.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3609]

Connections between wireless networks and fixed networks SHOULD be treated in the same way as connections between fixed networks and the Internet.

18.2.32. Wireless network footprint and Radio Frequency (RF) Controls

18.2.32.R.01. Rationale

Minimising the output power of wireless access points will reduce the footprint of wireless networks. Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power should be deployed to achieve the desired wireless network footprint. This has the added benefit of providing redundancy for a wireless network should a wireless access point become unserviceable. In such a case, the output power of other wireless access points can be temporarily increased to cover the footprint gap until the unserviceable wireless access point can be replaced.

18.2.32.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3614]

Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power SHOULD be deployed to achieve the desired wireless network footprint.

18.2.33. Radio Frequency (RF) Propagation & Controls

18.2.33.R.01. Rationale

An additional method to limit a wireless network's footprint is through the use of radio frequency (RF) shielding on an agency's premises. While expensive, this will limit the wireless communications to areas under the control of an agency. RF shielding on an agency's premises has the added benefit of preventing the jamming of wireless networks from outside of the premises in which wireless networks are operating.

18.2.33.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3617]

The effective range of wireless communications outside an agency's area of control SHOULD be limited by:

- Minimising the output power level of wireless devices.
- Implementing RF shielding within buildings in which wireless networks are used.

18.2.34. Interference between wireless networks

18.2.34.R.01. Rationale

Where multiple wireless networks are deployed in close proximity, there is the potential for RF interference to adversely impact the availability of the network, especially when networks are operating on commonly used default channels of 1 and 11. This interference is also apparent where a large number of wireless networks are is use in close proximity to the agency's premises.

18.2.34.R.02. Rationale

Sufficiently separating wireless networks through the use of channel separation can help reduce this risk. This can be achieved by using wireless networks that are configured to operate with at least one channel separation. For example, channels 1, 3 and 5 could be used to separate three wireless networks.

18.2.34.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3621]

Wireless networks SHOULD use channel separation.

18.3. Video & Telephony Conferencing and Internet Protocol Telephony

Objective

18.3.1. Video & Telephony Conferencing (VTC), Internet Protocol Telephony (IPT) and Voice over Internet Protocol (VoIP) systems are implemented in a secure manner that does not compromise security, information or systems and that they operate securely.

Context

Scope

18.3.2. This section covers information on VTC and IPT including Voice over Internet Protocol (VoIP). Although IPT refers generally to the transport of telephone calls over IP networks, the scope of this section includes connectivity to the PSTN as well as remote sites.

18.3.3. Additional information relating to topics covered in this section can be found in

- Chapter 12 – Product Security;
- Chapter 11 – Communications Systems and Devices;
- Chapter 19 – Gateways Security; and
- any section in this manual relating to the protection of data networks.

Exception for VTC and IPT gateways

18.3.4. Where a gateway connects between an analogue telephone network such as the PSTN and a computer network, Chapter 19 – Gateway Security **does not** apply.

18.3.5. Where a gateway connects between a VTC or IPT network and any other VTC or IPT network, Chapter 19 – Gateway Security applies.

Hardening VTC and IPT systems

18.3.6. Data in a VTC or IPT network consists of IP packets and should not be treated any differently to other data. In accordance with the principles of least-privilege and security-in-depth, hardening can be applied to all handsets, control units, software, servers and gateways. For example a Session Initiation Protocol (SIP) server could:

- have a fully patched software and operating system;
- only required services running;
- use encrypted non-replayable authentication; and
- apply network restrictions that only allow secure Session Initiation Protocol (SIP) and secure Real Time Transport (RTP) traffic from IP phones on a VLAN to reach the server.

References

18.3.7.

Reference	Title	Publisher	Source
SP 800-58	Security Considerations for Voice Over IP Systems	NIST	http://csrc.nist.gov/publications/nistpubs/
	Security Issues and Countermeasure for VoIP	SANS	http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701
Report Number: I332-016R-2005	Security Guidance for Deploying IP Telephony Systems Released: 14 February 2006	Systems and Network Attack Center (SNAC) NSA	https://www.nsa.gov/ia/_files/voip/i332-016r-2005.pdf
Report Number: I332-009R-2006	Recommended IP Telephony Architecture, Updated: 1 May 2006 Version 1.0	Systems and Network Attack Center (SNAC) NSA	https://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf
	Mobility Capability Package March 26 2012 - Secure VoIP Version 1.2	NSA	https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_1_2.pdf

	Protecting Telephone-based Payment Card Data PCI Data Security Standard (PCI DSS) Version: 2.0, March 2011	The PCI Security Standards Council (PCI SSC)	https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf
	PCI Mobile Payment Acceptance Security Guidelines Version: 1.0 Date: September 2012	PCI SSC	https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf
	PCI Mobile Payment Acceptance Security Guidelines Version: 1.0 Date: February 2013	PCI SSC	https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf
	Understanding Voice over Internet Protocol (VoIP): 2006	US-CERT	https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf
CNSS Instruction No. 5000 April 2007	Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony	Committee on National Security Systems	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
	DHS 4300A Sensitive Systems Handbook Attachment Q5 To Handbook v. 11.0 Voice over Internet Protocol (VoIP) Version 11.0 December 22, 2014	DHS	http://www.dhs.gov/sites/default/files/publications/4300A%20Handbook%20Attachment%20Q5%20-%20Voice%20over%20IP.pdf

Rationale & Controls

18.3.8. Video and voice-aware firewalls

18.3.8.R.01.   Rationale

The use of video, unified communications and voice-aware firewalls ensures that only video or voice traffic (e.g. signalling and data) is allowed for a given call and that the session state is maintained throughout the transaction.

18.3.8.R.02.   Rationale

The requirement to use a video, unified communication or voice-aware firewall does not necessarily require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. If possible, agencies are encouraged to implement one firewall that is either video and data-aware; voice and data-aware; or video, voice and data-aware depending on their needs.

18.3.8.R.03.   Rationale

Refer to Section 19.5 - Session Border Controllers.

18.3.8.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3721]

Agencies SHOULD use a video, unified communication or voice-aware firewall that meets the same minimum level of assurance as specified for normal firewalls.

18.3.9. Protecting IPT signalling and data

18.3.9.R.01.   Rationale

IPT voice and signalling data is vulnerable to eavesdropping but can be protected with encryption. This control helps protect against DoS, man-in-the-middle and call spoofing attacks made possible by inherent weaknesses in the VTC and IPT protocols.

18.3.9.R.02.   Rationale

When protecting IPT 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.

18.3.9.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3728]

Agencies SHOULD protect VTC and IPT signalling and data by using encryption.

18.3.9.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3729]

An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.

18.3.10. Establishment of secure signalling and data protocols

18.3.10.R.01.   Rationale

Use of secure signalling and data protects against eavesdropping, some types of DoS, man-in-the-middle and call spoofing attacks.

18.3.10.C.01.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3732]

Agencies SHOULD ensure that VTC and IPT functions are established using only the secure signalling and data protocols.

18.3.11. Local area network traffic separation

18.3.11.R.01.   Rationale

Availability and quality of service are the main drivers for applying the principles of separation and segregation.

18.3.11.C.01. Control

        Agencies MUST either separate or segregate the VTC and IPT traffic from other data traffic.

18.3.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3736]

        Agencies SHOULD either separate or segregate the IPT traffic from other data traffic.

18.3.12. VTC and IPT Device setup

18.3.12.R.01. Rationale

        VTC equipment and VoIP phones need to be hardened and separated or segregated from the data network to ensure they will not provide an easy entry point to the network for an attacker.

18.3.12.R.02. Rationale

        USB ports on these devices can be used to circumvent USB workstation policy and upload malicious software for unauthorised call recording/spoofing and entry into the data network. Unauthorised or unauthenticated devices should be blocked by default to reduce the risk of a compromise or denial of service.

18.3.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3740]

        Agencies MUST:

- configure VTC and VoIP devices 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; and
- use individual logins for IP phones.

18.3.12.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3741]

        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; and
- use individual logins for IP phones.

18.3.13. Call authentication and authorisation

18.3.13.R.01. Rationale

        This control ensures server-client mutual authentication.

18.3.13.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3745]

        Authentication and authorisation SHOULD be used for all actions on the IPT network, including:

- call setup;
- changing settings; and
- checking voice mail.

18.3.13.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3747]

        An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.

18.3.13.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3748]

        Authentication SHOULD be enforced for:

- registering a new phone;
- changing phone users;
- changing settings; and
- accessing voice mail.

18.3.14. VTC and IPT device connection to workstations

18.3.14.R.01. Rationale

        Availability and quality of service are the main drivers for applying the principles of separation and segregation.

18.3.14.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:3751]

        Agencies MUST NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.

18.3.14.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:3752]

        Agencies SHOULD NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.

18.3.15. Lobby and shared area IPT devices

18.3.15.R.01. Rationale

IPT devices in public areas may give an attacker opportunity to access the internal data network 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.

18.3.15.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3756]

Where an agency uses a VoIP phone in a lobby or shared area they SHOULD limit or disable the phone's:

- ability to access data networks;
- functionality for voice mail and directory services; and
- use a separate network segment.

18.3.15.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3758]

Agencies SHOULD, where available, use traditional analogue phones in a lobby and shared areas.

18.3.16. Usage of softphones, webcams and similar sound and video devices

18.3.16.R.01. Rationale

Software and applications for softphones and webcams can introduce additional attack vectors 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 network.

18.3.16.R.02. Rationale

Softphones and webcams typically require workstation to workstation communication, normally using 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.

18.3.16.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3766]

Agencies using softphones or webcams SHOULD have separate dedicated network interface cards on the host for VTC or IPT network access to facilitate VLAN separation.

18.3.16.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3768]

Agencies using softphones or webcams SHOULD install a host-based firewall on workstations utilising softphones or webcams that allows traffic only to and from a minimum number of ports.

18.3.16.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD NOT [CID:3770]

Agencies SHOULD NOT use softphones or webcams.

18.3.17. Workstations using USB softphones, webcams and similar sound and video devices

18.3.17.R.01. Rationale

Adding softphones and webcams 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.

18.3.17.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3777]

Agencies SHOULD use access control software to control USB ports on workstations using softphones and webcams by utilising the specific vendor and product identifier of the authorised device.

18.3.18. Developing a denial of service response plan

18.3.18.R.01. Rationale

Communications are considered critical for any business and are therefore especially vulnerable to Denial of Service (DoS). The guidance provided will assist in protecting against VTC or IPT DoS attacks, signalling floods, established call teardown and RTP data floods. These elements should be included in the agency's wider response plan (See Section 6.4 – Business Continuity and Disaster Recovery).

18.3.18.R.02. Rationale

Simple DoS attacks and incidents are often the result of bandwidth exhaustion. Agencies should also consider other forms of DoS including Distributed Denial of Service attacks (DdoS), DNS and latency incidents.

18.3.18.R.03. Rationale

System resilience can be improved by architecting a structured approach and providing layered defence such as network and application protection as separate layers.

18.3.18.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3782]

Agencies SHOULD develop a Denial of Service response plan including:

- how to identify the precursors and other signs of DoS;
- how to diagnose the incident or attack type and attack method;
- how to diagnose the source of the DoS;
- what actions can be taken to clear the DoS;
- how communications can be maintained during a DoS; and
- report the incident.

18.3.19. Content of a Denial of Service (DoS) response plan

18.3.19.R.01. Rationale

An VTC or IPT DoS response plan will need to address the following:

- how to identify the source of the DoS, either internal or external (location and content of logs);
- how to diagnose the incident or attack type and attack method;
- how to minimise the effect on VTC or IPT, of a DoS of the data network (e.g. Internet or internal DoS), including separate links to other office locations for VTC and IPT and/or quality of service prioritisation;
- strategies that can mitigate the DOS (banning certain devices/Ips at the call controller and firewalls, implementing quality of service, changing VoIP authentication, changing dial-in authentication; and
- alternative communication options (such as designated devices or personal mobile phones) that have been identified for use in case of an emergency.

18.3.19.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3785]

A Denial of Service response plan SHOULD include monitoring and use of:

- router and switch logging and flow data;
- packet captures;
- proxy and call manager logs and access control lists;
- VTC and IPT aware firewalls and voice gateways;
- network redundancy;
- load balancing;
- PSTN failover; and
- alternative communication paths.

18.4. Intrusion Detection and Prevention

Objective

18.4.1. An intrusion detection and prevention strategy is implemented for systems in order to respond promptly to incidents and preserve availability, confidentiality and integrity of systems.

Context

Scope

18.4.2. This section covers information relating to detection and prevention of malicious code propagating through networks as well as the detection and prevention of unusual or malicious activities.

Methods of infections or delivery

18.4.3. 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; or
- deliberate introduction of malicious code.

18.4.4. The speed at which malicious code can spread through a system presents significant challenges and an important part of any defensive strategy is to contain the attack and limit damage.

References

18.4.5.

Title	Publisher	Source
ISO/IEC 27001:2006, A.15.3, Information Systems Audit Considerations	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
HB 171:2003 Guidelines for the Management of Information Technology Evidence	Standards NZ	https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF

References - Endpoint Security

18.4.6.

Title	Publisher	Source
Transport Layer Protection Cheat Sheet	OWASP	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2	IETF	https://tools.ietf.org/html/rfc5246

RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3	IETF	https://tools.ietf.org/html/rfc8446
RFC 7525 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)	IETF	https://tools.ietf.org/html/rfc7525
RFC 6749 - The OAuth 2.0 Framework Authorization	IETF	https://tools.ietf.org/html/rfc6749
OpenID Connect	OpenID Foundation	http://openid.net/connect/
New Zealand Security Assertion Messaging Standard Web Page	NZ Government Department of internal affairs	https://www.ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/new-zealand-security-assertion-messaging-standard/
New Zealand Security Assertion Messaging Standard	NZ Government Department of internal affairs	https://www.ict.govt.nz/assets/Uploads/Documents/egif-authentication-NZSAMS-v1.0.pdf

Rationale & Controls

18.4.7. Intrusion Detection and Prevention strategy (IDS/IPS)

18.4.7.R.01. Rationale

An IDS/IPS when configured correctly, kept up to date and supported by appropriate processes, can be an effective way of identifying, responding to and containing known attack types, specific attack profiles or anomalous or suspicious network activities.

18.4.7.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3802]

Agencies MUST develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary;
- the audit analysis of event logs, including IDS/IPS logs;
- a periodic audit of intrusion detection procedures;
- information security awareness and training programs;
- a documented Incident Response Plans (IRP); and
- provide the capability to detect information security incidents and attempted network intrusions on gateways and provide real-time alerts.

18.4.7.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3803]

Agencies SHOULD develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary;
- the audit analysis of event logs, including IDS/IPS logs;
- a periodic audit of intrusion detection procedures;
- information security awareness and training programs; and
- a documented IRP.

18.4.7.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3804]

Agencies SHOULD ensure sufficient resources are provided for the maintenance and monitoring of IDS/IPS.

18.4.8. IDS/IPSs on gateways

18.4.8.R.01. Rationale

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

18.4.8.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3807]

Agencies SHOULD deploy IDS/IPSs in all gateways between the agency's networks and unsecure public networks or BYOD wireless networks.

18.4.8.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3808]

Agencies SHOULD deploy IDS/IPSs at all gateways between the agency's networks and any network not managed by the agency.

18.4.8.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3809]

Agencies SHOULD locate IDS/IPSs within the gateway environment, immediately inside the outermost firewall.

18.4.9. IDS/IPS Maintenance

18.4.9.R.01. Rationale

When signature-based intrusion detection is used, the effectiveness of the IDS/IPS will degrade over time as new intrusion methods are developed. It is for this reason that IDS/IPS systems and signatures need to be up to date to identify the latest intrusion detection methods.

18.4.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3815]

Agencies MUST select IDS / IPS that monitor uncharacteristic and suspicious activities.

18.4.9.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3843]

When signature-based intrusion detection is used, agencies MUST keep the signatures and system patching up to date.

18.4.10. Malicious code counter-measures

18.4.10.R.01. Rationale

Implementing policies and procedures for preventing and dealing with malicious code outbreaks that enables agencies to provide consistent incident response, as well as giving clear directions to system users on how to respond to an information security incident.

18.4.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3851]

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 an agency network;
    - detect any malicious code installed on a system;

- make their system users aware of the agency's policies and procedures; and
- ensure that all instances of detected malicious code outbreaks are handled according to established procedures.

18.4.11. Configuring the IDS/IPS

18.4.11.R.01. Rationale

Generating alerts for any information flows that contravene any rule within the firewall rule set will assist security personnel in identifying and reporting to any possible breaches of agency systems.

18.4.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3857]

In addition to agency defined configuration requirements, agencies SHOULD ensure that IDS/IPSs located inside a firewall are configured to generate a log entry, and an alert, for any information flows that contravene any rule within the firewall rule set.

18.4.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3859]

Agencies SHOULD test IDS/IPSs rule sets prior to implementation to ensure that they perform as expected.

18.4.11.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3864]

If a firewall is configured to block all traffic on a particular range of port numbers, the IDP/IPSs SHOULD inspect traffic for these port numbers and generate an alert if they are detected.

18.4.12. Event management and correlation

18.4.12.R.01. Rationale

Deploying tools to manage correlation of suspicious events or events of interest across all agency networks will assist in identifying suspicious patterns in information flows throughout the agency.

18.4.12.R.02. Rationale

The history of events is important in this analysis and should be accommodated in any archiving decisions.

18.4.12.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3875]

Agencies SHOULD deploy tools for:

- the management and archive of security event information; and
- the correlation of suspicious events or events of interest across all agency networks.

18.4.13. Host-based IDS/IPSs

18.4.13.R.01. Rationale

Host-based IDS/IPS use behaviour-based detection schemes and can therefore assist in the detection of previously unidentified anomalous and suspicious activities such as:

- process injection;
- keystroke logging;
- driver loading;
- library additions or supercessions;
- call hooking.

They may also identify new malicious code. It should be noted that some anti-virus and similar security products are evolving into converged endpoint security products that incorporate HIDS/HIPS.

18.4.13.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3886]

Agencies SHOULD install host-based IDS/IPSs on authentication, DNS, email, Web and other high value servers.

18.4.14. Active content blocking

18.4.14.R.01. Rationale

Filtering unnecessary content and disabling unwanted functionality reduces the number of possible entry points that an attacker can exploit.

18.4.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3892]

Agencies SHOULD use:

- filters to block unwanted content and exploits against applications that cannot be patched;
- settings within the applications to disable unwanted functionality; and
- digital signatures to restrict active content to trusted sources only.

18.5. Internet Protocol Version 6

Objective

18.5.1. IPv6 is disabled until it is ready to be deployed.

Context

Scope

18.5.2. This section covers information on IPv6 and its deployment within networks. Where this manual specifies requirements for network devices, the requirements apply equally whether deploying IPv6 or IPv4.

18.5.3. IPv6 was officially launched by the Internet Society in June 2012. With the change from IPv4 to IPv6, there is the potential to introduce vulnerabilities to agency networks through incorrect or mis-configuration, poor design and poor device compatibility. Attackers will also be actively seeking to exploit vulnerabilities that will inevitably be exposed.

18.5.4. Agencies unable to meet the compliance requirements as specified for a control when deploying IPv6 network infrastructure will need to follow the procedures as specified in this manual for varying from a control and the associated compliance requirements.

DNS Security Extensions (DNSSEC)

18.5.5. DNSSEC has been developed to enhance Internet security and can digitally 'sign' data to assure validity. It is essential that DNSSEC is deployed at each step in the lookup from root zone to final domain name (e.g., www.icann.org). Signing the root (deploying DNSSEC on the root zone) is a necessary step in this overall process. Importantly it does not encrypt data. It just attests to the validity of the address of the site you visit. DNSSEC and IPv6 have been engineered to integrate and thus enhance Internet security.

References

18.5.6.

Title	Publisher	Source
A strategy for the transition to IPv6 for Australian Government agencies. (archived document)	Australian Government Information Management Office	https://www.finance.gov.au/files/2011/10/Australian-Government-Transition-to-IPv6-2011.doc
Manageable Network Plan	NSA	https://www.nsa.gov/what-we-do/information-assurance/
Router Security Configuration Guide Supplement – Security for IPv6 Routers, 23 May 2006 Version: 1.0	NSA	http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf
Firewall Design Considerations for IPv6, 10/3/2007	NSA	http://www.hpc.mil/images/hpcdocs/ipv6/nsa-firewall-design-ipv6-i733-041r-2007.pdf
Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41, Revision 1, September 2009	NIST	http://csrc.nist.gov/publications/PubsSPs.html
Guidelines for secure deployment of IPv6, Special Publication 800-119, December 2010	NIST	http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
A Complete Guide on IPv6 Attack and Defense	SANS Institute	http://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904?show=complete-guide-ipv6-attack-defense-33904&cat=detection
Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998	IETF	http://www.ietf.org/rfc/rfc2460.txt
IP Version 6 Addressing Architecture, RFC 4291, February 2006	IETF	http://tools.ietf.org/html/rfc4291
A Recommendation for IPv6 Address Text Representation, ISSN: 2070-1721, RFC 5952, August 2010	IETF	http://tools.ietf.org/html/rfc5952
Ipv6 Addressing of IPv4/IPv6 Translators, ISSN: 2070-1721, RFC 6052, October 2010	IETF	http://tools.ietf.org/html/rfc6052
Significance of IPv6 Interface Identifiers, RFC 7136, ISSN: 2070-1721, February 2014	IETF	http://tools.ietf.org/html/rfc7136
DNSSEC Operational Practices, Version 2	IETF	http://tools.ietf.org/search/rfc6781

Clarifications and Implementation Notes for DNS Security (DNSSEC)	IETF	http://tools.ietf.org/search/rfc6840
A Framework for DNSSEC Policies and DNSSEC Practice Statements	IETF	http://tools.ietf.org/html/rfc6841
IETF RFC 7123 Security Implications of IPv6 on IPv4 Networks	IETF	http://tools.ietf.org/html/rfc7123
IETF RFC 4861 Neighbor Discovery for IP version 6 (IPv6)	IETF	http://tools.ietf.org/html/rfc4861
IETF RFC 5942 IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes	IETF	http://tools.ietf.org/html/rfc5942
IETF RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	IETF	http://www.ietf.org/rfc/rfc3315.txt
IETF RFC 6104 Rogue IPv6 Router Advertisement Problem Statement	IETF	http://tools.ietf.org/html/rfc6104
IPv6 First-Hop Security Concerns	Cisco	http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html
DNSSEC – What Is It and Why Is It Important?	Internet Corporation for Assigned Names and Numbers (ICAAN)	http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm

Rationale & Controls

18.5.7.   Use of dual-stack equipment

18.5.7.R.01.   Rationale

In order to reduce the attack surface area of agency systems, it is good practice that agencies disable unused services and functions within network devices and operating systems. If agencies are deploying dual-stack equipment but not using the IPv6 functionality, then that functionality should be disabled. It can be re-enabled when required. This will reduce the opportunity to exploit IPv6 functionality before appropriate security measures have been implemented.

18.5.7.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3951]

Agencies not using IPv6, but which have deployed dual-stack network devices and ICT equipment that supports IPv6, MUST disable the IPv6 functionality, unless that functionality is required.

18.5.7.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3952]

Network security devices on IPv6 or dual-stack networks MUST be IPv6 capable.

18.5.8.   Using IPv6

18.5.8.R.01.   Rationale

The information security implications around the use of IPv6 are still largely unknown and un-tested. As many of the deployed network protection technologies, such as firewalls and IDSs, do not consistently support IPv6, agencies choosing to implement IPv6 face an increased risk of systems compromise.

18.5.8.R.02.   Rationale

A number of tunnelling protocols have been developed to facilitate interoperability between IPv4 and IPv6. Disabling IPv6 tunnelling protocols when this functionality is not explicitly required will reduce the risk of bypassing network defences by means of encapsulating IPv6 data inside IPv4 packets.

18.5.8.R.03.   Rationale

Stateless Address Autoconfiguration (SLAAC) is a method of stateless IP address configuration in IPv6. SLAAC reduces the ability to maintain complete logs of IP address assignment on the network. To avoid this constraint, stateless IP addressing SHOULD NOT be used.

18.5.8.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3960]

Agencies using IPv6 MUST conduct a security risk assessment on risks that could be introduced as a result of running a dual stack environment or transitioning completely to IPv6.

18.5.8.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3961]

Agencies implementing a dual stack or wholly IPv6 network or environment MUST re-accredit their networks.

18.5.8.C.03.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3962]

IPv6 tunnelling MUST be disabled on all network devices, unless explicitly required.

18.5.8.C.04.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3965]

Dynamically assigned IPv6 addresses SHOULD be configured with DHCPv6 in a stateful manner and with lease information logged and logs stored in a centralised logging facility.

18.5.9.   New systems and networks

18.5.9.R.01. Rationale

Planning and accommodating changes in technology are an essential part of securing architectures and systems development.

18.5.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3971]

Any network defence elements and devices MUST be IPv6 aware.

18.5.9.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3972]

New network devices, including firewalls, IDS and IPS, MUST be IPv6 capable.

18.5.9.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3974]

Agencies SHOULD consider the use of DNSSEC.

18.5.10. Introducing IPv6 capable equipment to gateways

18.5.10.R.01. Rationale

Introducing IPv6 capable network devices into agency gateways can introduce a significant number of new security risks. Undergoing reaccreditation when new IPv6 equipment is introduced will ensure that any IPv6 functionality that is not intended to be used cannot be exploited by an attacker before appropriate information security mechanisms have been put in place.

18.5.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4012]

IPv6 tunnelling MUST be blocked by network security devices at externally connected network boundaries.

18.5.10.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4014]

Agencies deploying IPv6 equipment in their gateway but not enabling the functionality SHOULD undergo reaccreditation.

18.5.11. Enabling IPv6 in gateways

18.5.11.R.01. Rationale

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 information security mechanisms for IPv6 are working effectively.

18.5.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4018]

Agencies enabling a dual-stack environment or a wholly IPv6 environment in their gateways MUST reaccredit their gateway systems.

18.6. Peripheral (KVM) Switches

Objective

18.6.1. An evaluated peripheral switch is used when sharing keyboards, monitors and mice or other user interface devices, between different systems.

Context

Scope

18.6.2. This section covers information relating specifically to the use of keyboard/video/mouse (KVM) switches.

18.6.3. It is important to recognise that any cross-connection of system must be carefully controlled in order not to compromise trust zones. The principles of separation and segregation must be applied. These principles are discussed in Section 22.1 – Cloud Computing and Section 22.2 – Virtualisation.

18.6.4. Cross-connection of system may also functionally create a gateway, whether or not it meets the technical definition of gateways. It is important to refer to Section 19.1 – Gateways and Section 19.2 – Cross Domain Solutions.

Peripheral switches with more than two connections

18.6.5. If the peripheral switch has more than two systems connected then the level of assurance needed is determined by the highest and lowest of the classifications involved.

Electrical Safety

18.6.6. Electrical safety is paramount. Cross-connecting systems may create ground loops if different power sources are used for different elements of the computer system. This may result in catastrophic failure if power supplies connected to different phases are cross-connected.

Product Assurance

18.6.7. Product assurance is discussed in Chapter 12- Product Security It is important to note the role of the Common Criteria, the related CCRA and the use of assurance levels in determining product assurance. chapter 12 also provides essential reference to assurance levels, evaluation levels and defines high assurance as shown in the table 18.6.8 Assurance requirements.

Rationale & Controls

18.6.8. Assurance requirements

18.6.8.R.01. Rationale

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.

18.6.8.R.02. Rationale

It is important to maintain the integrity of Trust Zones and adhere to the principles of separation and segregation in order to avoid inadvertently compromising Trust Zones – even if they are at the same level of classification.

18.6.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4051]

Agencies accessing a classified system and a less classified system via a peripheral switch MUST use an evaluated product with a level of assurance as indicated in the table below.

High System	Low system / Alternate Trust Domain	Required Level of Assurance
RESTRICTED	UNCLASSIFIED	EAL2 or PP
CONFIDENTIAL	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
TOP SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
	TOP SECRET	high assurance

18.6.9. Assurance requirements for NZEO systems

18.6.9.R.01. Rationale

NZEO systems are particularly sensitive. Additional security measures need to be put in place when connecting them to other systems.

18.6.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4058]

Agencies accessing a system containing NZEO information and a system of the same classification that is not accredited to process NZEO information, MUST use an evaluated product with an EAL2 (or higher) or a PP level of assurance.

18.6.10. Cross-Connecting Systems with a device other than a KVM

18.6.10.R.01. Rationale

Cross-connecting systems with any device other than a KVM approved gateway or an approved cross-domain solution may be high risk, may compromise the integrity of Trust Zones, and may create an electrical hazard.

18.6.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4066]

Cross-connection of security domains and Trust Zones MUST be enabled through an approved KVM, Gateway or Cross-Domain solution only.

High system	Low system/ Alternate Trust Domain	Level of assurance
RESTRICTED & all lower classifications	UNCLASSIFIED	EAL2 or PP
CONFIDENTIAL	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
TOP SECRET	UNCLASSIFIED	high assurance
	RESTRICTED	high assurance
	CONFIDENTIAL	high assurance
	SECRET	high assurance
	TOP SECRET	high assurance

19. Gateway security

19.1. Gateways

Objective

19.1.1. To ensure that gateways are properly configured to protect agency systems and information transferred between systems from different security domains.

Context

Scope

19.1.2. Gateways can be considered to be information flow control mechanisms operating at the Network layer and may also control information flow at the Transport, Session, Presentation and Application layers of the Open Systems Interconnection model (OSI). Specific controls for different technologies can be found in Section 19.3 –Firewalls, Section 19.4 – Diodes, Section 18.6 – Peripheral (KVM) switches and Section 19.5 – Session Border Controllers.

19.1.3. Additional information relating to topics covered in this section can be found in the following sections of this manual:

- Section 4.4 – Accreditation Framework;
- Section 8.2 – Servers and Network Devices;
- Section 8.3 – Network Infrastructure;
- Section 8.4 – IT Equipment;
- Chapter 12 – Product Security;
- Section 16.1 – Identification and Authentication;
- Section 16.5 – Event Logging and Auditing;
- Section 19.3 – Firewalls;
- Section 19.4 – Diodes;
- Section 19.5 – Session Border Controllers;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 20.3 – Content Filtering.

Deploying Gateways

19.1.4. This section provides a baseline for agencies deploying gateways. Agencies will need to consult additional sections of this manual depending on the specific type of gateways deployed.

19.1.5. For network devices used to control data flow in bi-directional gateways, Section 19.3 – Firewalls will need to be consulted. Section 19.4 – Diodes will also need to be consulted for one-way gateways. Additionally, for both types of gateways, Section 20.1 - Data Transfers and Section 19.2 - Cross-Domain Solutions, will need to be consulted for requirements on appropriately controlling data flows.

19.1.6. The requirements in this manual for content filtering, data import and data export apply to all types of gateways.

Gateway classification

19.1.7. For the purposes of this chapter, the gateway assumes the highest classification of the connected domains.

References

19.1.8. Further references can be found at:

Title	Publisher	Source
ISO/IEC 27033-4:2014 **Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways**	ISO	Revising ISO/IEC 18028-3:2005 http://www.iso.org
Gateway / Cross Domain Solution Audit Guide, Australian Government	ASD	http://www.asd.gov.au/publications/Gateway_CDS_Audit_Guide.docx
Guidelines on Firewalls and Firewall Policy, NIST SP800-41,	NIST	http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
Good Practices for deploying DNSSEC, ENISA	ENISA	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec
The OSI model **ISO/IEC 7498-1:1994** **Information Technology – Open Systems Interconnection: The Basic Model**	ISO / IEC	http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

PSR references

19.1.9. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/
PSR content protocols	Management protocol for information security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Supply chain security Understand the information security lifecycle	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/governance/supply-chain-security/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/
Managing specific scenarios	Outsourced ICT facilities Outsourcing, Offshoring and supply chains Communication security Physical security for ICT systems Transacting online with the public	https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/outsourced-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/communications-security/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/transacting-online-with-the-public/

Rationale & Controls

19.1.10. Gateways involving cascaded connections

19.1.10.R.01. Rationale

Protecting a cascaded connection path with the minimum assurance requirement of a direct connection between the highest and lowest networks ensures appropriate reduction in security risks of the extended connection. An illustration of a cascaded connection can be seen below.

This gateway MUST meet the requirements of connecting highest to lowest security domains

19.1.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3538]

When agencies have cascaded connections between networks involving multiple gateways they MUST ensure that the assurance levels specified for network devices between the overall lowest and highest networks are met by the gateway between the highest network and the next highest network within the cascaded connection.

19.1.11. Using gateways

19.1.11.R.01. Rationale

Physically locating all gateway components inside a secure server room will reduce the risk of unauthorised access to the device(s).

19.1.11.R.02. Rationale

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. 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.

Gateway components may also reside in a virtual environment – refer to Section 22.2 – Virtualisation and Section 22.3 – Virtual Local Area Networks

19.1.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3548]

Agencies MUST ensure that:

- all agency networks are protected from networks in other security domains by one or more gateways;
- all gateways contain mechanisms to filter or limit data flow at the network and content level to only the information necessary for business purposes; and
- all gateway components, discrete and virtual, are physically located within an appropriately secured server room.

19.1.11.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3551]

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.

19.1.12. Configuration of gateways

19.1.12.R.01. Rationale

Gateways are essential 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 give rise to information security incidents are especially important for gateways.

19.1.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3562]

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 (i.e. physically at the gateway or on a dedicated administration network);
- provide sufficient logging and audit capabilities to detect information security incidents, attempted intrusions or anomalous usage patterns; and
- provide real-time alerts.

19.1.13. Operation of gateways

19.1.13.R.01. Rationale

Providing an appropriate logging and audit capability will help to detect information security incidents and attempted network intrusions, allowing the agency to respond and to take measures to reduce the risk of future attempts.

19.1.13.R.02. Rationale

Storing event logs on a separate, secure log server will assist in preventing attackers from deleting logs in an attempt to destroy evidence of any intrusion.

19.1.13.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3578]

Agencies MUST ensure that all gateways connecting networks in different security domains:

- include a firewall of an appropriate assurance level 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; and
- have all controls tested to verify their effectiveness after any changes to their configuration.

19.1.14. Demilitarised zones

19.1.14.R.01. Rationale

Demilitarised zones are used to prevent direct access to information and systems on internal agency networks. Agencies that require certain information and systems to be accessed *from* the Internet or some other form of remote access, should place them in the less trusted demilitarised zone instead of on internal agency networks.

19.1.14.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3622]

Agencies MUST use demilitarised zones to house systems and information directly accessed externally.

19.1.14.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3623]

Agencies SHOULD use demilitarised zones to house systems and information directly accessed externally.

19.1.15. Risk assessment

19.1.15.R.01. Rationale

Performing a risk assessment on the gateway and its configuration prior to its implementation will assist in the early identification and mitigation of security risks.

19.1.15.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3626]

Agencies MUST perform a risk assessment on gateways and their configuration *prior* to their implementation.

19.1.16. Risk transfer

19.1.16.R.01. Rationale

Gateways could connect networks with different domain owners, including across agency boundaries. As a result, all domain and system owners MUST understand and accept the risks from all other networks before gateways are implemented.

19.1.16.C.01. Control

> All domain and system owners connected through a gateway MUST understand and accept the residual security risk of the gateway and from any connected domains including those via a cascaded connection.

19.1.16.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3633]

> Agencies SHOULD annually review the security architecture of the gateway and risks of all connected domains including those via a cascaded connection.

19.1.17. Information stakeholders and Shared Ownership

19.1.17.R.01. Rationale

> Changes to a domain connected to a gateway can affect the security posture of other connected domains. All domains owners should be considered stakeholders in all connected domains.

19.1.17.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3637]

> Once connectivity is established, domain owners MUST be considered information stakeholders for all connected domains.

19.1.17.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3640]

> Once connectivity is established, domain owners SHOULD be considered information stakeholders for all connected domains.

19.1.18. System user training

19.1.18.R.01. Rationale

> It is important that system users are competent to use gateways in a secure manner. This can be achieved through appropriate training before being granted access.

19.1.18.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3648]

> All system users MUST be trained on the secure use and security risks of the gateways before being granted access.

19.1.18.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3649]

> All system users SHOULD be trained in the secure use and security risks of the gateways before being granted access.

19.1.19. Administration of gateways

19.1.19.R.01. Rationale

> Application of role separation and segregation of duties in administration activities will protect against security risks posed by a malicious system user with extensive access to gateways.

19.1.19.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3660]

> Agencies MUST limit access to gateway administration functions.

19.1.19.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3663]

> Agencies MUST ensure that system administrators are formally trained to manage gateways by qualified trainers.

19.1.19.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:3668]

> Agencies MUST ensure that all system administrators of gateways that process NZEO information meet the nationality requirements for these endorsements.

19.1.19.C.04. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3672]

> Agencies MUST separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

19.1.19.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3676]

> Agencies SHOULD separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

19.1.20. System user authentication

19.1.20.R.01. Rationale

> Authentication to networks as well as gateways can reduce the risk of unauthorised access and provide an audit capability to support the investigation of information security incidents.

19.1.20.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3683]

> Agencies MUST authenticate system users to all classified networks accessed through gateways.

19.1.20.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3685]

> Agencies MUST ensure that only authenticated and authorised system users can use the gateway.

19.1.20.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3686]

> Agencies SHOULD use multi-factor authentication for access to networks and gateways.

19.1.21. IT equipment authentication

19.1.21.R.01. Rationale

> Authenticating IT equipment to networks accessed through gateways will assist in preventing unauthorised IT equipment connecting to a network.

19.1.21.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3695]

Agencies SHOULD authenticate any IT equipment that connects to networks accessed through gateways.

19.1.22. Configuration control

19.1.22.R.01. Rationale

To avoid changes that may introduce vulnerabilities into a gateway, agencies should fully consider any changes and associated risks. Changes may also necessitate re-certification and accreditation of the system, see Chapter 4 – System Certification and Accreditation.

19.1.22.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3702]

Agencies MUST undertake a risk assessment and update the SRMP before changes are implemented.

19.1.22.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3705]

Agencies MUST document any changes to gateways in accordance with the agency's Change Management Policy.

19.1.22.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3707]

Agencies SHOULD undertake a risk assessment and update the SRMP before changes are implemented.

19.1.23. Testing of gateways

19.1.23.R.01. Rationale

The testing of security measures on gateways will assist in ensuring that the integrity of the gateway is being maintained. An attacker who is aware of the regular testing schedule may cease malicious activities during such periods to avoid detection. Any test should, therefore, be unannounced and conducted at irregular intervals.

19.1.23.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:3712]

Agencies SHOULD ensure that testing of security measures is performed at random intervals no more than six months apart.

19.2. Cross Domain Solutions (CDS)

Objective

19.2.1. Cross-Domain Solutions secure transfers between systems of differing classifications or trust levels with high assurance over the security of systems and information.

Context

Scope

19.2.2. This section describes the use and implementation of Cross Domain Solutions (CDS).

19.2.3. CDS provide information flow control mechanisms at each layer of the OSI model with a higher level of assurance than typical gateways. This section extends the preceding Gateways section. CDS systems must apply controls from each section.

19.2.4. 19.2.1.   Additional information relating to topics covered in this section can be found in the following chapters and sections:

- Section 4.4 – Accreditation Framework;
- Section 8.2 – Servers and Network Devices;
- Section 8.3 – Network Infrastructure;
- Section 8.4 – IT Equipment;
- Chapter 12 – Product Security;
- Section 16.1 – Identification and Authentication;
- Section 16.5 – Event Logging and Auditing;
- Section 19.1 – Gateways;
- Section 19.3 – Firewalls;
- Section 19.4 – Diodes;
- Section 19.5 – Session Border Controllers;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 20.3 – Content Filtering.

Deploying Cross Domain Solutions

19.2.5. Consult the section on Firewalls in this chapter for devices used to control data flow in bi-directional gateways.

19.2.6. Consult the section on Diodes in this chapter for devices used to control data flow in uni-directional gateways.

19.2.7. Consult the Data Transfers and Content Filtering sections for requirements on appropriately controlling data flows in both bi-directional and uni-directional gateways
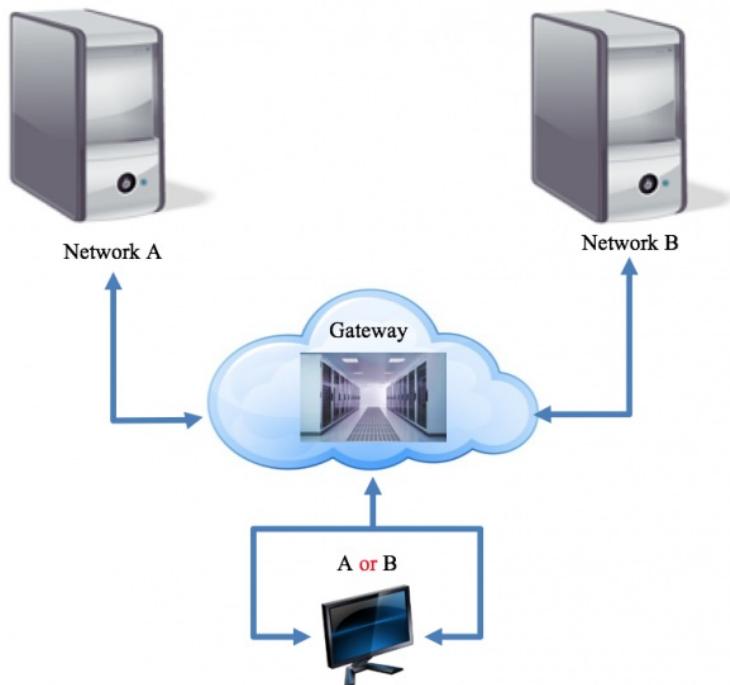
Types of gateways

19.2.8. This manual defines three types of gateways:

- access gateways;
- multilevel gateways; and
- transfer gateways.
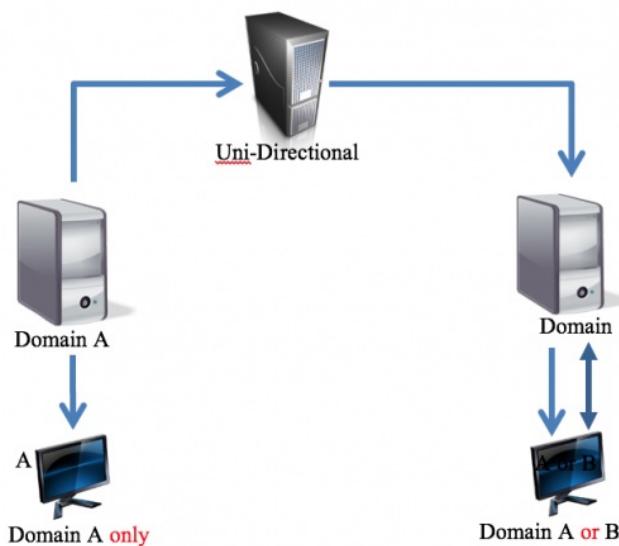
Access Gateway

19.2.9.   An access gateway provides the system user with access to multiple security domains from a single device.
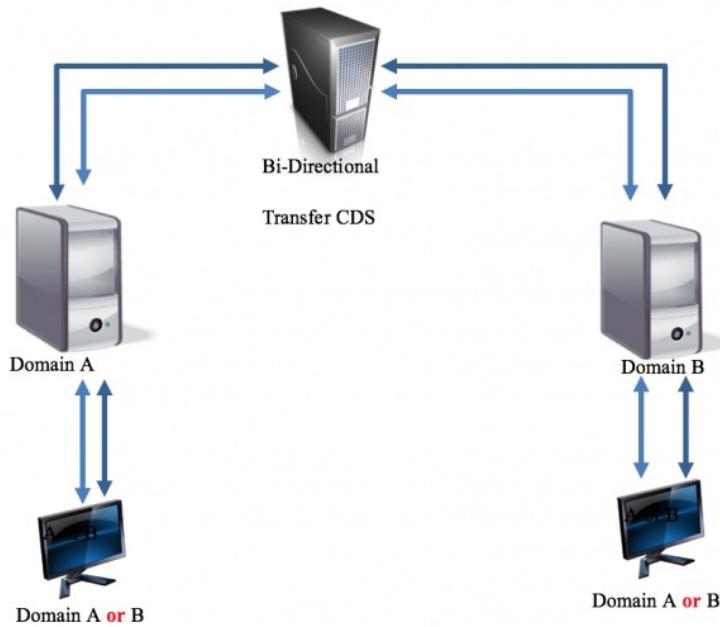
19.2.10. A transfer gateway facilitates the transfer of information, in one or multiple directions (low to high or high to low) between different security domains. A traditional gateway to the Internet is considered a form of transfer gateway.
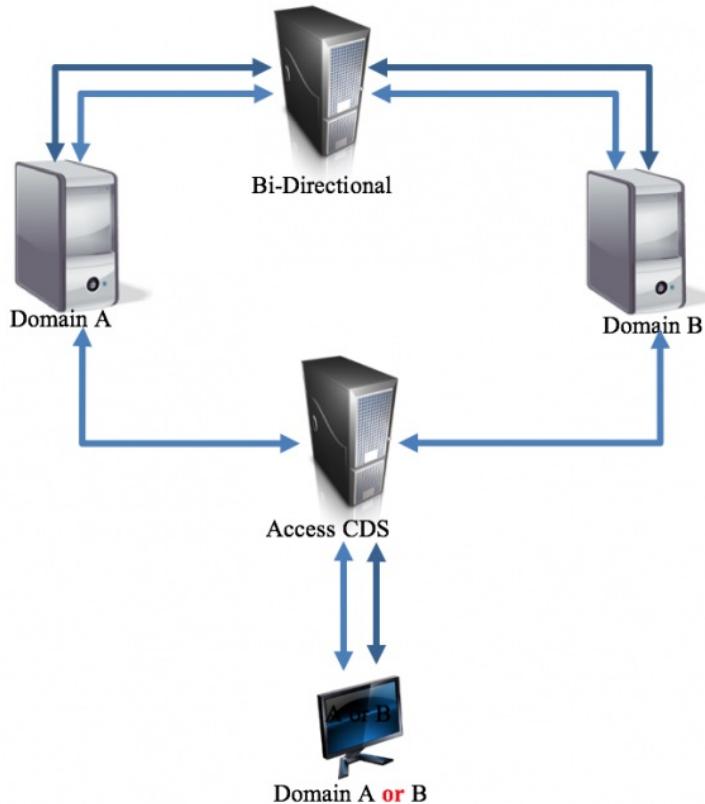
19.2.11. The following illustrates a Uni-Directional Transfer Cross Domain Solution.

19.2.12. A Bi-Directional Cross Domain Solution enables access, based on authorisations, to data at multiple classifications and releasability levels.

19.2.13. A Multi-Level Transfer Cross Domain Solution enables access, based on authorisations, to data at multiple classifications and releasability levels.

References

19.2.14. Additional guidance can be found at:

Title	Publisher	Source
Information Assurance Guidance For Systems Based On A Security Real-Time Operating System Systems Security Engineering, Sse-100-1, 14 December 2005	NSA	http://www.nsa.gov/ia/_files/SSE-100-1.pdf
Solving the Cross-Domain Conundrum, Colonel Bernard F. Koelsch United States Army, 2013	US Army War College	http://handle.dtic.mil/100.2/ADA589325
Client Side Cross-Domain Security, Microsoft Corporation June 2008	Microsoft	https://msdn.microsoft.com/en-us/library/cc709423(v=vs.85).aspx

Secure Cross Domain Solution	Detica, BAE Systems	https://www.apm.org.uk/sites/default/files/protected/Secure%20Cross%20Domain%20Solutions%20v0.10c.pdf
Cross Domain Security Primer	CSE Canada	https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsb120-eng.pdf
Shedding Light on Cross Domain Solutions	SANS	https://www.sans.org/reading-room/whitepapers/dlp/shedding-light-cross-domain-solutions-36492

Rationale & Controls

19.2.15. Gateway classification

19.2.15.R.01. Rationale

The trust level or classification of systems directs users and systems administrators to the appropriate handling instructions and level of protection required for those systems. This aids in the selection of systems controls.

19.2.15.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3870]

For the purposes of this Manual, the CDS MUST be classified at the highest classification of connected domains.

19.2.16. Allowable gateways

19.2.16.R.01. Rationale

Connecting systems to the Internet attracts significant risk and so highly classified systems are prohibited from being *directly* connected to each other or to the Internet. If an agency wishes to connect a highly classified system to the Internet the connection will need to be cascaded through a system of a lesser classification that is approved to connect directly to the Internet.

19.2.16.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3880]

Agencies connecting a TOP SECRET, SECRET OR CONFIDENTIAL network to any other network MUST implement a CDS.

19.2.16.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:3887]

Agencies MUST NOT implement a gateway permitting data to flow directly from:

- a TOP SECRET network to any network below SECRET;
- a SECRET network to an UNCLASSIFIED network; or
- a CONFIDENTIAL network to an UNCLASSIFIED network.

19.2.17. Implementing Cross Domain Solutions

19.2.17.R.01. Rationale

Connecting multiple sets of gateways and Cross Domain Solutions (CDS) increases the threat surface and, consequently, the likelihood and impact of a network compromise. When a gateway and a CDS share a common network, the higher security domain (such as a classified agency network) can be exposed to malicious activity, exploitation or denial of service from the lower security domain (such as the Internet).

19.2.17.R.02. Rationale

To manage this risk, CDS should implement products that have completed a high assurance evaluation, see Chapter 12 – Product Security. The AISEP Evaluated Product List (EPL) includes products that have been evaluated in the high assurance scheme but is not an exhaustive list.

Where CDS are not listed on the AISEP EPL, the GCSB can provide guidance on product selection and implementation on request.

19.2.17.C.01. Control System Classification(s): Confidential, Secret; Compliance: MUST [CID:3926]

When designing and deploying a CDS, agencies MUST consult with the GCSB and comply with all directions provided.

19.2.17.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3927]

Agencies connecting a typical gateway and a CDS to a common network MUST consult the GCSB on the impact to the security of the CDS and comply with all directions provided.

19.2.18. Separation of data flows

19.2.18.R.01. Rationale

Gateways connecting highly classified systems to lower classified, or Internet connected systems need to incorporate physically separate paths to provide stronger control of information flows. Typically this is achieved through separate pathing and the use of diodes. Such gateways are generally restricted to process and communicate only highly-structured formal messaging traffic.

19.2.18.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3929]

Agencies MUST ensure that all bi-directional gateways between TOP SECRET and SECRET networks, SECRET and less classified networks, and CONFIDENTIAL and less classified networks, have separate upward and downward paths which use a diode and physically separate infrastructure for each path.

19.2.19. Trusted sources

19.2.19.R.01. Rationale

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such the CISO and the ITSM.

19.2.19.C.01. Control

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

19.2.19.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3933]

Trusted sources MUST authorise all data to be exported from a security domain.

19.2.20. Operation of the Cross Domain Solution

19.2.20.R.01. Rationale

The highly sensitive nature of the data within cross domain solutions requires additional audit and logging for control, management, record and forensic purposes. This is in addition to the audit and logging requirements in Section 16.5 – Event Logging and Auditing.

19.2.20.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:3936]

All data exported from a security domain MUST be logged.

19.3. Firewalls

Objective

19.3.1. Agencies operating bi-directional gateways implement firewalls and traffic flow filters to provide a protective layer to their networks in both discrete and virtual environments.

Context

Scope

19.3.2. This section covers information relating to filtering requirements for bi-direction gateways between networks of different security domains.

19.3.3. When a control specifies a requirement for a diode or filter the appropriate information can be found within Section 19.4 –Diodes and Section 20.3 – Content Filtering.

19.3.4. Additional information that also applies to topics covered in the section can be found in:

- Chapter 12 – Product Security which provides advice on the selection of evaluated products;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 22.2 – Virtualisation.

Inter-connecting networks within an agency

19.3.5. When connecting networks accredited to the same classification and set of endorsements within an agency the requirements of this section may not apply. When connecting networks accredited with different classifications or endorsements within an agency the information in this section applies.

Connecting agency networks to the Internet

19.3.6. When connecting an agency network to the Internet, the Internet is considered an UNCLASSIFIED and insecure network.

References

19.3.7. Further information on the Network Device Protection Profile (NDPP) and firewalls can be found at:

Title	Publisher	Source
Network Device Protection Profile (NDPP)	(US) National Information Assurance Partnership	http://www.niap-ccevs.org/pp/pp_nd_v1.0/

Rationale & Controls

19.3.8. Firewall assurance levels

19.3.8.R.01. Rationale

The higher the required assurance level for a firewall, the greater the assurance that it provides an appropriate level of protection against an attacker. For example, an EAL2 firewall is certified to provide protection against a basic threat potential, whilst an EAL4 firewall is certified to provide protection against a moderate threat potential. A Protection Profile (PP) is considered to be equivalent to EAL2 under its Common Criteria Recognition Arrangement.

19.3.8.R.02. Rationale

If a uni-directional connection between two networks is being implemented only one gateway is necessary with requirements being determined based on the source and destination networks. However, if a bi-directional connection between two networks is being implemented both gateways will be configured and implemented with requirements being determined based on the source and destination networks.

19.3.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:3970]

All gateways MUST contain a firewall in both physical and virtual environments.

19.3.8.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:3973]

Agencies MUST check the evaluation has examined the security enforcing functions by reviewing the target of evaluation/security target and other testing documentation.

19.3.8.C.03.   Control

Agencies MUST use devices as shown in the following table for their gateway when connecting two networks of different classifications or two networks of the same classification but of different security domains.

Your network		Their network	You require	They require
RESTRICTED and below		UNCLASSIFIED	EAL4 firewall	N/A
		RESTRICTED	EAL2 or PP firewall	EAL2 or PP firewall
		CONFIDENTIAL	EAL2 or PP firewall	EAL4 firewall
		SECRET	EAL2 or PP firewall	EAL4 firewall
		TOP SECRET	EAL2 or PP firewall	Consultation with GCSB
CONFIDENTIAL		UNCLASSIFIED	Consultation with GCSB	N/A
		RESTRICTED	EAL4 firewall	EAL2 or PP firewall
		CONFIDENTIAL	EAL2 or PP firewall	EAL2 or PP firewall
		SECRET	EAL2 or PP firewall	EAL4 firewall
		TOP SECRET	EAL2 or PP firewall	Consultation with GCSB
SECRET		UNCLASSIFIED	Consultation with GCSB	N/A
		RESTRICTED	EAL4 firewall	EAL2 or PP firewall
		CONFIDENTIAL	EAL4 firewall	EAL2 or PP firewall
		SECRET	EAL2 or PP firewall	EAL2 or PP firewall
		TOP SECRET	EAL2 or PP firewall	EAL4 firewall
TOP SECRET		UNCLASSIFIED	Consultation with GCSB	N/A
		RESTRICTED	Consultation with GCSB	EAL2 or PP firewall
		CONFIDENTIAL	Consultation with GCSB	EAL2 or PP firewall
		SECRET	EAL4 firewall	EAL2 or PP firewall
		TOP SECRET	EAL4 firewall	EAL4 firewall

19.3.8.C.04.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3996]

The requirement to implement a firewall as part of gateway architecture MUST be met separately and independently by both parties (gateways) in both physical and virtual environments.

Shared equipment DOES NOT satisfy the requirements of this control.

19.3.9. Firewall assurance levels for NZEO networks

19.3.9.R.01.   Rationale

As NZEO networks are particularly sensitive, additional security measures need to be put in place when connecting them to other networks.

19.3.9.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:3999]

Agencies MUST use a firewall of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for firewalls between networks of different classifications or security domains.

19.3.9.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4000]

In all other circumstances the table at 19.3.8.C.03 MUST apply.

19.3.9.C.03.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4001]

Agencies SHOULD use a firewall of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.

19.4. Diodes

Objective

19.4.1. Networks connected to one-way (uni-directional) gateways implement diodes in order to protect the higher classified system.

Context

Scope

19.4.2. This section covers information relating to filtering requirements for one-way gateways used to facilitate data transfers. Additional information that also applies to topics covered in the section can be found in:

- Chapter 12 – Product Security which provides advice on selecting evaluated products.
- Section 20.1 – Data Transfers; and
- Section 20.2 – Data Import and Export;

References

19.4.3. Further information on the Evaluated Products List can be found at:

Title	Publisher	Source
Evaluated Products List (EPL)	AISEP	https://www.cyber.gov.au/publications/evaluated-products-list

Rationale & Controls

19.4.4. Diode assurance levels

19.4.4.R.01. Rationale

A diode enforces one-way flow of network traffic thus requiring separate paths for incoming and outgoing data. As such, it is much more difficult for an attacker to use the same path to both launch an attack and release the information. Using diodes of higher assurance levels for higher classified networks provides an appropriate level of assurance to agencies that the specified security functionality of the product will operate as claimed.

19.4.4.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4015]

Agencies MUST use devices as shown in the following table for controlling the data flow of one-way gateways between networks of different classifications.

High networr		Low network	You require
RESTRICTED		UNCLASSIFIED	EAL2 or PP diode
		RESTRICTED	EAL2 or PP diode
CONFIDENTIAL		UNCLASSIFIED	high assurance diode
		RESTRICTED	high assurance diode
		CONFIDENTIAL	high assurance diode
SECRET		UNCLASSIFIED	high assurance diode
		RESTRICTED	high assurance diode
		CONFIDENTIAL	high assurance diode
		SECRET	high assurance diode
TOP SECRET		UNCLASSIFIED	high assurance diode
		RESTRICTED	high assurance diode
		CONFIDENTIAL	high assurance diode
		SECRET	high assurance diode
		TOP SECRET	high assurance diode

19.4.5. Diode assurance levels for NZEO networks

19.4.5.R.01. Rationale

As NZEO networks are particularly sensitive additional security measures are necessary when connecting them to other networks.

19.4.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4028]

Agencies MUST use a diode of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for diodes between networks of different classifications.

19.4.5.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4030]

In all other circumstances the table at 19.4.4.C.01 MUST apply.

19.4.5.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4032]

Agencies SHOULD use a diode of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.

19.4.6. Volume Checking

19.4.6.R.01.   Rationale

Monitoring the volume of data being transferred across a diode will ensure 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.

19.4.6.C.01.   ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4039]

Agencies deploying a diode to control data flow within one-way gateways SHOULD monitor the volume of the data being transferred.

19.5. Session Border Controllers

Objective

19.5.1.   To ensure the use of Session Border Controllers (SBCs) is integrated with the agency's security architecture and that use is consistent with other requirements for gateway security in this chapter.

Context

Scope

19.5.2.   This section encompasses the use of SBCs in Voice over Internet Protocol (VoIP) and Unified Communication (UC) networks within an agency. It describes key risks and threats and provides guidance on the conceptual design of security for such systems.

19.5.3.   It is important to note that Service Providers generally have operational objectives different to those of the agency and typically they will:

- Design a highly operationally optimised network requiring minimal maintenance;
- Provide resources, including SBCs, softswitches and media gateways that are shared between a number of customers (such as multi-tenanted data centres);
- The standard model may not accommodate all unique agency or NZ Government requirements which will then require special consideration.

19.5.4.   Reference should also be made to the following sections:

- Chapter 6 – Information Security Monitoring;
- Chapter 7 – Information Security Incidents;
- Chapter 9 – Personnel Security;
- Chapter 11 – Communications Systems and Devices;
- Section 13.1.12 – Archiving;
- Chapter 16 – Access Control;
- Section 18.3 - Video & Telephony Conferencing and Internet Protocol Telephony

Definitions

19.5.5.   A **Session Border Controller** (**SBC**) is a device (physical or virtual) used in IP networks to control and manage the signalling and media streams of real-time UC and VoIP connections. See also Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony It includes establishing, controlling, and terminating calls, interactive media communications or other VoIP connections. SBCs enable VoIP traffic to navigate gateways and firewalls and ensure interoperability between different SIP implementations. Careful selection of SBCs will provide such functionality as prevention of toll fraud, resistance to denial of service attacks and resistance to eavesdropping.

19.5.6.   **Unified Communications (UC)** is a term describing the integration of real-time and near real time communication and interaction services in an organisation or agency. UC may integrate several communication systems including unified messaging, collaboration, and interaction systems; real-time and near real-time communications; and transactional applications.

19.5.7.   UC may, for example, include services such as instant messaging (chat), presence information, voice, mobility, audio, web & video conferencing, data sharing (such as interactive whiteboards), voicemail, e-mail, SMS and fax. UC is not necessarily a single product, but more usually a set of products designed to provide a unified user-interface and user-experience across multiple devices and media-types.

Purpose

19.5.8.   Traditional demarcation points, such as media gateways, are no longer natural boundaries. Older firewall technology impacts the performance of communications systems, including VoIP and UC. SBCs were introduced to improve performance and provide interoperability with real-time and near real-time communications. They provide a new natural demarcation point.

19.5.9.   SBCs can provide a demarcation or normalisation point within the agency's network, allow enforcement of agency specific security policies and provide a greater degree of accountability than the usual contract with service providers.

Risks and Threats

19.5.10. Risks and threats associated with the use of VoIP and UC include:

- Confidentiality (eavesdropping);
- Integrity (enabling fraud and theft as well as compromising privacy); and
- Availability (including Denial of Service [DoS or DDoS]).

Confidentiality

19.5.11. There is a high likelihood of eavesdropping in VoIP systems. Traditional telephone systems require physical access to tap a line or compromise a PABX or switch. In VoIP networks, virtual LAN environments can be exploited remotely to identify weaknesses within and between virtual LANs and gain access to valuable information. Sniffing is another form of eavesdropping that involves capturing unencrypted voice traffic with malware or a specific VoIP sniffer tool. In common with other Internet connected systems, man-in-the-middle exploits are also used to eavesdrop on both data and VoIP networks.

Integrity

19.5.12. Exploits such as caller ID spoofing are relatively easy to execute and can be extremely costly to businesses. Information from a stolen credit card or acquisition of other sensitive data, can compromise an employee's caller ID, and have funds transferred while posing as the employee. Cyber criminals

can also change an employee's registration information in order to eavesdrop on or intercept all incoming calls for that individual.

19.5.13. Integrity compromise may include modification or insertion into UC. As many UC elements, such as voicemail or email, may encompass electronic records as defined in legislation it is vital that these elements are preserved unaltered.

Availability

19.5.14. Because VoIP and UC places high levels of demand on any network, managing Quality of Service (QoS), latency, jitter, packet loss and other service impediments are important aspects of availability. In the event of major faults or outages, diversity and fault tolerance is vital for all key sites. To enable failover, for example, where calls leave the customer network, call diversity and call failover are essential configuration elements.

Denial of Service

19.5.15. Denial of Service (DoS) attacks abuse signalling protocols to deny availability of VoIP data and degrade performance. If the telecommunications network is compromised, it is possible to also traverse systems to attack or infect the agency's data networks and other systems.

Common VoIP and UC Security Risks and Threats

19.5.16. Common VoIP and UC security risks and threats.

Risk	Typical Symptoms	Threst	Countermeasures
Reconnaissance scan	Address or port scan is used to footprint network topology	Targeted denial of service, fraud, theft	- Intrusion detection - Protection against registration floods
Man in the middle	Attacker intercepts session to impersonate(spoof) caller	Targeted denial of service, breach of privacy, fraud, theft	TLS encryption for SIP with separate TLS certificates for SIP Service Providers
Eavesdropping	Attacker "sniffs" session for the purpose of social engineering	Breach of privacy, fraud, theft	- Intrusion detection - Encryption
Session hijacking	Attacker compromises valuable information by rerouting call	Breach of privacy, fraud, theft	Intrusion detection
Session overload	Excessive signalling or media traffic(malicious, non-malicious) is experienced	Denial of service	Protection against registration floods
Protocol fuzzing	Malformed packets, semantically or syntactically incorrect flows are encountered	Denial of service	- Malformed packet protection - Protocol anomaly protection - TCP reassembly for fragmented packet protection - Strict TCP validation to ensure TCP session state enforcement, validation of sequence and acknowledgement numbers, rejection of bad TCP flag combinations
Media injection	Attacker inserts unwanted or corrupted content into messages compromising packet/data stream integrity	Denial of service, fraud	- Application aware firewalls - Intrusion prevention /detection - Encryption
Toll Fraud	Unexplained/unusual calling activity, increased costs/carrier notification/alert	Fraud, financial loss, breach of privacy, information loss	- Application aware firewalls - Intrusion prevention /detection - Encryption

19.5.17. Encryption is discussed in Chapter 17 - Cryptography.

Product Selection

Protection Profiles

19.5.18. One Protection Profile for SBCs has been published by NIAP (dated July 24, 2015 - see reference table). Several other Protection profiles (PPs) specifically for SBCs are in development but not yet published (as at September 2015). Gateway and other border control device PPs are used as surrogates in the interim. Refer to Chapter 12 – Product Security.
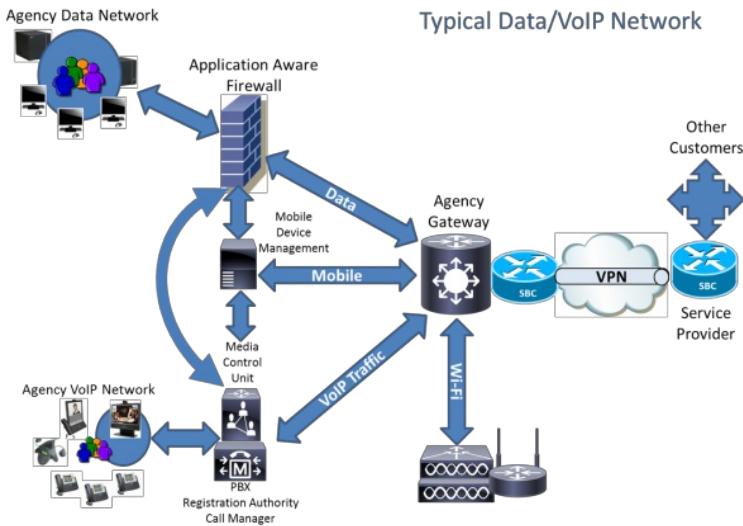
Desirable SBC Functionality

19.5.19. To manage risks and threats and to safeguard performance there are a number of desirable features in an SBC. These include:

- Security – SBC DoS protection, access control, topology hiding, VPN separation, service infrastructure DoS prevention;
- Encryption – Support for Suite B encryption;
- Service Reach – surrogate registration IP PBX endpoints, SIP IMS-H.323 PBX IWF; VPN bridging;
- SLA assurance – admission control; bandwidth per VPN & site, session agent constraints, policy server; intra-VPN media release; QoS marking/mapping; QoS reporting;
- Fraud and Revenue protection – bandwidth policing, QoS theft protection, accounting, session timers;
- Regulatory compliance – provision of emergency service calls (111) & lawful intercept.

Security Architecture

19.5.20. Typical use of session border controller in an agency gateway is illustrated in Figure 1 below:

General References

19.5.21. Additional information on Session Border Controllers can be found in the following references:

Reference	Title	Publisher	Source
SP 800-58	Security Considerations for Voice Over IP Systems	NIST	http://csrc.nist.gov/publications/nistpubs/
	Security Issues and Countermeasure for VoIP	SANS	http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701
Report Number: I332-016R-2005	Security Guidance for Deploying IP Telephony Systems Released: 14 February 2006	Systems and Network Attack Center (SNAC) NSA	https://www.nsa.gov/ia/_files/voip/i332-016r-2005.pdf
Report Number: I332-009R-2006	Recommended IP Telephony Architecture, Updated: 1May2006 Version1.0	Systems and Network Attack Center (SNAC) NSA	https://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf
	Mobility Capability Package March 26 2012 - Secure VoIP Version 1.2	NSA	https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_1_2.pdf
	Protecting Telephone-based Payment Card Data PCI Data Security Standard (PCI DSS) Version: 2.0, March 2011	The PCI Security Standards Council (PCI SSC)	https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf
	Understanding Voice over Internet Protocol (VoIP): 2006	US-CERT	https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf

CNSS Instruction No. 5000 April 2007	Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony	Committee on National Security Systems	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
	Infrastructure qualified for Microsoft Lync	Microsoft TechNet	https://technet.microsoft.com/en-us/office/dn788945.aspx
	A Guide to the Public Records Act	Archives New Zealand	http://records.archives.govt.nz/home/public-records-act-2005/
Public Act 2002 No.35	Electronic Transactions Act 2002		http://www.legislation.govt.nz/act/public/2002/0035/latest/DLM154185.html
	Network Device Collaborative Protection Profile (NDcPP) Extended Package Session Border Controller, July 2015	NIAP	https://www.niap-ccevs.org/pp/cpp_nd_sbc_ep_v1.0.pdf
	Protection Profile for Voice Over IP (VoIP) Applications, 3 November 2014, Version 1.3		https://www.niap-ccevs.org/pp/cpp_nd_sbc_ep_v1.0.pdf
	DHS 4300A Sensitive Systems Handbook Attachment Q5 To Handbook v. 11.0 Voice over Internet Protocol (VoIP) Version 11.0 December 22, 2014	DHS	http://www.dhs.gov/sites/default/files/publications/4300A%20Handbook%20Attachment%20Q5%20-%20Voice%20over%20VoIP.pdf
	2015 Global Fraud Loss Survey	CFCA	http://www.cfca.org/fraudlosssurvey

Media Technical References

19.5.22. Media technical references are listed below:

Reference	Title	Publisher	Source
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	IETF	www.ietf.org/
RFC 3313	Private Session Initiation Protocol (SIP) Extensions for Media Authorization	IETF	www.ietf.org/
RFC 3550	RTP: A Transport Protocol for Real-Time Applications	IETF	www.ietf.org/
RFC 3685	Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)	IETF	www.ietf.org/
RFC 3362	Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration	IETF	www.ietf.org/
T.38 (09/2010)	Procedures for real-time Group 3 facsimile communication over IP networks	International Telecommunication Union	http://www.itu.int/rec/T-REC-T.38/e
V.150.1 (01/2003)	Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs	International Telecommunication Union	https://www.itu.int/rec/T-REC-V.150.1-200301-I/en
G.711	Pulse code modulation (PCM) of voice frequencies	International Telecommunication Union	http://www.itu.int/rec/T-REC-G.711/
G.726	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)	International Telecommunication Union	http://www.itu.int/rec/T-REC-G.726/e
G. 729 (06/2012)	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)	International Telecommunication Union	http://www.itu.int/rec/T-REC-G.729/e

Signalling Technical References

19.5.23. Signalling technical references are listed below:

Reference	Title	Publisher	Source
RFC 2705	Media Gateway Control Protocol (MGCP) Version 1.0	IEFT	www.ietf.org/
RFC 3525	Gateway Control Protocol Version 1.0	IEFT	www.ietf.org/
RFC 3261	SIP: Session Initiation Protocol	IEFT	www.ietf.org/
RFC 3263	Locating SIP Servers	IEFT	www.ietf.org/
draft-ietf-sip-session-timer	SIP Session Timer	IEFT	www.ietf.org/
RFC 3966	The tel URI for Telephone Numbers	IEFT	www.ietf.org/
RFC 3924	Cisco Architecture for Lawful Intercept in IP Networks	IEFT	www.ietf.org/
RFC 2327	Session Description Protocol	IEFT	www.ietf.org/
RFC 3025	Gateway Control Protocol Version 1, June 2003	IEFT	www.ietf.org/
H.248 (03/2013)	Media Gateway Control (Megaco): Version 3	International Telecommunication Union	http://www.itu.int/rec/T-REC-H.248.1/en
H.323 (12/2009)	Packet-based multimedia communications systems	International Telecommunication Union	http://www.itu.int/rec/T-REC-H.323/en/
H.450	Supplementary Services for H.323	International Telecommunication Union	http://www.itu.int/
MSF Technical Report MSF-TR-QoS-001-FINAL	Quality of Service for next generation VoIP networks framework	Multiservice Switching Forum	http://www.recursosvoip.com/docs/english/MSF-TR-QoS-001-FINAL.pdf
ETSI TS 129 305 V8.0.0 (2009-01)	Universal Mobile Telecommunications System (UMTS); LTE; InterWorking Function (IWF) between MAP based and Diameter based interfaces.	European Telecommunications Standards Institute	http://www.etsi.org/deliver/etsi_ts/129300_129399/129305/08.00.00.60/ts_129305v080000p.pdf

Rationale & Controls

19.5.24. Risk Assessment

19.5.24.R.01. Rationale

The adoption of Voice over Internet Protocol (VoIP) and Unified Communication (UC) networks will introduce a range of technology risks *in addition* to the technology and systems risks that already exist for agency systems. It is vital that these risks are identified and assessed in order to design a robust security architecture and to select appropriate controls and countermeasures.

19.5.24.R.02. Rationale

The availability of agency systems, business functionality and any customer or client online services, is subject to further risks in an outsourced environment. A risk assessment will include consideration of business requirements on availability in a VoIP and UC environment.

19.5.24.R.03. Rationale

Risks to business functionality may include service outages, such as communications, data centre power, backup and other failures or interruptions. Entity failures such as the merger, acquisition or liquidation of the service provider may also present a significant business risk to availability.

19.5.24.R.04. Rationale

Testing is a valuable tool when assessing risk. A UC environment with complex communications streams can provide opportunities for exploitation, especially where the configuration is weak or has itself been compromised. One of the fundamental tools is penetration testing.

19.5.24.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4703]

Agencies intending to adopt VoIP or UC technologies or services MUST conduct a comprehensive risk assessment *before* implementation or adoption.

19.5.24.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4705]

Agencies intending to adopt VoIP or UC technologies or services MUST consider the risks to the availability of systems and information in their design of VoIP and UC systems architecture, fault tolerance, fail over and supporting controls and governance processes.

19.5.24.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4706]

Agencies MUST ensure risks for any VoIP or UC service adopted are understood and formally accepted by the agency's Accreditation Authority as part of the Certification and Accreditation process (See Chapter 4 - System Certification and Accreditation).

19.5.24.C.04. Control [CID:4707]

Agencies intending to adopt VoIP or UC technologies or services MUST determine where the responsibility (agency or VoIP and UC service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.

19.5.24.C.05. Control System Classification(s): All Classifications; Compliance: MUST [CID:4708]

Any contracts for the provision of VoIP or UC services MUST include service level, availability, recoverability and restoration provisions as formally determined by business requirements.

19.5.24.C.06. Control System Classification(s): All Classifications; Compliance: MUST [CID:4709]

Agencies MUST ensure contracts with VoIP or UC service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of VoIP or UC services.

19.5.24.C.07. Control System Classification(s): All Classifications; Compliance: MUST [CID:4710]

Agencies procuring or using VoIP or UC services to be used by multiple agencies MUST ensure all interested parties formally agree to the risks, controls and any residual risks of such VoIP and UC services. The lead agency normally has this responsibility (see Chapter 2 - Information Security within Government and Chapter 4 - System Certification and Accreditation).

19.5.24.C.08. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4711]

Agencies SHOULD consider the use of assessment tools, such as penetration testing, when undertaking the risk assessment.

19.5.25. Non-Agency Networks

19.5.25.R.01. Rationale

Networks furnished by a service provider are invariably shared networks. Much of the security configuration is designed to maximise operational efficiency of the Service Providers network. Any agency specific security requirements may attract additional cost.

19.5.25.R.02. Rationale

It is preferable to maintain an agency designed and controlled gateway to ensure security requirements are properly accommodated. The use of SBCs should be carefully considered in order to maximise efficiency consistent with security requirements.

19.5.25.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4715]

Agencies MUST follow the gateway requirements described in Chapter 19 - Gateway Security.

19.5.26. Security Architecture and Configuration

19.5.26.R.01. Rationale

Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied. Trust zones and trust boundaries are discussed in 22.1.3. The use of SBCs will assist with the definition of trust boundaries and allow the segregation of UC and normal data.

19.5.26.R.02. Rationale

The threat model for IP is well understood. Data packets can be intercepted or eavesdropped anywhere along the transmission path including the corporate network, by the internet service provider and along the backbone. The prevalence and ease of packet sniffing and other techniques for capturing packets on an IP based network increases this threat level. VoIP Encryption is an effective means of mitigating this threat.

19.5.26.R.03. Rationale

The nature of traffic through an SBC is an important factor in determining the type and configuration of the SBC. This also plays an important role in determining the resilience of the system. Systems may require high availability (HA), depending on business requirements for availability and continuity of service. The use of split trunks for HA normal traffic may provide resilience at reduced costs.

19.5.26.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4720]

Agencies intending to adopt VoIP or UC technologies or services MUST determine trust boundaries *before* implementation.

19.5.26.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4721]

Updates to the SBC and related devices MUST be verified by the administrator to ensure they are obtained from a trusted source and are unaltered.

19.5.26.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4722]

Agencies MUST include defence mechanisms for the Common VoIP and UC Security Risks and Threats described in 19.5.10.

19.5.26.C.04. Control System Classification(s): All Classifications; Compliance: MUST [CID:4723]

Agency networks MUST ensure the SBC includes a topology hiding capability.

19.5.26.C.05. Control System Classification(s): All Classifications; Compliance: MUST [CID:4724]

Agency networks MUST consider the use of call diversity and call failover configurations.

19.5.26.C.06. Control System Classification(s): All Classifications; Compliance: MUST [CID:4725]

In a virtualised environment, agencies MUST ensure any data contained in a protected resource is deleted or not available when the virtual resource is reallocated.

19.5.26.C.07. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4726]

Agencies SHOULD conduct a traffic analysis to ensure the agency's network and architecture is capable of supporting all VoIP, media and UC traffic. The traffic analysis SHOULD also determine any high availability requirements.

19.5.26.C.08. Control

Agencies SHOULD design a security and gateway architecture that segregates UC and normal data traffic. Firewall requirements (Section 19.3 - Firewalls) continue to apply to data traffic.

19.5.26.C.09. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4728]

In a virtualised environment, agencies SHOULD create separate virtual LANs for data traffic and UC traffic.

19.5.26.C.10. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4729]

In a non-virtualised environment, agencies SHOULD create separate LANs for data traffic and UC traffic.

19.5.26.C.11. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4730]

Agency networks SHOULD use encryption internally on VoIP and unified communications traffic.

19.5.26.C.12. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4731]

Agency networks SHOULD ensure intrusion prevention systems and firewalls are VoIP-aware.

19.5.27. Access Control

19.5.27.R.01. Rationale

Network access control and password requirements are described in Chapter 16 - Access Control, in particular Section 16.5 – Event Logging and Auditing. Event logging helps improve the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected and assist in the investigation of incidents. A fundamental of access control is to manage access rights including physical access, file system and data access permissions and programme execution permissions. In addition, access control provides a record of usage in the event of an incident. Retention of records and archiving is discussed in 13.1.12 - Archiving.

19.5.27.R.02. Rationale

Similar requirements apply to VoIP and UC networks as these are also IP based. This will include any service enabled as part of the UC environment, such as Chat, IM, video and teleconferencing.

19.5.27.R.03. Rationale

There may be special cases, such as a 24x7 operations centre, where VoIP phones are shared by several duty officers on a shift basis. Workloads may require a number of duty personnel at any one time. In such cases it may be impractical to allocate individual VoIP or UC UserID and passwords. The risks in such cases must be clearly identified and compensating controls applied to ensure traceability in the event of fault finding or an incident. Examples of compensating controls include physical access control, CCTV, and duty registers. Identification of shared facilities is important and may comprise a UserID such as "Duty Officer", SOC, or agency name in a multi-agency facility.

19.5.27.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4737]

Any shared facilities MUST be clearly identifiable both physically and logically.

19.5.27.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4738]

Agencies MUST provide a protected communication channel for administrators, and authorised systems personnel. Such communication MUST be logged.

19.5.27.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4739]

Agencies MUST ensure administrative access to the SBC is available only through a trusted LAN and secure communication path.

19.5.27.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4740]

Access control and password requirements SHOULD apply to VoIP and UC networks in all cases where individual access is granted.

19.5.27.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4741]

In special cases where individual UserIDs and Passwords are impractical, a risk assessment SHOULD be completed and compensating controls applied.

19.5.27.C.06. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4742]

Event logs covering all VoIP and UC services SHOULD be maintained in accordance with the requirements of the NZISM. See section 16.5 - Event logging and Auditing and 13.1.12 - Archiving.

19.5.28. Incident Handling and Management

19.5.28.R.01. Rationale

Service providers may not provide the same level of incident identification and management as provided by agencies. In some cases, these services will attract additional costs. Careful management of contracts is required to ensure agency requirements for incident detection and management are fully met when adopting VoIP and UC services.

19.5.28.R.02. Rationale

Blacklisting allows blocking of calls to specific numbers, range of numbers or countries. Whitelisting specifically allows calls to numbers, range of numbers or countries. A combination of black and white listing enables a flexible method of preventing call fraud (hijacking and "call pumping") where forbidden destinations are blacklisted and exceptions are whitelisted. This, for example, allows calls to a specific number within a forbidden country.

19.5.28.R.03. Rationale

Call Rate Limiting allows the restriction of outbound call volumes to specific numbers, range of numbers or countries. This is a useful mitigation

for "traffic pumping" call fraud schemes. Call rate limiting also allows temporary limits to be placed on call from or to particular destinations while a security incident is investigated.

19.5.28.R.04. Rationale

Call Redirection enables the transfer of blocked calls to another destination including via monitoring and recording systems. Blocked calls may be dropped or a message played indicating, for example, that calls cannot be connected.

19.5.28.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4748]

Agencies MUST include incident handling and management services in contracts with service providers.

19.5.28.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4749]

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

19.5.28.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4750]

Agencies SHOULD implement fraud detection monitoring to identify suspicious activity and provide alerting so that remedial action can be taken.

19.5.28.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4751]

Agencies SHOULD regularly review call detail records for patterns of service theft.

19.5.28.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4752]

Agencies SHOULD consider the use of blacklisting and whitelisting to manage fraudulent calls to known fraudulent call destinations.

19.5.28.C.06. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4753]

Agencies SHOULD consider the use of call rate limiting as a fraud mitigation measure.

19.5.28.C.07. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4755]

Agencies SHOULD consider the use of call redirection to manage blocked calls.

19.5.29. User Awareness and Training

19.5.29.R.01. Rationale

The introduction of VoIP and UC services will introduce change to the appearance and functionality of systems, how users access agency systems and types of user support. It is essential that users are aware of information security and privacy concepts and risks associated with the services they use.

Support provided by the VoIP and UC service provider may attract additional charges.

19.5.29.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4758]

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of VoIP and UC services (See Section 9.1 – Information Security Awareness and Training).

20. Data management

20.1. Data Transfers

Objective

20.1.1. Data transfers between systems are controlled and accountable.

Context

Scope

20.1.2. This section covers the fundamental requirements of data transfers between systems and applies equally to data transfers using removal media and to data transfers via gateways.

20.1.3. Additional requirements for data transfers using removal media can be found in the Section 13.3 – Media Usage and additional requirements for data transfers via gateways can be found in the Section 20.2 – Data Import and Export.

20.1.4. Transfers from a classified system where strong information security controls exist to a system of lower classification where controls may not be as robust, can lead to data spills, information loss and privacy breaches. It is important that appropriate levels of oversight and accountability are in place to minimise or prevent the undesirable loss or leakage of information.

PSR references

20.1.5. Relevant PSR requirements can be found at:

Reference	Title	Source

PSR Mandatory Requirements	GOV2, GOV6, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PERSEC1, PERSEC2, PERSEC3 and PERSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/personnel-security/mandatory-requirements/
PSR content protocols	Management protocol for information security Management protocol for personnel security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/personnel-security/management-protocol-for-personnel-security/
PSR requirements sections	Classify and assign protective markings Understand the information security lifecycle	https://www.protectivesecurity.govt.nz/information-security/lifecycle/understand-what-information-and-ict-systems-you-need-to-protect/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/
Managing specific scenarios	Transacting online with the public	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/transacting-online-with-the-public/

Rationale & Controls

20.1.6.   User responsibilities

20.1.6.R.01.   Rationale

When users transfer data to and from systems 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. Accordingly agencies will need to hold personnel accountable for all data transfers that they make.

20.1.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4138]

Agencies MUST establish a policy and train staff in the processes for data transfers between systems and the authorisations required before transfers can take place.

20.1.6.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4141]

Agencies MUST ensure that system users transferring data to and from a system are held accountable for the data they transfer.

20.1.7.   Data transfer processes and procedures

20.1.7.R.01.   Rationale

Personnel can assist in preventing information security incidents by checking protective markings (classifications, endorsements and releasability) checks to ensure that the destination system is appropriate for the protection of the data being transferred, performing antivirus checks on data to be transferred to and from a system, and following all processes and procedures for the transfer of data.

20.1.7.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4147]

Agencies MUST ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.

20.1.7.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4148]

Agencies SHOULD ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.

20.1.8.   Data transfer authorisation

20.1.8.R.01.   Rationale

Using a trusted source to approve transfers from a classified system to another system of a lesser classification or where a releasability endorsement is applied to the data to be transferred, ensures appropriate oversight and reporting of the activity.

20.1.8.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4151]

Agencies MUST ensure that all data transferred to a system of a lesser classification or a less secure system, is approved by a trusted source.

20.1.9.   Trusted sources

20.1.9.R.01.   Rationale

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such as the CISO and the ITSM.

20.1.9.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4156]

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

20.1.10. Import of data

20.1.10.R.01. Rationale

Scanning imported data for active or malicious content reduces the security risk of a system or network being infected, thus allowing the continued confidentiality, integrity and availability of the system or network.

20.1.10.R.02. Rationale

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 activity or usage.

20.1.10.R.03. Rationale

Personnel reporting unexpected events through the agency's incident management process provide an early opportunity to contain malware, limit damage and correct errors.

20.1.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4165]

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

20.1.10.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4168]

Agencies importing data to a system MUST implement the following controls:

- scanning for malicious and active content;
- data format checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

20.1.11. Export of highly formatted textual data

20.1.11.R.01. Rationale

When highly formatted textual data with no free text fields is to be transferred between systems, the checking requirements are lessened because the format of the information is strongly defined.

20.1.11.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4239]

When agencies export formatted textual data with no free text fields and all fields have a predefined set of permitted formats and data values, agencies MUST implement the following controls:

- protective marking checks;
- data validation and format checks;
- size limits;
- keyword checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

20.1.12. Export of other data

20.1.12.R.01. Rationale

Textual data that it is not highly formatted can be difficult to check in an automated manner. Agencies will need to implement measures to ensure that classified information is not accidentally being transferred to another system not accredited for that classification or transferred into the public domain.

20.1.12.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4245]

When agencies export data, other than highly formatted textual data, agencies MUST implement the following controls:

- protective marking checks;
- data validation and format checks;
- limitations on data types;
- size limits;
- keyword checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

20.1.13. Preventing export of NZEO data to foreign systems

20.1.13.R.01. Rationale

In order to reduce the security risk of spilling data with an endorsement onto foreign systems, it is important that procedures are developed to detect NZEO marked data and to prevent it from crossing into foreign systems or being exposed to foreign nationals.

20.1.13.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4249]

Agencies MUST:

- ensure that keyword searches are performed on all textual data;
- ensure that any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator; and

- develop procedures to prevent NZEO information in both textual and non-textual formats from being exported.

20.2. Data Import and Export

Objective

20.2.1. Data is transferred through gateways in a controlled and accountable manner.

Context

Scope

20.2.2. This section covers the specific requirements relating to the movement of data between systems via gateways. Fundamental requirements of data transfers between systems can be found in Section 20.1 – Data Transfers. These fundamental requirements apply to gateways.

Rationale & Controls

20.2.3. User responsibilities

20.2.3.R.01. Rationale

When 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 sensitive or classified data onto systems not accredited to handle the data, or the unintended introduction of malicious code to a system.   Accordingly, users need to be held accountable for all data transfers they make.

20.2.3.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4264]

Users transferring data to and from a system MUST be held accountable for the data they transfer.

20.2.4. Data Transfer authorisation

20.2.4.R.01. Rationale

Users can help prevent information security incidents by:

- checking protective markings to ensure that the destination system is appropriate for the data being transferred;
- performing antivirus checks on data to be transferred to and from a system;
- following the processes and procedures for the transfer of data.

20.2.4.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4269]

All data transferred to a system of a lesser sensitivity or classification MUST be approved by a trusted source.

20.2.5. Trusted sources

20.2.5.R.01. Rationale

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such as the CISO and the ITSM.

20.2.5.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4277]

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

20.2.6. Import of data through gateways

20.2.6.R.01. Rationale

In order to ensure the continued functioning of systems it is important to constantly analyse data being imported. Converting data from one format into another can effectively destroy most malicious active content.

20.2.6.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4280]

When agencies import data to a system through gateways, the data MUST be filtered by a product specifically designed for that purpose, including filtering malicious and active content.

20.2.6.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4281]

When agencies import data to a system through gateways, full or partial audits of the event logs MUST be performed at least monthly.

20.2.6.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:4282]

Agencies SHOULD convert data being imported at gateways into an alternative format before entering the network.

20.2.7. Export of data through gateways

20.2.7.R.01. Rationale

In order to ensure the continued integrity and confidentiality of data on an agency network, data MUST pass through a series of checks before it is exported onto systems of a lesser classification.

20.2.7.R.02. Rationale

Filtering content based on protective markings is an adequate method to protect the confidentiality of lesser classified material.

20.2.7.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4286]

Agencies SHOULD restrict the export of data to a system of a lesser classification by filtering data using at least protective marking checks.

20.2.8.   Export of highly formatted textual data through gateways

20.2.8.R.01.   Rationale

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. Risk is further reduced when there is a gateway filter that blocks (rejects) the export of data classified above the classification of the network outside of the gateway, and logs are regularly reviewed to detect if there has been unusual usage or overuse.

20.2.8.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4289]

When the export of highly formatted textual data occurs through gateways agencies MUST implement:

- checks for protective markings;
- data filtering performed by a product specifically designed for that purpose;
- data range and data type checks; and
- full or partial audits of the event logs performed at least monthly.

20.2.9.   Export of other data through gateways

20.2.9.R.01.   Rationale

Textual data which is not highly formatted can contain hidden data as well as having a higher classification due to the aggregated content. Risk is somewhat reduced by running additional automated checks on non-formatted data being exported, in addition to those checks for highly formatted textual data. Where a classification cannot be automatically determined, a human trusted source should make that determination.

20.2.9.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4292]

When agencies export data, other than highly formatted textual data, through gateways, agencies MUST implement data filtering performed by a product specifically designed for that purpose.

20.2.9.C.02.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4293]

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.

20.2.9.C.03.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:4294]

Where the classification cannot be determined automatically, a human trusted source SHOULD assess the classification of the data.

20.2.9.C.04.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:4295]

When the export of other data occurs through gateways agencies SHOULD perform audits of the complete data transfer logs at least monthly.

20.2.10. Preventing export of NZEO data to foreign systems

20.2.10.R.01.   Rationale

NZEO networks are particularly sensitive and further security measures need to be put in place when connecting them to other networks.

20.2.10.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4301]

To prevent the export of NZEO data to foreign systems, agencies MUST implement NZEO data filtering performed by a product specifically designed or configured for that purpose.

20.2.10.C.02.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4303]

Agencies MUST undertake checks of protective markings and keywords before permitting data export.

20.2.11. Requirement to sign exported data

20.2.11.R.01.   Rationale

Digitally signing data being exported, demonstrates authenticity and improves assurance that the data has not been altered in transit.

20.2.11.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4308]

A trusted source MUST sign the data to be exported if the data is to be communicated over a network to which untrusted personnel or systems have access.

20.2.11.C.02.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4309]

Agencies MUST ensure that the gateway verifies authority to release prior to the release of the data to be exported.

20.2.11.C.03.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD [CID:4310]

Agencies SHOULD use a product evaluated to at least an EAL4 assurance level for the purpose of data signing and signature confirmation.

20.3. Content Filtering

Objective

20.3.1.   The flow of data within gateways is examined and controls applied in accordance with the agency's security policy. To prevent unauthorised or malicious content crossing security domain boundaries.

Context

Scope

20.3.2. This section covers information relating to the use of content filters within bi-directional or one-way gateways in order to protect security domains.

20.3.3. Content filters reduce the risk of unauthorised or malicious content crossing a security domain boundary.

Rationale & Controls

20.3.4.   Limiting transfers by file type

20.3.4.R.01.   Rationale

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

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

Reducing the number of allowed file types reduces the number of potential vulnerabilities available for an attacker to exploit.

20.3.4.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4321]

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.

20.3.4.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4322]

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.

20.3.5.   Blocking active content

20.3.5.R.01.   Rationale

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 within the file, which increases the attack surface.

20.3.5.C.01.   Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4325]

Agencies MUST block all executables and active content from entering a security domain.

20.3.5.C.02.   Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4326]

Agencies SHOULD block all executables and active content from being communicated though gateways.

20.3.6.   Blocking suspicious data

20.3.6.R.01.   Rationale

The definition of suspicious content will depend on the system's 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 format(s).
Data range check	Checks the data within each field to ensure that it falls within the expected/permitted range.
Data type check	Inspects each file header to determine the file type.
File extension check	Checks file extensions to ensure that they are permitted.
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 endorsements.
Manual 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, multi-media or content-rich files.

20.3.6.C.01.   Control System Classification(s): All Classifications; Compliance: MUST [CID:4329]

Agencies MUST block, quarantine 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.

20.3.7.   Content validation

20.3.7.R.01.   Rationale

Content validation aims to ensure that the content received conforms to a defined, approved standard. Content validation can be an effective means of identifying malformed content, allowing agencies to block potentially malicious content. Content validation operates on a whitelisting principle, blocking all content except for that which is explicitly permitted. Examples of content validation include:

- ensuring numeric fields only contain numeric numbers;
- other fields operate with defined character sets;
- ensuring content falls within acceptable length boundaries;
- ensuring XML documents are compared to a strictly defined XML schema.

20.3.7.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4332]

Agencies MUST perform validation on all data passing through a content filter, blocking content which fails the validation.

20.3.7.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4333]

Agencies SHOULD perform validation on all data passing through a content filter, blocking content which fails the validation.

20.3.8. Content conversion and transformation

20.3.8.R.01. Rationale

Content conversion, file conversion or file transformation can be an effective method to render potentially malicious content harmless by separating the presentation format from the data. By converting a file to another format, the exploit, active content and/or payload can often be removed or disrupted enough to be ineffective.
Examples of file conversion and content transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a PDF file;
- converting a Microsoft PowerPoint presentation to a series of JPEG images;
- converting a Microsoft Excel spreadsheet to a Comma Separated Values (CSV) file; or
- converting a PDF document to a plain text file.

Some file types, such as XML, will not benefit from conversion. The conversion process should also be applied to any attachments or files contained within other files, for example, archive files or encoded files embedded in XML.

20.3.8.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4336]

Agencies SHOULD perform content conversion, file conversion or both for all ingress or egress data transiting a security domain boundary.

20.3.9. Content sanitisation

20.3.9.R.01. Rationale

Sanitisation is the process of attempting to make potentially malicious content safe to use by removing or altering active content while leaving the original content as intact as possible. Sanitisation is not as secure a method of content filtering as conversion, though many techniques may be combined. Extraneous application and protocol data, including metadata, should also be inspected and filtered where possible. Examples of sanitisation to mitigate the threat of content exploitation include:

- removal of document properties information in Microsoft Office documents;
- removal or renaming of Javascript sections from PDF files;
- removal of metadata such as EXIF information from within JPEG files.

20.3.9.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4339]

Agencies SHOULD perform content and file sanitisation on suitable file types if content conversion or file conversion is not appropriate for data transiting a security domain boundary.

20.3.10. Antivirus scans

20.3.10.R.01. Rationale

Antivirus scanning is used to prevent, detect and remove malicious software that includes computer viruses, worms, Trojans, spyware and adware.

20.3.10.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4348]

Agencies SHOULD perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines.

20.3.11. Archive and container files

20.3.11.R.01. Rationale

Archive and container files can be used to bypass content filtering processes if the content filter does not handle the file type and embedded content correctly. The content filtering process should recognise archived and container files, ensuring the embedded files they contain are subject to the same content filtering measures as un-archived files.

20.3.11.R.02. Rationale

Archive files can be constructed in a manner which can pose a denial-of-service risk due to processor, memory or disk space exhaustion. To limit the risk of such an attack, content filters can specify resource constraints/quotas while extracting these files. If these constraints are exceeded the inspection is terminated, the content blocked and a security administrator alerted.

20.3.11.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4401]

Agencies SHOULD extract the contents from archive and container files and subject the extracted files to content filter tests.

20.3.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4402]

Agencies SHOULD perform controlled inspection of archive and container files to ensure that content filter performance and availability is not

adversely affected.

20.3.11.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4403]

Agencies SHOULD block files that cannot be inspected and generate an alert or notification.

20.3.12. Whitelisting permitted content

20.3.12.R.01. Rationale

Creating and enforcing a whitelist of allowed content/files is a strong content filtering method. Allowing content that satisfies a business requirement only can reduce the attack surface of the system. As a simple example, an email content filter might allow only Microsoft Office documents and PDF files.

20.3.12.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4406]

Agencies MUST create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

20.3.12.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4407]

Agencies SHOULD create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

20.3.13. Data integrity

20.3.13.R.01. Rationale

Ensuring the authenticity and integrity of content reaching a security domain is a key component in ensuring its trustworthiness. It is also essential that content that has been authorised for release from a security domain is not modified or contains other data not authorised for release, for example by the addition or substitution of sensitive information.

20.3.13.R.02. Rationale

If content passing through a filter contains a form of integrity protection, such as a digital signature, the content filter should verify the content's integrity before allowing it through. If the content fails these integrity checks it may have been spoofed or tampered with and should be dropped or quarantined for further inspection.

Examples of data integrity checks include:

- an email server or content filter verifying an email protected by DKIM;
- a web service verifying the XML digital signature contained within a SOAP request;
- validating a file against a separately supplied hash;
- checking that data to be exported from the security domain has been digitally signed by the release authority.

20.3.13.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4411]

If data is signed, agencies MUST ensure that the signature is validated before the data is exported.

20.3.13.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4412]

Agencies SHOULD verify the integrity of content where applicable, and block the content if verification fails.

20.3.14. Encrypted data

20.3.14.R.01. Rationale

Encryption can be used to bypass content filtering if encrypted content cannot be subject to the same checks performed on unencrypted content. Agencies will need to consider the need to decrypt content, depending on:

- the security domain they are communicating with;
- whether the need-to-know principle is to be enforced;
- end-to-end encryption requirements; or
- any privacy and policy requirements.

20.3.14.R.02. Rationale

Choosing not to decrypt content poses a risk of encrypted malicious software communications and data moving between security domains. Additionally, encryption could mask the movement of information at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill.

20.3.14.R.03. Rationale

Some systems allow encrypted content through external/boundary/perimeter controls to be decrypted at a later stage, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

20.3.14.C.01. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4417]

Agencies SHOULD decrypt and inspect all encrypted content, traffic and data to allow content filtering.

20.3.15. Monitoring data import and export

20.3.15.R.01. Rationale

To ensure the continued confidentiality and integrity of systems and data, import and export processes should be monitored and audited.

20.3.15.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4420]

Agencies MUST use protective marking checks to restrict the export of data from each security domain, including through a gateway.

20.3.15.C.02. Control

When importing data to each security domain, including through a gateway, agencies MUST audit the complete data transfer logs at least monthly.

20.3.16. Exception Handling

20.3.16.R.01. Rationale

Legitimate reasons may exist for the transfer of data that may be identified as suspicious according to the criteria established for content filtering. It is important to have an accountable and auditable mechanism in place to deal with such exceptions.

20.3.16.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4424]

Agencies SHOULD create an exception handling process to deal with blocked or quarantined file types that may have a valid requirement to be transferred.

20.4. Databases

Objective

20.4.1. Database content is protected from personnel without a need-to-know.

Context

Scope

20.4.2. This section covers information relating to databases and interfaces to databases such as search engines.

Rationale & Controls

20.4.3. Data labelling

20.4.3.R.01. Rationale

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

20.4.3.C.01. Control System Classification(s): Top Secret; Compliance: MUST [CID:4434]

Agencies MUST ensure that all classified information stored within a database is associated with an appropriate protective marking if the information:

- could be exported to a different system; or
- contains differing classifications or different handling requirements.

20.4.3.C.02. Control System Classification(s): Top Secret; Compliance: MUST [CID:4435]

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

20.4.3.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4436]

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

- could be exported to a different system; or
- contains differing classifications or different handling requirements.

20.4.3.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4437]

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

20.4.4. Database files

20.4.4.R.01. Rationale

Even though a database may provide access controls to stored data, the database files themselves MUST also be protected.

20.4.4.C.01. Control System Classification(s): Top Secret; Compliance: MUST [CID:4440]

Agencies MUST protect database files from access that bypasses the database's normal access controls.

20.4.4.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4441]

Agencies SHOULD protect database files from access that bypass normal access controls.

20.4.5. Accountability

20.4.5.R.01. Rationale

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.

20.4.5.C.01. Control System Classification(s): Top Secret; Compliance: MUST [CID:4444]

Agencies MUST enable logging and auditing of system users' actions.

20.4.5.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4445]

Agencies SHOULD ensure that databases provide functionality to allow for auditing of system users' actions.

20.4.6. Search engines

20.4.6.R.01. Rationale

Even if a search engine restricts viewing of classified information that a system user does not have sufficient security clearances to access, the associated metadata can contain information above the security clearances of the system user. In such cases, restricting access to, or sanitising, this metadata effectively controls the possible release of information the system user is not cleared to view.

20.4.6.C.01. Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4448]

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.

20.4.6.C.02. Control **System Classification(s): All Classifications; Compliance: SHOULD** [CID:4449]

Agencies SHOULD ensure that system users who do not have sufficient security clearances to view database contents cannot see or interrogate associated metadata in a list of results from a search engine query.

21. Working Off-Site

21.1. Agency-owned Mobile Devices

Objective

21.1.1. Information on agency-owned mobile devices is protected from unauthorised disclosure.

Context

Scope

21.1.2. This section covers information relating to the use of agency-owned mobile devices including, but not restricted to, mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers, and other portable Internet connected devices.

21.1.3. It is important to note that product security, selection, maintenance, sanitisation and disposal requirements in Chapter 12 - Product Security also apply to agency-owned mobile devices.

Trusted Operating Environments

21.1.4. A Trusted Operating Environment (TOE) provides assurance that every reasonable effort has been made to secure the operating system of a mobile device such that it presents a managed risk to an agency's information and systems. Any residual risks are explicitly accepted by the agency.

21.1.5. Special care is necessary when dealing with All-of-Government systems or systems that affect several agencies. Security measures that can be implemented to assist in the development of a TOE include:

- strong usage policies are in place;
- unnecessary hardware, software and operating system components are removed;
- unused or undesired functionality in software and operating systems is removed or disabled;
- anti-malware and other security software is installed and regularly updated;
- downloads of software, data or documents are limited or not permitted;
- installation of unapproved applications is not permitted;
- software-based firewalls limiting inbound and outbound network connections are installed;
- patching of installed the operating system and other software is current;
- each connection is authenticated (multi-factor) before permitting access to an agency network;
- both the user and mobile device are authenticated during the authentication process;
- mobile device configurations may be validated before a connection is permitted;
- privileged access from the mobile device to the agency network is not allowed;
- access to some data may not be permitted; and
- agency control of the mobile device may supersede any convenience aspects.

Treating workstations as mobile devices

21.1.6. When an agency issues a workstation for home-based work instead of a mobile device the requirements in this section apply equally to the issued workstation.

Devices with multiple operating states

21.1.7. Some mobile devices may have functionality to allow them to operate in either an unclassified state or a classified state. In such cases the mobile devices will need to be handled according to the state that it is being operated in at the time. For example, some devices can start-up in an unclassified mode or start-up in a cryptographically protected mode.

Bluetooth and Infra-Red Devices

21.1.8. Bluetooth and Infra-Red devices, such as keyboards, headsets and mice are subject to an additional set of risks. Refer to Chapter 11 – Communication Systems and Devices.

PSR references

21.1.9. Relevant PSR requirements can be found at:

Reference	Title	Source

PSR Mandatory Requirements	GOV2, GOV4, GOV6, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/physical-security/physical-security-mandatory-requirements-2/
PSR content protocols	Management protocol for information security Management protocol for physical security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/ https://www.protectivesecurity.govt.nz/physical-security/management-protocol/
PSR requirements sections	Build security awareness Working away from the office	https://www.protectivesecurity.govt.nz/governance/build-security-awareness/ https://www.protectivesecurity.govt.nz/working-away-from-the-office/
Managing specific scenarios	Mobile and remote working Communications security	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/communications-security/

Rationale & Controls

21.1.10. Mobile devices usage policy

21.1.10.R.01. Rationale

As mobile devices routinely leave the office environment and the physical protection it affords it is important that policies are developed to ensure that they are protected in an appropriate manner when used outside of controlled agency facilities.

21.1.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4471]

Agencies MUST develop a policy governing the use of mobile devices.

21.1.10.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4472]

Agencies MUST NOT allow mobile devices to process or store TOP SECRET information unless explicitly approved by GCSB to do so.

21.1.10.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4473]

Agencies SHOULD implement a Mobile Device Management (MDM) solution.

21.1.11. Personnel awareness

21.1.11.R.01. Rationale

Mobile devices can have both a data and voice component capable of processing or communicating classified information. In such cases, personnel will need to be aware of the approved classification level for each function.

This includes Paging Services, Multi-Media Message Service (MMS) and Short Message Service (SMS) which are NOT appropriate for sensitive or classified information. Paging and message services do not appropriately encrypt information and cannot be relied upon for the communication of classified information.

21.1.11.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4476]

Agencies MUST advise personnel of the maximum permitted classifications for data and voice communications when using mobile devices.

21.1.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4477]

Agencies SHOULD NOT use Paging Services, SMS or MMS for sensitive or classified communications.

21.1.12. Non-agency owned and controlled mobile devices

21.1.12.R.01. Rationale

Agencies need to retain control of any non-agency device that contains agency or government information. Non-agency devices are discussed in Section 21.4 – BYOD.

21.1.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4480]

Agencies MUST apply the full set of BYOD controls for devices NOT directly owned and controlled by the agency. These controls are detailed in Section 21.4 – BYOD.

21.1.13. Agency owned mobile device storage encryption

21.1.13.R.01. Rationale

Encrypting the internal storage and removable media of agency owned mobile devices will reduce the risk of data loss associated with a lost or stolen device. While the use of encryption may not be suitable to treat the device as an unclassified asset it will still present a significant challenge to a malicious actor looking to gain easy access to information stored on the device. To ensure that the benefits of encryption on mobile devices are maintained, users must not store passphrases, passwords, PINS or other access codes for the encryption software on, or with, the device.

21.1.13.R.02. Rationale

Information on the use of encryption to reduce storage and physical transfer requirements is detailed in Section 17.1 – Cryptographic Fundamentals and 17.2 – Approved Cryptographic Algorithms.

21.1.13.R.03. Rationale

Refer to the PSR - Mobile and Remote working

Refer to the PSR - Handling Requirements for protectively marked information and equipment

21.1.13.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4483]

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 store or transfer the device as a classified asset in accordance with the relevant handling instructions.

21.1.13.C.02. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4484]

Users MUST NOT store passwords, passphrases, PINs or other access codes for encryption on or with the mobile device on which data will be encrypted when the device is issued for normal operations.

21.1.13.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4485]

Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption SHOULD physically store or transfer the device as a classified asset in accordance with the relevant handling instructions.

21.1.13.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4486]

Agencies SHOULD encrypt classified information on all mobile devices using an Approved Cryptographic Algorithm.

21.1.13.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4487]

Pool or shared devices SHOULD be reissued with unique passwords, passphrases, PINs or other access codes for each separate issue or deployment.

21.1.14. Mobile device communications encryption

21.1.14.R.01. Rationale

The above approach cannot be used for communicating classified information over public infrastructure, the internet or non-agency controlled networks. If appropriate encryption is not available the mobile device will not be approved for communicating classified information.

21.1.14.R.02. Rationale

Note: This applies to information and systems classified as RESTRICTED/SENSITIVE and any higher classification.

21.1.14.R.03. Rationale

Encryption does not change the classification level of the information or system itself but allows reduced handling requirements to be applied.

21.1.14.C.01. Control System Classification(s): Confidential, Secret, Top Secret, Restricted/Sensitive; Compliance: MUST [CID:4492]

Agencies MUST use encryption on mobile devices communicating over public infrastructure, the Internet or non-agency controlled networks.

21.1.14.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4493]

Agencies SHOULD use encryption for Official Information or any classified information on mobile devices communicating over public infrastructure, the Internet or non-agency controlled networks.

21.1.15. Mobile device privacy filters

21.1.15.R.01. Rationale

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 a shoulder surfing or other oversight attack or compromise.

21.1.15.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4496]

Agencies SHOULD apply privacy filters to the screens of mobile devices.

21.1.16. Disabling Bluetooth functionality

21.1.16.R.01. Rationale

As Bluetooth provides little security for the information that is passed between devices and a number of exploits have been publicised, it SHOULD NOT be used on mobile devices. Refer to Chapter 11 – Communications Systems and Devices

21.1.16.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4499]

Agencies MUST NOT enable Bluetooth functionality on mobile devices.

21.1.16.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4500]

Agencies SHOULD NOT enable Bluetooth functionality on mobile devices.

21.1.17. Configuration control

21.1.17.R.01. Rationale

Poorly controlled devices are more vulnerable to compromise and provide an attacker with a potential access point into agency systems. Although agencies may initially provide a secure device, the state of security may degrade over time. The agency will need to revaluate the security of devices regularly to ensure their integrity.

21.1.17.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4503]

Agency personnel MUST NOT disable security functions or security configurations on a mobile device once provisioned.

21.1.17.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4504]

Agencies SHOULD control the configuration of mobile devices in the same manner as devices in the agency's office environment.

21.1.17.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4505]

Agencies SHOULD prevent personnel from installing unauthorised applications on a mobile device once provisioned.

21.1.18. Maintaining mobile device security

21.1.18.R.01. Rationale

As mobile devices are not continually connected to ICT systems within an agency it is important that they are routinely returned to the agency so that patches can be applied and they can be tested to ensure that they are still secure.

Alternatively a mobile device management solution may implement policy checks and updates on connection to agency systems.

21.1.18.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4508]

Agencies SHOULD ensure that mobile devices have security updates applied on a regular basis and are tested to ensure that the mobile devices are still secure.

21.1.18.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4509]

Agencies SHOULD conduct policy checks as mobile devices connect to agency systems.

21.1.19. Connecting mobile devices to the Internet

21.1.19.R.01. Rationale

During the period that a device is connected to the Internet, without a VPN connection, it is exposed to attacks. This period needs to be minimised to reduce the security risks. Minimising this period includes ensuring that system users do not connect directly to the Internet to access the Web between VPN sessions.

21.1.19.R.02. Rationale

A split tunnel VPN can allow access to an agency's systems from another network, including unsecure networks such as the Internet. If split tunnelling is enabled there is an increased security risk that the VPN connection is susceptible to attack from such networks.

21.1.19.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4513]

Agencies MUST disable split tunnelling when using a VPN connection from a mobile device to connect to an agency network.

21.1.19.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: SHOULD NOT [CID:4514]

Agencies SHOULD NOT allow mobile devices to connect to the Internet except when temporarily connecting to facilitate the establishment of a VPN connection to an agency network.

21.1.20. Emergency destruction

21.1.20.R.01. Rationale

Where a mobile device carries classified information, or there is an increased risk of loss or compromise of the device, agencies will need to develop emergency destruction procedures. Such procedures should focus on the destruction of information on the mobile device and not necessarily the device itself. Many mobile devices used for classified information achieve this through the use of a cryptographic key zeroise or sanitisation function.

21.1.20.R.02. Rationale

Staff will need to understand the rationale and be familiar with emergency destruction procedures, especially where there is a higher probability of loss, theft or compromise.

21.1.20.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4519]

Agencies MUST develop an emergency destruction plan for mobile devices.

21.1.20.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4520]

If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a mobile device it MUST be used as part of the emergency destruction procedures.

21.1.20.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4521]

Agencies SHOULD ensure personnel are trained in emergency destruction procedures and are familiar with the emergency destruction plan.

21.1.21. Labelling

21.1.21.R.01. Rationale

Agencies may wish to affix an additional label to mobile devices asking finders of lost devices to hand it in to any New Zealand police station, or if overseas, a New Zealand embassy, consulate or high commission.

21.1.21.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4524]

Agencies SHOULD use soft labelling for mobile devices when appropriate to reduce their attractiveness value.

21.1.22. Unauthorised use of mobile devices

21.1.22.R.01. Rationale

Where mobile devices are issued to personnel for business purposes their use for private purposes should be governed by agency policy and agreed by the employee or contractor to whom the device is issued.

21.1.22.R.02. Rationale

Agencies must recognise the risks and costs associated with personal use of an agency device.

21.1.22.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4530]

Agencies SHOULD develop a policy to manage the non-business or personal use of an agency owned device.

21.1.22.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4531]

Mobile devices SHOULD NOT be used other than by personnel specifically authorised by the agency.

21.2. Working Outside the Office

Objective

21.2.1. Information on mobile devices is not accessed from public or insecure locations.

Context

Scope

21.2.2. This section covers information on accessing information using agency-owned 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 Section 21.3 – Working From Home. Further information on the use of mobile devices can be found in Section 21.1 – Agency Owned Mobile Devices.

21.2.3. Also refer to Chapter 12 - Product Security for requirements on product security, selection, maintenance, sanitisation and disposal.

Rationale & Controls

21.2.4. Working outside the office

21.2.4.R.01. Rationale

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, hotel lobbies, and coffee shops, mobile devices are **not** approved to process classified information as the security risk of classified information being overheard or observed is considered to be too high in such locations.

21.2.4.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4541]

Agencies MUST NOT allow personnel to access or communicate classified information on mobile devices outside of secure areas unless there is a reduced chance of being overheard and having the screen of the device observed.

21.2.4.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4542]

Agencies allowing personnel to access or communicate classified information outside of the office SHOULD NOT allow personnel to do so in public locations (e.g. public transport, transit lounges, hotel lobbies and coffee shops).

21.2.5. Carrying mobile devices

21.2.5.R.01. Rationale

Mobile devices used outside the office are frequently transferred 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 those devices.

21.2.5.R.02. Rationale

When agencies apply encryption to mobile devices to reduce their physical transfer requirements it is only effective when the encryption function of the device is not authenticated. 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.

21.2.5.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4546]

Agencies MUST ensure mobile devices are carried in a secured state when not being actively used, by:

- power off; or
- power on but pass code enabled.

21.2.6. Using mobile devices

21.2.6.R.01. Rationale

Mobile devices are portable in nature and can be easily stolen or misplaced. It is strongly advised that personnel do not leave mobile devices unattended at any time.

21.2.6.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4550]

When in use mobile devices MUST be kept under continual direct supervision.

21.2.7. Travelling with mobile devices

21.2.7.R.01. Rationale

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.

21.2.7.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4554]

When travelling with mobile devices and media, personnel MUST retain control over them at all times including by not placing them in checked-in luggage or leaving them unattended.

21.2.7.C.02.   Control**System Classification(s): All Classifications; Compliance: MUST** [CID:4555]

Travelling personnel requested to decrypt mobile devices for inspection or from whom mobile devices are taken out of sight by border control MUST report the potential compromise of classified information or the device to an ITSM as soon as possible.

21.3. Working From Home

Objective

21.3.1.   Personnel working from home protect classified information in the same manner as in the office environment.

Context

Scope

21.3.2.   This section covers accessing official information and agency information using mobile devices from a home environment in order to conduct home-based work. Further information on the use of mobile devices can be found in Section 21.1 – Agency Owned Mobile Devices.

The use of workstations instead of mobile devices

21.3.3.   Where an agency chooses to issue a workstation for home-based work instead of a mobile device, the requirements for mobile devices within Section 21.1 – Agency Owned Mobile Devices, equally apply to the workstation that is used.

21.3.4.   It is important to note that product security, selection, maintenance, sanitisation and disposal requirements in Chapter 12 - Product Security apply to **all** agency-owned mobile devices.

Rationale & Controls

21.3.5.   Storage requirements

21.3.5.R.01.   Rationale

All mobile devices have the potential to store classified information and therefore need protection against loss and compromise.

21.3.5.R.02.   Rationale

Refer to the PSR - Mobile and Remote working

Refer to the PSR - Handling Requirements for protectively marked information and equipment

21.3.5.C.01.   Control**System Classification(s): All Classifications; Compliance: MUST** [CID:4571]

Agencies MUST ensure that when mobile devices are not being actively used they are secured in accordance with the minimum physical security requirements as stated in the PSR.

21.3.6.   Processing requirements

21.3.6.R.01.   Rationale

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, or the provision of approved containers or secure storage units at the expense of the agency.

21.3.6.R.02.   Rationale

Refer to the PSR - Mobile and Remote working

Refer to the PSR - Handling Requirements for protectively marked information and equipment

21.3.6.C.01.   Control**System Classification(s): All Classifications; Compliance: MUST** [CID:4575]

Agencies MUST ensure that the area within which mobile devices are used meets the minimum physical security requirements as stated in the PSR.

21.4. Non-Agency Owned Devices and Bring Your Own Device (BYOD)

Objective

21.4.1.   Where an Agency permits personnel to supply their own mobile devices (such as smartphones, tablets and laptops), Official Information and agency information systems are protected to a level equivalent to an agency provided and managed office environment.

Context

Scope

21.4.2.   This section provides information on the use and security of **non-agency owned or provided** mobile devices when used for official business. This is commonly known as Bring Your Own Device (BYOD). The use of agency owned devices is described earlier in Section 21.1 – Agency Owned Mobile Devices.

21.4.3.   In the context of this section, a BYOD Network is any agency owned or provided network dedicated to BYOD. A BYOD Network is usually within an agency's premises but does NOT include networks and related services provided by commercial telecommunication or other technology providers.

21.4.4.   BYOD will introduce a wide range of risks, including information and privacy risks, to an organisation, in addition to the existing ICT risks and threats. Agencies will need to carefully examine and consider the security, privacy, governance, assurance and compliance risks and implications of BYOD.

21.4.5.   Mobile devices are a "soft" target for malware and cybercrime providing a further attack channel or vector for organisational ICT infrastructures and networks. Risks fall principally into the following categories:

- Data exfiltration and theft;
- Data tampering;

- Data loss;
- Malware;
- System outages and Denial of Service; and
- Increased incident management and recovery costs.

References

21.4.6.

Title	Publisher	Source
Risk Management of Enterprise Mobility including Bring Your Own Device	ASD	http://www.asd.gov.au/publications/csocprotect/Enterprise_Mobility_BYOD.pdf
End User Devices Security and Configuration Guidance	NCSC, UK	https://www.ncsc.gov.uk/eud-guidance
NIST 800-121 Guide to Bluetooth Security	NIST	http://www.csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf
NIST Special Publication 800-46 Revision 2 - Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
NIST Special Publication 800-114 Revision 1 User's Guide to Telework and Bring Your Own Device (BYOD) Security	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
BYOD Guidance: Device Security Considerations	GOV.UK	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf

Rationale & Controls

21.4.7. Risk Assessment

21.4.7.R.01. Rationale

Commonly termed "Bring Your Own Device" (BYOD), personal use of mobile computing in an organisational environment is widespread and personnel have become accustomed to the use of a variety of personal mobile devices. BYOD can have many advantages for an agency and for personnel. At the same time, BYOD will introduce a range of new information security risks and threats and may exacerbate existing risks.

21.4.7.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4597]

Agencies MUST undertake a risk assessment and implement appropriate controls BEFORE implementing a BYOD Policy and permitting the use of BYOD.

21.4.7.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4598]

Agencies MUST take an integrated approach to BYOD security, covering policy, training, support, systems architecture, security, systems management, change management, incident detection & management and business continuity.

21.4.8. Applicability and Usage

21.4.8.R.01. Rationale

BYOD introduces number of additional risks and attack vectors to agency systems. Not all BYOD risks can be fully mitigated with technologies available today. It is therefore important that, where feasible, all the controls specified in this section are implemented.

21.4.8.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4623]

BYOD MUST **only** be permitted for agency information systems up to and including RESTRICTED.

21.4.8.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4624]

BYOD MUST NOT be used for CONFIDENTIAL, SECRET or TOP SECRET systems.

21.4.9. Technical Controls

21.4.9.R.01. Rationale

"Jail-Breaking" and "rooting" are terms applied to devices where operating systems controls have been by-passed to allow installation of alternate operating systems or software applications that are not otherwise permitted. This is a risky practice and can create opportunities for device compromise. Users may wish to alter settings to allow the download of personal apps. This can result in security setting violations.

21.4.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4627]

Devices that have been "jail-broken", "rooted" or have settings violations MUST NOT be used for any agency business or be allowed to connect to any agency systems UNLESS this been specifically authorised.

21.4.10. BYOD Policy

21.4.10.R.01. Rationale

Technical controls fall into two categories: organisational systems and device controls. Protection for organisational systems will start with a risk assessment which guides the development of a secure architecture to support BYOD operations. Additional controls will need to be applied

to individual devices. The privacy of user data should be considered. A user policy is essential.

21.4.10.C.01. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4630]

Agencies may identify additional policy provisions and controls that are required, based on their assessment of risk. Agencies MUST implement the additional controls and protocols before implementing BYOD.

21.4.10.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4631]

Agencies MUST implement a BYOD acceptable use policy, agreed and signed by each person using a BYOD device.

21.4.10.C.03. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4632]

The agency's policy MUST clearly establish eligibility of personnel for participation in the agency BYOD scheme.

21.4.10.C.04. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4633]

Personnel MUST have written authorisation (usually managerial approval) before a connection is enabled (on-boarding).

21.4.10.C.05. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4634]

Written authorisation MUST include the nature and extent of agency access approved, considering:

- time, day of the week;
- location; and
- local or roaming access.

21.4.10.C.06. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4635]

Procedures MUST be established for removal of agency installed software and any agency data when the user no longer has a need to use BYOD, is redeployed or ceases employment (off-boarding).

21.4.10.C.07. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4637]

Standard Operating Procedures for the agency's BYOD network MUST be established.

21.4.10.C.08. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4638]

Provision MUST be made for contractors and other authorised non-employees. It is at the agency's discretion whether this activity is permitted. The risk assessment MUST reflect this factor.

21.4.10.C.09. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4639]

Ownership of data on BYOD devices MUST be clearly articulated and agreed.

21.4.10.C.10. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4643]

Agency policies MUST clearly articulate the separation between corporate support and where individuals are responsible for the maintenance and support of their own devices.

21.4.10.C.11. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4644]

Agency policies MUST clearly articulate the acceptable use of any GPS or other tracking capability.

21.4.10.C.12. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4645]

Individual responsibility for the cost of any BYOD device and its accessories MUST be agreed.

21.4.10.C.13. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4646]

Individual responsibility for replacement in the event of loss or theft MUST be agreed.

21.4.10.C.14. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4647]

Individuals MUST be responsible for the installation and maintenance of any mandated BYOD-based firewalls and anti-malware software and for implementing operating system updates and patches on their device.

21.4.10.C.15. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4648]

The procedures for purchasing and installing business related applications on the mobile devices MUST be specified and agreed.

21.4.10.C.16. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4650]

The responsibility for payment of voice and data plans and roaming charges MUST be specified and agreed.

21.4.11. BYOD Infrastructure and System Controls

21.4.11.R.01. Rationale

The use of BYOD presents increased risk and threat to agency systems. Changes to an agency's security architecture are necessary in order to minimise and manage the increased risk and threat to agency systems, information and information privacy.

21.4.11.R.02. Rationale

It is important that the principles of separation and segregation are applied to any system architecture or design to assist in the management of risk in BYOD systems.

21.4.11.R.03. Rationale

BYOD devices will seek to establish multiple connections through Wi-Fi "hot spots", Bluetooth connection and simultaneous internet and cellular connections. This behaviour creates multiple simultaneous "back channels" which can provide attack vectors for malicious activities and is considered to be high risk.

21.4.11.C.01. Control

A security architectural review MUST be undertaken by the agency before allowing BYOD devices to connect to agency systems.

21.4.11.C.02. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4656]

The BYOD network segment MUST be segregated from other elements of the agency's network.

21.4.11.C.03. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4657]

Agencies MUST architecturally separate guest and public facing networks from BYOD networks.

21.4.11.C.04. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4658]

Network configuration policies and authentication mechanisms MUST allow access to agency resources ONLY through the BYOD network segment.

21.4.11.C.05. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4659]

Access to internal resources and servers MUST be carefully managed and confined to only those services for which there is a defined and properly authorised business requirement.

21.4.11.C.06. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4660]

Wireless accesses points used for access to agency networks MUST be implemented and secured in accordance with the directions in this manual (See Section 18.2 – Wireless Local Area Networks).

21.4.11.C.07. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4661]

Bluetooth on BYOD devices MUST be disabled while within designated secure areas on agency premises.

21.4.11.C.08. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4662]

Access Controls MUST be implemented in accordance with Chapter 16 – Access Control.

21.4.11.C.09. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4663]

Agencies MUST maintain a list of permitted operating systems, including operating system version numbers, for BYOD devices.

21.4.11.C.10. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4664]

Agencies MUST check each BYOD device for malware and sanitise the device appropriately before installing agency software or operating environments.

21.4.11.C.11. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4665]

Agencies MUST check each BYOD device for malware and sanitise the device appropriately before permitting access to agency data.

21.4.11.C.12. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4666]

BYOD MUST have a Mobile Device Management (MDM) solution implemented with a minimum of the following enabled:

- The MDM is enabled to "wipe" devices of any agency data if lost or stolen;
- If the MDM cannot discriminate between agency and personal data, all data, including personal data, is deleted if the device is lost or stolen;
- The MDM is capable of remotely applying agency security configurations for BYOD devices;
- Mobile device security configurations are validated (health check) by the MDM before a device is permitted to connect to the agency's systems;
- "Jail-broken", "rooted" or settings violations MUST be detected and isolated;
- "Jail-broken" devices are NOT permitted to access agency resources;
- Access to agency resources is limited until both the device and user is fully compliant with policy and SOPs;
- Auditing and logging is enabled; and
- Changes of Subscriber Identity Module (SIM) card are monitored to allow remote blocking and wiping in the event of theft or compromise.

21.4.11.C.13. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4667]

Intrusion detection systems MUST be implemented.

21.4.11.C.14. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4668]

Continuous monitoring MUST be established to detect actual or potential security compromises or incidents from BYOD devices. Refer also to Chapter 6 - Information Security Monitoring.

21.4.11.C.15. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4669]

Agencies MUST maintain a list of approved cloud applications that may be used on BYOD devices.

21.4.11.C.16. ControlSystem Classification(s): All Classifications; Compliance: MUST [CID:4670]

Agencies MUST block the use of unapproved cloud applications for processing any agency or organisational data.

21.4.11.C.17. ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:4671]

BYOD devices MUST NOT be permitted direct connection to internal hosts, including all other devices on the local network.

21.4.11.C.18. ControlSystem Classification(s): All Classifications; Compliance: MUST NOT [CID:4672]

BYOD devices connecting to guest and public facing networks MUST NOT be permitted access to the corporate network other than through a VPN over the Internet.

21.4.11.C.19. Control

> Bluetooth on BYOD devices SHOULD be disabled while within agency premises and while accessing agency systems and data.

21.4.11.C.20. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4675]

> BYOD devices and systems SHOULD use Multi-factor (at least two-factor) authentication to connect to agency systems and prior to being permitted access to agency data.

21.4.12. Wireless IDS / IPS systems

21.4.12.R.01. Rationale

> Devices will automatically associate with the strongest signal and associated Access Point (AP). A rogue AP may belong to another organisation in an adjacent building, contractor, customer, supplier or other visitor. Association with a rogue AP can provide a means for the installation of malware.

21.4.12.R.02. Rationale

> Wireless IDS / IPS systems have the ability to detect rogue wireless AP's by channel, MAC address, frequency band and SSID. They can continuously monitor wireless networks and detect and block denial-of-service and man-in-the-middle wireless attacks. Establishing baselines of known authorised and unauthorised devices and AP's will assist in detecting and isolating any rogue devices and AP's.

21.4.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4679]

> Agencies MUST implement a wireless IDS /IPS on BYOD wireless networks.

21.4.12.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4680]

> Agencies MUST implement rogue AP and wireless "hot spot" detection and implement response procedures where detection occurs.

21.4.12.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4681]

> Agencies SHOULD conduct a baseline survey to identify:
>
> - All authorised devices and AP's; and
> - Any unauthorised devices and AP's.

21.4.13. BYOD Device Controls

21.4.13.R.01. Rationale

> Mobile devices are susceptible to loss, theft and being misplaced. These devices can be easily compromised when out of the physical control of the authorised user or owner. To protect agency systems it is important that BYOD devices are also secured and managed on an ongoing basis.

21.4.13.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4684]

> Any agency data exchanged with the mobile device MUST be encrypted in transit (See Chapter 17 – Cryptography).

21.4.13.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4685]

> Any agency data stored on the device MUST be encrypted (including keys, certificates and other essential session establishment data).

21.4.13.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4686]

> The use of virtual containers, sandboxes, wraps or similar mechanisms on the mobile device MUST be established for each authorised session for any organisational data. These mechanisms MUST be non-persistent and be removed at the end of each session.

21.4.13.C.04. Control System Classification(s): All Classifications; Compliance: MUST [CID:4687]

> Any sensitive agency data MUST be removed and securely deleted, or encrypted at the end of a session.

21.4.13.C.05. Control System Classification(s): All Classifications; Compliance: MUST [CID:4688]

> Connections to the agency network MUST be time limited to avoid leaving a session "logged on".

21.4.13.C.06. Control System Classification(s): All Classifications; Compliance: MUST [CID:4689]

> Communications between the mobile device and the agency network MUST be established through a Virtual Private Network (VPN).

21.4.13.C.07. Control System Classification(s): All Classifications; Compliance: MUST [CID:4690]

> Agencies MUST disable split-tunnelling when using a BYOD device to connect to an agency network (See Section 21.1 – Agency Owned Mobile Devices).

21.4.13.C.08. Control System Classification(s): All Classifications; Compliance: MUST [CID:4691]

> Agencies MUST disable the ability for a BYOD device to establish simultaneous connections (e.g. wireless and cellular) when connected to an agency's network.

21.4.13.C.09. Control System Classification(s): All Classifications; Compliance: MUST [CID:4692]

> The use of passwords or PINs to unlock the BYOD device MUST be enforced in addition to all other agency authentication mechanisms.

21.4.13.C.10. Control System Classification(s): All Classifications; Compliance: MUST [CID:4693]

> BYOD device passwords MUST be distinct from any agency access and authentication passwords.

21.4.13.C.11. Control System Classification(s): All Classifications; Compliance: MUST [CID:4694]

> BYOD passwords MUST be distinct from other fixed or mobile agency network passwords (See Section 16.1 – Identification and Authentication

for details on password requirements).

21.4.14. Additional Controls

21.4.14.R.01. Rationale

There are many new devices and operating system versions being frequently released. It may not be feasible or cost-effective for an agency to support all combinations of device and operating system.

21.4.14.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4697]

Agencies SHOULD compile a list of approved BYOD devices and operating systems for the guidance of staff.

21.4.14.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4698]

Agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.

21.4.14.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4699]

Agencies SHOULD consider the use of bandwidth limits as a means of controlling data downloads and uploads.

21.4.14.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4700]

Agencies SHOULD take legal advice on the provisions in their BYOD policy.

22. Enterprise systems security

22.1. Cloud Computing

Objective

22.1.1. Cloud systems risks are identified and managed and that Official Information and agency information systems are protected in accordance with Cabinet Directives, the PSR, the New Zealand Government Security Classification System, the NZISM and with other government security requirements and guidance.

Context

Terminology

22.1.2. Terminology and definitions of cloud models and services used in this section are consistent with NIST Special Publication 800-145, The NIST Definition of Cloud Computing, dated September 2011 (see table of References below).

22.1.3. A fundamental construct in the management of risk in cloud environment is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular trust Zone. Refer also to Section 22.2 – Virtualisation.

Separation and Segregation

22.1.4. Separation and Segregation is determined by system function and the sensitivity of the data the system stores, processes and transmits. One common example is placing systems that require a connection to the Internet into a demilitarized zone (DMZ) that is separated and segregated (isolated) from more sensitive systems.

22.1.5. Separation and Segregation limits the ability of an intruder to exploit a vulnerability with the intent of elevating privileges to gain access to more sensitive systems on the internal network. VLANs may be used to further separate systems by controlling access and providing segregation thus giving additional protection.

Mandates and Requirements

22.1.6. In August 2013, the Government introduced their approach to cloud computing, establishing a 'cloud first' policy and an All-of-Government direction to cloud services development and deployment. This is enabled by the Cabinet Minute [CAB Min (13) 37/6B].

22.1.7. Under the 'cloud first' policy state service agencies are expected to adopt approved cloud services either when faced with new procurements, or an upcoming contract extension decision.

22.1.8. In October 2013 the Government approved the GCIO risk and assurance framework for cloud computing, which agencies must follow when they are considering using cloud services [CAB Min (13) 37/6B]. It also directs that no data classified above RESTRICTED should be held in a *public* cloud, whether it is hosted onshore or offshore.

22.1.9. It is important to note that although agencies can outsource **responsibility** to a service provider for implementing, managing and maintaining security controls, they cannot outsource their **accountability** for ensuring their data is appropriately protected.

Background

22.1.10. The adoption of cloud technologies and services, the hosting of critical data in the cloud and the risk environment requires that agencies exercise caution. Many cloud users are driven by the need for performance, scalability, resource sharing and cost saving so a comprehensive risk assessment is essential in identifying and managing jurisdictional, sovereignty, governance, technical and security risks.

22.1.11. Typically agencies and other organisations start with a small, private cloud, allowing technical and security architectures, management processes and security controls to be developed and tested and gain some familiarity with cloud technologies and processes. These organisations then progress by using non-critical data, for example email, and other similar applications, in a hybrid, private or public cloud environment.

22.1.12. There are a number of technical risks associated with cloud computing, in addition to the existing risks inherent in organisational systems. Attention must also be paid to the strategic, governance and management risks of cloud computing. Security architecture and security controls also require careful risk assessment and consideration.

22.1.13. Cloud service providers will invariably seek to limit services, liability, compensation or penalties through carefully worded service contracts, which may present particular risks.

22.1.14. Much has been made of the operational cost savings related to cloud technologies, particularly a lower cost of operating. Less obvious are the risks and related cost of managing risk to an acceptable level. It is important to note that short term overall cost increases may, in some cases, be attributed to the adoption of cloud technologies and architectures.

22.1.15. Some valuable work in mapping the cloud risk landscape has been undertaken by such organisations as the Cloud Security Alliance, the US National Institute of Standards and Technology (NIST), the UK's Cloud Industry Forum and the European Network and Information Security Agency (ENISA). It is important to note that the extent of the risk landscape continues to evolve and expand.

Scope

22.1.16. This section provides information and some guidance on the risks associated with cloud computing, its implementation and ongoing use. Some controls are specified but agencies will necessarily undertake their own comprehensive risk assessment and select controls to manage those risks.

References - Guidance

22.1.17. While NOT an exhaustive list, further information on Cloud can be found at:

Title	Publisher	Source
Cabinet Minute of Decision – CAB Min (12) 29/8A – 'Cloud First' Policy	Cabinet Office	http://ict.govt.nz/assets/Uploads/Documents/CabMin12-cloud-computing.pdf
Cabinet Minute of Decision – CAB Min (13) 37/6B – Cloud Computing Risk and Assurance Framework	Cabinet Office	http://ict.govt.nz/assets/Cabinet-Papers/Cab-Minute-Cloud-Computing-Risk-and-Assurance-Framework-Oct-2013.pdf
All-of-Government cloud computing approach	Government Chief Information Officer	http://ict.govt.nz/programmes/government-approach
Requirements for Cloud Computing	Government Chief Information Officer	https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/
Cloud Computing: Security and Privacy Considerations	Government Chief Information Officer	https://www.digital.govt.nz/assets/Documents/1Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf
Risk Assessment Process: Information Security	Government Chief Information Officer	https://www.digital.govt.nz/dmsdocument/3~Risk-Assessment-Process-Information-Security.pdf
Government Use of Offshore Information and Communication Technologies (ICT) Service Providers – Advice on Risk Management April 2009	State Services Commission	http://ict.govt.nz/assets/ICT-System-Assurance/offshore-ICT-service-providers-april-2009.pdf
Cloud Computing a Guide to Making the Right Choices – February 2013	Office of the Privacy Commissioner (OPC)	http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-Cloud-Computing-guidance-February-2013.pdf
Cloud Computing Security Considerations	Australian Signals Directorate (ASD)	http://www.dsd.gov.au/infosec/cloudsecurity.htm
Cloud Computing Policy and Guidance	Australian Government Information Management Office (AGIMO)	http://www.finance.gov.au/agict//policy-guides-procurement/cloud
Cloud Control Matrix V3.0	Cloud Security Alliance (CSA)	https://cloudsecurityalliance.org/media/news/csa-releases-ccm-version-3/
Security Guidance for Critical Areas of Focus in Cloud Computing V3.0	CSA	http://www.cloudsecurityalliance.org/guidance
Top Threats to Cloud Computing	CSA	http://www.cloudsecurityalliance.org/topthreats.html
Governance, Risk Management and Compliance Stack	CSA	http://www.cloudsecurityalliance.org/grcstack.html
Security & Resilience in Governmental Clouds - Making an informed decision	The European Network and Information Security Agency (ENISA)	http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
Cloud Computing Information Assurance Framework	ENISA	http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework

Cloud Computing Security Risk Assessment	ENISA	http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
Critical Cloud Computing – A CIIP perspective on cloud computing services	ENISA	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport
Guidelines on Security and Privacy in Public Cloud Computing ,Special Publication 800-144	Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
Enterprise Risk Management for Cloud Computing	The Committee of Sponsoring Organizations of the Treadway Commission (COSO)	http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf
Cloud Security	Cloud Industry Forum	http://www.cloudindustryforum.org/content/cloud-security
OASIS – various reference and guidance documents	Organization for the Advancement of Structured Information Standards (OASIS)	https://www.oasis-open.org/committees/tc_cat.php?cat=cloud

References - Standards

22.1.18. Further standards can be found at:

Title	Publisher	Source
The NIST Definition of Cloud Computing , Special Publication 800-145, September 2011	NIST	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146	NIST	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
Cloud Computing Standards Roadmap, NIST Special Publication 500-291	NIST	http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
Cloud Computing Reference Architecture NIST Special Publication 500-292	NIST	http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
ISO/IEC 17788:2014 Information technology -- Cloud computing -- Overview and vocabulary	ISO / IEC	http://www.iso.org
ISO/IEC 17789:2014 Information technology -- Cloud computing -- Reference architecture	ISO / IEC	http://www.iso.org
ISO/IEC 17826:2012 Information technology -- Cloud Data Management Interface (CDMI)	ISO / IEC	http://www.iso.org
ISO/IEC CD 19086-1 Information technology -- Cloud computing -- Service level agreement (SLA) fr amework and Technology -- Part 1: Overview and concepts	ISO / IEC	http://www.iso.org
ISO/IEC NP 19086-2 Information technology -- Cloud computing -- Service level agreement (SLA) fr amework and Technology -- Part 2: Metrics	ISO / IEC	http://www.iso.org
ISO/IEC NP 19086-3 Information technology -- Cloud computing -- Service level agreement (SLA) fr amework and Technology -- Part 3: Core requirements	ISO / IEC	http://www.iso.org
ISO/IEC AWI 19941 Information Technology -- Cloud Computing -- Interoperability and Portability	ISO / IEC	http://www.iso.org
ISO/IEC AWI 19944 Information Technology - Cloud Computing - Data and their Flow across Devices and Cloud Services	ISO / IEC	http://www.iso.org
ISO/IEC DIS 27017 (In Draft) Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO / IEC	http://www.iso.org

ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	ISO / IEC	http://www.iso.org

PSR references

22.1.19. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	http://www.protectivesecurity.govt.nz https://www.protectivesecurity.govt.nz/governance/mandatory-requirements-2/ https://www.protectivesecurity.govt.nz/information-security/mandatory-requirements-2/
PSR content protocols	Management protocol for information security	https://www.protectivesecurity.govt.nz/information-security/management-protocol/
PSR requirements sections	Handling requirements for protectively marked information and equipment Supply chain security Classify and assign protective markings Assess the risks to your information security	https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/handling-requirements/ https://www.protectivesecurity.govt.nz/governance/supply-chain-security/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/understand-what-information-and-ict-systems-you-need-to-protect/classify-and-assign-protective-markings/ https://www.protectivesecurity.govt.nz/information-security/lifecycle/assess-the-risks/
Managing specific scenarios	Cloud Computing Outsourced ICT facilities Outsourcing, Offshoring and supply chains Transacting online with the public	https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/cloud-computing/ https://www.protectivesecurity.govt.nz/physical-security/specific-scenarios/physical-security-for-ict/outsourced-ict-facilities/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/outsourcing-offshoring-and-supply-chains/ https://www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/transacting-online-with-the-public/

Rationale & Controls

22.1.20. Applicability

22.1.20.R.01. Rationale

Security controls may not be available, cost effective or appropriate for all information classification levels. Much will depend on the cloud computing deployment model adopted. It is important that agencies understand when it is appropriate to use cloud services and how to select appropriate cloud services and service models, based on the classification of the information, any special handling endorsements and associated confidentiality, availability and integrity risks.

22.1.20.R.02. Rationale

Systems and information classified CONFIDENTIAL and above require higher levels of prtotection. This applies in all types of cloud models including private, community, hybrid and public cloud models and deployments.

22.1.20.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4800]

The use of cloud services and infrastructures for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET MUST be approved by the GCSB.

22.1.20.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4801]

Agencies intending to adopt cloud technologies or services MUST ensure cloud service providers apply the controls specified in this manual to any systems hosting, processing or storing agency data and systems.

22.1.20.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4802]

Agencies MUST NOT use public, hybrid (incorporating a public element), or other external cloud services for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET.

22.1.20.C.04. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4803]

Agencies MUST NOT use public or hybrid (incorporating a public element) cloud services to host, process, store or transmit NZEO endorsed information.

22.1.20.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4804]

Agencies intending to adopt cloud technologies or services SHOULD obtain formal assurance cloud service providers will apply the controls specified in this manual to any cloud service hosting, processing or storing agency data and systems.

22.1.21. Risk Assessment

22.1.21.R.01. Rationale

The adoption of cloud technologies will introduce a wide range of technology and information system risks *in addition* to the risks that already exist for agency systems. It is vital that these additional risks are identified and assessed in order to select appropriate controls and countermeasures. Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied.

22.1.21.R.02. Rationale

The **responsibility** for the implementation, management and maintenance of controls will depend on the service model and deployment model (refer to NIST SP800-145) used in the delivery of cloud services.

22.1.21.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4808]

Agencies intending to adopt cloud technologies or services MUST conduct a risk assessment *before* implementation or adoption.

22.1.21.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4809]

Agencies intending to adopt cloud technologies or services MUST determine trust boundaries *before* implementation.

22.1.21.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4810]

Agencies intending to adopt cloud technologies or services MUST determine where the responsibility (agency or cloud service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.

22.1.21.C.04. Control System Classification(s): All Classifications; Compliance: MUST [CID:4811]

Agencies MUST ensure cloud risks for any cloud service adopted are understood and formally accepted by the Agency Head or Chief Executive (or their formal delegate) and the agency's Accreditation Authority.

22.1.21.C.05. Control System Classification(s): All Classifications; Compliance: MUST [CID:4812]

Agencies MUST consult with the GCDO to ensure the strategic and other cloud risks are comprehensively assessed.

22.1.21.C.06. Control System Classification(s): All Classifications; Compliance: MUST [CID:4813]

Agencies procuring or using cloud services to be used by multiple agencies MUST ensure all interested parties formally agree the risks, controls and any residual risks of such cloud services.

22.1.21.C.07. Control System Classification(s): All Classifications; Compliance: MUST [CID:4814]

Agencies using cloud services MUST ensure they have conducted a documented risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.

22.1.22. Offshore Services

22.1.22.R.01. Rationale

Cloud services hosted offshore introduce several additional risks, in particular, jurisdictional, sovereignty and privacy risks. Foreign owned cloud service providers operating in New Zealand, are subject to New Zealand legislation and regulation. They may, however, also be subject to a foreign government's privacy, lawful access and data intercept legislation.

22.1.22.R.02. Rationale

The majority of these jurisdictional, sovereignty and privacy risks cannot be adequately managed with controls available today. They must therefore be carefully considered and accepted by the Agency Head or Chief Executive before the adoption of such cloud services.

22.1.22.R.03. Rationale

Some cloud services hosted within New Zealand may be supported by foreign based technical staff. This characteristic introduces a further risk element to the use of foreign-owned cloud service providers.

22.1.22.R.04. Rationale

Further complexity can be introduced when All-of-Government or multi-agency systems are deployed or integrated with cloud services. Any security breach can affect several agencies and compromise large or aggregated data sets.

22.1.22.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4820]

Agencies using cloud services hosted offshore MUST ensure jurisdictional, sovereignty and privacy risks are fully considered and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.

22.1.22.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4821]

Agencies using cloud services hosted offshore MUST ensure that the agency retains ownership of its information in any contract with the cloud service provider.

22.1.22.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4822]

Agencies using cloud services hosted offshore and connected to All-of-Government systems MUST ensure they have conducted a risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.

22.1.22.C.04. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4823]

Agencies MUST NOT use cloud services hosted offshore for information or systems classified CONFIDENTIAL, SECRET or TOP SECRET.

22.1.22.C.05. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4824]

Agencies MUST NOT use cloud services hosted offshore for information with an NZEO endorsement.

22.1.22.C.06. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4825]

Agencies SHOULD NOT use cloud services hosted offshore *unless*:

- privacy, information sensitivity and information value has been fully assessed by the agency;
- a comprehensive risk assessment is undertaken by the agency;
- controls to manage identified risks have been specified by the agency; and

- the cloud service provider is able to provide adequate assurance that these controls have been properly implemented *before* the agency uses the cloud service.

22.1.23. System Availability

22.1.23.R.01. Rationale

The availability of agency systems, business functionality and any customer or client online services, is subject to additional risks in an outsourced cloud environment. A risk assessment will include consideration of business requirements on availability in a cloud environment.

22.1.23.R.02. Rationale

Risks to business functionality may include service outages, such as communications, data centre power, back and other failures or interruptions. Entity failures such the merger, acquisition or liquidation of the cloud service provider may also present a significant business risk to availability.

22.1.23.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4829]

Agencies intending to adopt cloud technologies or services MUST consider the risks to the availability of systems and information in their design of cloud systems architectures and supporting controls and governance processes.

22.1.23.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4830]

Any contracts for the provision of cloud services MUST include service level, availability, recoverability and restoration provisions.

22.1.23.C.03. Control System Classification(s): All Classifications; Compliance: MUST [CID:4831]

Agencies MUST ensure contracts with cloud service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of cloud services.

22.1.24. Unauthorised Access

22.1.24.R.01. Rationale

Cloud service providers may not provide adequate physical security and physical and logical access controls to meet agencies requirements. An assessment of cloud service risks will include physical and systems security. Refer also to Chapter 19 – Gateway Security, Section 22.2 – Virtualisation and Section 22.3 – Virtual Local Area Networks.

22.1.24.R.02. Rationale

Some cloud services hosted within New Zealand may be supported by technical staff, presenting additional risk. In some cases the technical staff are based offshore. The use of encryption can provide additional assurance against unauthorised access – refer to Chapter 17 – Cryptography.

22.1.24.R.03. Rationale

Data Loss Prevention (DLP) technologies and techniques are implemented to safeguard sensitive or critical information from leaving the organisation. They operate by identifying unauthorised access and data exfiltration and take remedial action by monitoring, detecting and blocking unauthorised attempts to exfiltrate data. For DLP to be effective, all data states (processing, transmission and storage) are monitored.

22.1.24.C.01. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4836]

Agencies intending to adopt cloud technologies or services SHOULD ensure cloud service providers apply the physical, virtual and access controls specified in this manual for agency systems and data protection.

22.1.24.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4837]

Agencies intending to adopt cloud technologies or services SHOULD apply separation and access controls to protect data and systems where support is provided by offshore technical staff.

22.1.24.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4838]

Agencies intending to adopt cloud technologies or services SHOULD apply controls to detect and prevent unauthorised data transfers and multiple or large scale data transfers to offshore locations and entities.

22.1.24.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4839]

Agencies intending to adopt cloud technologies or services SHOULD consider the use of encryption for data in transit and at rest.

22.1.25. Incident Handling and Management

22.1.25.R.01. Rationale

Cloud service providers may not provide the same level of incident identification and management as provided by agencies. In some cases, these services will attract additional costs. Careful management of contracts is required to ensure agency requirements for incident detection and management are fully met when adopting cloud services.

22.1.25.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4842]

Agencies MUST include incident handling and management services in contracts with cloud service providers.

22.1.25.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4843]

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

22.1.26. Backup, Recovery Archiving and Data Remanence

22.1.26.R.01. Rationale

Cloud service providers will invariably provide some business continuity and disaster recovery plans, including system and data backup, for

their own operational purposes. These plans may not include customer data or systems. Where cloud service providers do not adequately meet agency business requirements, an agency defined backup and recovery plan may be necessary.

22.1.26.R.02.   Rationale

Residual information remaining on a device or storage media after clearing or sanitising the device or media is described as data remanence. This characteristic is sometimes also described as data persistence, although this description may include the wider implication of multiple copies.

22.1.26.R.03.   Rationale

Full consideration of risks associated with data remanence and data persistence is required to ensure agency requirements for backup, recovery, archiving and data management is included in any cloud service contract.

22.1.26.R.04.   Rationale

In addition to backups, cloud service providers may also archive data. Multi-national or foreign based cloud service providers may have established data centres in several countries. Backup and archiving is invariably automated and there may be no feasible method of determining where and in what jurisdiction the data have been archived. This can create an issue of data remanence and persistence where cloud service contracts are terminated but not all agency data can be effectively purged or deleted from the provider's systems.

22.1.26.C.01.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4849]

Agencies MUST develop and implement a backup, recovery and archiving plan and supporting procedures (See Section 6.4 – Business Continuity and Disaster Recovery).

22.1.26.C.02.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4850]

Agencies MUST include a data purge or secure delete process in any cloud service contracts.

22.1.26.C.03.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4851]

Any data purge or secure delete process in any cloud service contracts MUST be independently verifiable.

22.1.27. User Awareness and Training

22.1.27.R.01.   Rationale

The introduction of cloud services will introduce change to the appearance and functionality of systems, how users access agency systems and types of user support. It is essential that users are aware of information security and privacy concepts and risks associated with the services they use.

Support provided by the cloud service provider may attract additional charges.

22.1.27.C.01.   Control **System Classification(s): All Classifications; Compliance: MUST** [CID:4854]

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of cloud services (See Section 9.1 – Information Security Awareness and Training).

22.2. Virtualisation

Objective

22.2.1.   To identify virtualisation specific risks and apply mitigations to minimise risk and secure the virtual environment.

Context

22.2.2.   Virtualisation is the software simulation of the components of an information system and may include the simulation of hardware, operating systems, applications, infrastructure and storage. Underlying the simulation is hardware and control or simulation software, often described as a virtual machine (VM).

22.2.3.   A Hypervisor is a fundamental component of a virtual environment and provides a supervisory function and framework that enables multiple operating systems, often described as "Guest Operating Systems", to run on a single physical device.

22.2.4.   A fundamental construct in the management of risk in virtual environments is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular trust Zone. As assets are added to a Trust Zone, they inherit the security policies set for that Trust Zone.

22.2.5.   Trust Zones will also apply the Principal of Least Privilege, which requires that each element in the network is permitted to access only those other network elements that are required for the node to perform its business function.

22.2.6.   Virtualisation is radically changing how agencies and other organisations select, deploy implement and manage ICT. While offering significant benefits in efficiency, resource consolidation and utilisation of CIT assets, virtualisation can add risks to the operation of a system and the security of the data processed and managed by that system.

22.2.7.   Virtualisation adds layers of technology and can combine many, traditionally discrete and physically separate components, into a single physical system. This consolidation invariably creates greater impact if faults occur or the system is compromised. Virtual systems are designed to be dynamic and to facilitate the movement and sharing of data. This characteristic is also a prominent attack vector and can make the enforcement and maintenance of security boundaries much more complex.

22.2.8.   Virtualisation is susceptible to the same threats and vulnerabilities as traditional ICT assets but traditional security offers limited visibility of virtualised environments where the assets configurations and security postures are constantly changing. Incidents in virtualised environments can rapidly escalate across multiple services, applications and data sets, causing significant damage and making recovery complex.

Virtualisation risks

22.2.9.   Virtualisation risks can be considered in four categories:

- Risks directly related to virtualisation technologies;
- Systems architecture; implementation and management;
- The usage and business models; and
- Generic technology risks.

Mitigations

22.2.10. The controls described elsewhere in this manual deal with generic technology risks. Important steps in risk mitigation for virtual environments include:

- Identify and accurately characterise all deployed virtualisation and security measures beyond built-in hypervisor controls on VMs.
- Comparing security controls against known threats and industry standards to determine gaps and select appropriate controls.
- Identify and implement anti-malware tools, intrusion prevention and detection, active vulnerability scanning and systems security management and reporting tools.

References

22.2.11. Further references can be found at:

Title	Publisher	Source
NIST Special Publication 800-125, Guide to Security for Full Virtualisation Technologies	NIST	http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf
The Security Technical Implementation Guides,	Defense Information Systems Agency,	http://iase.disa.mil/stigs/Pages/index.aspx
Virtualization Security Checklist	ISACA	http://www.isaca.org/Knowledge-Center/Research/Documents/Virtualization-Security-Checklist-26Oct2010-Research.pdf
A Guide to Virtualization Hardening Guides	SANS	http://www.sans.org/reading_room/analysts_program/vmware-guide-may-2010.pdf
Virtual Machine Security Guidelines	The Center for Internet Security	http://benchmarks.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf
Software-Defined Networking (SDN) Definition	Open Networking Foundation	https://www.opennetworking.org/sdn-resources/sdn-definition
Network segmentation and segregation	ASD	http://www.asd.gov.au/publications/csocprotect/Network_Segmentation_Segregation.pdf

Rationale & Controls

22.2.12. Functional segregation between servers

22.2.12.R.01. Rationale

Agencies may implement segregation through the use of techniques to restrict a process to a limited portion of the file system, but this is often less effective. Virtualisation technology MUST be carefully architected to avoid cascade failures.

22.2.12.R.02. Rationale

The key element in separating security domains of differing classifications is physical separation. Current virtualisation technology cannot guarantee separation.

22.2.12.R.03. Rationale

The use of virtualisation technology within a security domain is a recognised means of efficiently architecting a system.

22.2.12.C.01. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4877]

Virtualisation technology MUST NOT be used for functional segregation between servers of different classifications.

22.2.12.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4878]

Virtualisation technology MUST NOT be used for functional segregation between servers in different security domains at the same classification.

22.2.12.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4879]

Agencies SHOULD ensure that functional segregation between servers is achieved by:

- physically, using single dedicated machines for each function; or
- using virtualisation technology to create separate virtual machines for each function within the same security domain.

22.2.12.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4880]

Virtualisation technology SHOULD NOT be used for functional segregation between servers in different security domains at the same classification.

22.2.13. Risk Management

22.2.13.R.01. Rationale

Where virtualisation technologies are to be used, risk identification, assessment and management are important in order to identify

virtualisation specific risks, threats and treatments.

22.2.13.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4883]

Agencies MUST undertake a virtualisation specific risk assessment in order to identify risks, related risk treatments and controls.

22.2.13.C.02. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4884]

Agencies SHOULD undertake a virtualisation specific risk assessment in order to identify risks and related risk treatments.

22.2.14. Systems Architecture

22.2.14.R.01. Rationale

It is important to include virtualisation specific concepts, constraints, mitigations and controls in the design of systems architectures that propose using virtualisation technologies, in order to gain maximum advantage from the use of these technologies and to ensure security of systems and data is maintained.

22.2.14.R.02. Rationale

Virtual environments enable a small number of technical specialists to cover a wide range of activities such as network, security, storage and application management. Such activities are usually undertaken as discrete activities by a number of individuals in a physical environment. To remain secure and correctly and safely share resources, VMs must be designed following the principles of separation and segregation through the establishment of trust zones.

22.2.14.R.03. Rationale

Software-defined networking (SDN) is an approach to networking in which control is decoupled from hardware and managed by a separate application described as a controller. SDNs are intended to provide flexibility by enabling network engineers and administrators to respond to rapidly changing business requirements. Separation and segregation principles also apply to SDNs.

22.2.14.R.04. Rationale

In addition to segregation of key elements, VM security can be strengthened through functional segregation. For example, the creation of separate security zones for desktops and servers with the objective of minimising intersection points.

22.2.14.R.05. Rationale

Poor control over VM deployments can lead to breaches where unauthorised communication and data exchange can take place between VMs. This can create opportunity for attackers to gain access to multiple VMs and the host system.

22.2.14.C.01. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4891]

Agencies MUST architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones or security domains.

22.2.14.C.02. ControlSystem Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4892]

Agencies MUST NOT permit the sharing of files or other operating system components between host and guest operating systems.

22.2.14.C.03. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4893]

Agencies SHOULD architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones.

22.2.14.C.04. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4894]

Agencies SHOULD design virtualised systems and environments to enable functional segregation within a security domain.

22.2.14.C.05. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4895]

Agencies SHOULD harden the host operating systems following an agency or other approved hardening guide.

22.2.14.C.06. ControlSystem Classification(s): All Classifications; Compliance: SHOULD [CID:4896]

Agencies SHOULD separate production from test or development virtual environments.

22.2.14.C.07. ControlSystem Classification(s): All Classifications; Compliance: SHOULD NOT [CID:4897]

Agencies SHOULD NOT permit the sharing of files or other operating system components between host and guest operating systems.

22.2.15. Systems Management

22.2.15.R.01. Rationale

VMs are easy to deploy, often without formal policies or controls to manage the creation, management and decommissioning of VMs. This is sometimes described as "VM sprawl", which is the unplanned proliferation of VMs. Attackers can take advantage of poorly managed and monitored resources. More deployments also mean more failure points, so VM sprawl can create operational difficulties even if no malicious activity is involved.

22.2.15.R.02. Rationale

A related difficulty occurs with **unsecured VM migration** when a VM is migrated to a new host, and security policies and configuration are not updated. VMs may also be migrated to other physical servers with little or no indication to users that a migration has occurred. Unsecured migration can introduce vulnerabilities through poor configuration and incomplete security and operational monitoring.

22.2.15.R.03. Rationale

Denial of service attacks can be designed specifically to exploit virtual environments. These attacks range from traffic flooding to the exploit of the virtual environment host's own resources.

22.2.15.R.04. Rationale

The ability to monitor VM backbone network traffic is vital to maintain security and operations. Conventional methods for monitoring network traffic are generally not effective because the traffic is largely contained and controlled within the virtual environment. Careful selection and implementation of hypervisors will ensure effective monitoring tools are enabled, tested and monitored.

22.2.15.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4903]

Agencies MUST ensure a VM migration policy and related SOPs are implemented.

22.2.15.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4904]

Agencies MUST implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.

22.2.15.C.03. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4905]

Agencies MUST implement controls to safely decommission VMs when no longer required, including elimination of images, snapshots, storage, backup, archives and any other residual data.

22.2.15.C.04. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4906]

Agencies SHOULD ensure a VM migration policy and related SOPs are implemented.

22.2.15.C.05. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4907]

Agencies SHOULD implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.

22.2.15.C.06. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4908]

Agencies SHOULD implement controls to safely decommission VMs when no longer required.

22.2.15.C.07. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4909]

Agencies SHOULD implement security and operational management and monitoring tools which include the following minimum capabilities:

- Identify VMs when initiated;
- Validate integrity of files prior to installation;
- Scan new VMs for vulnerabilities and misconfigurations;
- Load only minimum operating system components and services;
- Set resource usage limits;
- Establish connections to peripherals only as required;
- Ensure host and guest time synchronisation;
- Detect snapshot rollbacks and scans after restores;
- Track asset migration; and
- Monitor the security posture of migrated assets.

22.2.16. Authentication and Access

22.2.16.R.01. Rationale

VM sprawl can compromise authentication and access procedures, identity management, and system logging. This can be complicated with the use of customer-facing interfaces, such as websites.

22.2.16.R.02. Rationale

Host and guest interactions and their system vulnerabilities can magnify virtual system vulnerabilities. The co-hosting and multi-tenancy nature of virtual systems and the existence of multiple data sets can make a serious attack on a virtual environment particularly damaging.

22.2.16.R.03. Rationale

A guest OS can avoid or ignore its VM encapsulation to interact directly with the hypervisor either as a direct attack or through poor design, configuration and control. This can give the attacker access to all VMs in the virtual environment and potentially, the host machine. Described as a "VM escape", it is considered to be one of the most serious threats to virtual systems.

22.2.16.R.04. Rationale

Hyperjacking is a form of attack that takes direct control of the hypervisor in order to gain access to the hosted VMs and data. This attack typically requires direct access to the hypervisor. While technically challenging, hyperjacking is considered a real-world threat.

22.2.16.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4915]

Agencies MUST maintain strong physical security and physical access controls.

22.2.16.C.02. Control System Classification(s): All Classifications; Compliance: MUST [CID:4916]

Agencies MUST maintain strong authentication and access controls.

22.2.16.C.03. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4917]

Agencies SHOULD maintain strong data validation checks.

22.3. Virtual Local Area Networks

Objective

22.3.1. Virtual local area networks (VLANs) are deployed in a secure manner that does not compromise the security of information and systems.

Scope

22.3.2. This section covers information relating to the use of VLANs within agency networks.

Multiprotocol Label Switching

22.3.3. For the purposes of this section Multiprotocol Label Switching (MPLS) is considered to be equivalent to VLANs and is subject to the same controls.

Exceptions for connectivity

22.3.4. A single network, managed in accordance with a single SecPlan, for which some functional separation is needed for administrative or similar reasons, can use VLANs to achieve that functional separation.

22.3.5. VLANs can also be used to separate VTC and IPT traffic from data traffic at the same classification (See Section 18.3 – Video and Telephony Conferencing and Internet Protocol Telephony).

Software Defined Networking (SDN)

22.3.6. Software-defined networking (SDN) is an approach to networking in which control is decoupled from hardware and managed by a separate application described as a controller. SDNs are intended to provide flexibility by enabling network engineers and administrators to respond to rapidly changing business requirements.

22.3.7. Separation and Segregation principles also apply to SDNs. Refer to Section 22.2 – Virtualisation.

References

22.3.8. Further references can be found at:

Title	Publisher	Source
IEEE 802.1Q-2011 IEEE Standard for Local and Metropolitan area networks – Media Access Control (MAC) Bridges, and Virtual Bridged Local Area Networks.	Institute of Electrical and Electronics Engineers (IEEE)	http://standards.ieee.org
Inter-Switch Link and IEEE 802.1Q Frame Format	CISCO	http://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html
Dynamic Trunking Protocol (DTP)	CISCO	http://www.cisco.com/c/en/us/tech/lan-switching/dynamic-trunking-protocol-dtp/index.html

Rationale & Controls

22.3.9. Using VLANs

22.3.9.R.01. Rationale

Limiting the sharing of a common (physical or virtual) switch between VLANs of differing classifications reduces the chance of data leaks that could occur due to VLAN vulnerabilities. Furthermore, disabling trunking on physical switches that carry VLANs of differing security domains will reduce the risk of data leakage across the VLANs. The principles of separation and segregation must be applied to all network designs and architectures.

22.3.9.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4942]

The principles of separation and segregation MUST be applied to the design and architecture of VLANs.

22.3.9.C.02. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST NOT [CID:4943]

Agencies MUST NOT use VLANs between classified networks and any other network of a lower classification.

22.3.9.C.03. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4944]

Agencies MUST NOT use VLANs between any classified network and any unclassified network.

22.3.9.C.04. Control System Classification(s): All Classifications; Compliance: MUST NOT [CID:4945]

VLAN trunking MUST NOT be used on switches managing VLANs of differing security domains.

22.3.10. Configuration and administration

22.3.10.R.01. Rationale

When administrative access is limited to originating from the highest classified network on a switch, the security risk of a data spill is reduced.

22.3.10.C.01. Control System Classification(s): All Classifications; Compliance: MUST [CID:4948]

Administrative access MUST be permitted only from the most trusted network.

22.3.11. Disabling unused ports

22.3.11.R.01. Rationale

Disabling unused ports on a switch will reduce the opportunity for direct or indirect attacks on systems.

22.3.11.C.01. Control System Classification(s): Confidential, Secret, Top Secret; Compliance: MUST [CID:4951]

Unused ports on the switches MUST be disabled.

22.3.11.C.02. Control System Classification(s): All Classifications; Compliance: SHOULD [CID:4952]

Unused ports on the switches SHOULD be disabled.

23. Supporting Information

23.1. Glossary of Abbreviations

Glossary of Abbreviations

23.1.1.

Abbreviation	Meaning
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AH	Authentication Header
AISEP	Australasian Information Security Evaluation Program
AoG	All-of-Government
AS	Australian Standard
ASD	Australian Signals Directorate
BYOD	Bring Your Own Device
BYOK	Bring Your Own Keys
CC	Common Criteria
CCI	Controlled Cryptographic Item
CCRA	Common Criteria Recognition Arrangement
CDS	Cross-Domain Solution
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COMSEC	Communications Security
CSO	Chief Security Officer
DdoS	Distributed Denial-Of-Service
DH	Diffie-Hellman
DIS	Draft International Standard
DKIM	Domainkeys Identified Mail
DoS	Denial-Of-Service
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
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
FPGA	Field Programmable Gate Array
FTL	Flash Transition Layer
GCDO	NZ Government Chief Digital Officer
GCSB	Government Communications Security Bureau
GPU	Graphics Processing Unit
HA	High Availability
HACE	High Assurance Cryptographic Equipment
HB	Handbook
HGCE	High Grade Cryptographic Equipment. Terminology superseded by HACE.
HGCP	High Grade Cryptographic Products. Terminology superseded by HACE.
HMAC	Hashed Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HYOK	Hold Your Own Keys
ICT	Information And Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute Of Electrical And Electronics Engineers
IETF	International Engineering Task Force
IKE	Internet Key Exchange
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IODEF	Incident Object Description Exchange Format
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Infra-Red
IRC	Internet Relay Chat
IPT	Internet Protocol Telephony
IRP	Incident Response Plan
ISAKMP	Internet Security Association Key Management Protocol
ISO	International Organization For Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITSM	Information Technology Security Manager
IWF	Inter-Working Function
KMP	Key Management Plan

MDM	Mobile Device Manager
MFA	Multi-Factor Authentication
MFD	Multifunction Device
MMS	Multimedia Message Service
MSL	(New Zealand) Measurement Standards Laboratory
NAND	Flash Memory Named After The NAND Logic Gate
NAND	NOT AND – A Binary Logic Operation
NDPP	Network Device Protection Profile
NIST	National Institute Of Standards And Technology
NOR	Flash Memory Named After The NOR Logic Gate
NOR	NOT OR – A Binary Logic Operation
NTP	Network Time Protocol
NZCSI	New Zealand Communications-Electronic Security Instruction
NZCSS	New Zealand Communications Security Standard
NZ e-GIF	New Zealand E-Government Interoperability Framework
NZEO	New Zealand Eyes Only
NZISM	New Zealand Information Security Manual
NZS	New Zealand Standard
OTP	One-Time Password
PAM	Privileged Access Management
PBX	Private Branch Exchange
PED	Portable Electronic Device
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
PSR	Protective Security Requirements
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAM	Random Access Memory
RF	Radio Frequency
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SCEC	Security Construction And Equipment Committee
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDN	Software Defined Networking
SecPlan	System Security Plan

SecPol	System Security Policy
SitePlan	System Site Plan
SHA	Secure Hashing Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
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
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation (in Common Criteria)
TOE	Trusted Operating Environment
UC	Unified Communication
UTC	Co-ordinated Universal Time
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

23.2. Glossary of Terms

Glossary of Terms

23.2.1.

Term	Meaning
802.11	The Institute of Electrical and Electronics Engineers standard defining WLAN communications. Formally titled IEEE 82.11.
Access Gateway	An architectural construct that provides the system user access to multiple security domains from a single device, typically a workstation.
Accountable	Required or expected to justify actions or decisions; being answerable and responsible for those actions & decisions.

Accountable Material	Accountable information, an accountable item or accountable material refers to the accountability controls applied to specified information, equipment or materials. Accountable information, items or materials are usually uniquely identifiable (usually a serial or identification number) and are tracked from acquisition or creation to final disposal. Safe custody is a fundamental and is achieved through:
	
	    • is easily to compute;
	    • will usually output a significantly different value, even for small changes made to the input; and
	    • can detect many types of data corruptions.
	    • allocation to a specific individual (issued or responsibility designated);
	    • allocation or designation of responsibility may also require a specific briefing related to the handling, care and protection of particular types of classified information and COMSEC equipment;
	    • the allocation, issue or designation being recorded;
	    • strict controls over access and movement (special handling requirements);
	    • maintenance of a register (manual or electronic); and
	    • regular audits to ensure accountability conditions continue to be adhered to and any briefings are current.
	
	As a general rule, accountable information, items or materials are afforded physical security protection by specifying special handling and accountability conditions. Examples may include cryptographic or COMSEC equipment, other high value equipment, money, computers or information subject to privacy legislation and regulation. Cryptographic or COMSEC equipment and any information classified as CONFIDENTIAL, SECRET or TOP SECRET is accountable by definition.

Accountability	Most contemporary definitions include two key elements:
	
	    • the conferring of responsibility and authority; and
	    • the answering for the use of that authority.
	
	Accountability exists when the performance of tasks or functions by an individual or organisation, are subject to another's oversight, direction or request that they provide information or justification for their actions. Answering for the use of authority means reporting, explaining actions, assuming obligations, and submitting to outside or external judgement. Having responsibility means having the authority to act, the power to control and the freedom to decide. It also means that one must behave rationally, reliably and consistently in exercising judgement.

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 and issues a formal approval to operate the system.
Accreditation Authority	The authoritative body or individual responsible for systems accreditation.
Adaptive Authentication	This varies the level or degree of authentication required where unusual login requests occur. For example, out of normal hours, from an unusual geolocation, from an unknown device and so on. When an unusual authentication request is received, Adaptive Authentication may request additional credentials such as a one-time code provided to a known mobile phone number.
Agency	New Zealand Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the Public Service Act.
Agency Control	This description applies where an Agency has of agency information systems **direct control** and data. It follows that Non-Agency Control occurs where direct control is impaired or does not or cannot exist.
Agency Head	The government employee with ultimate responsibility for the secure operation of agency functions, whether performed inhouse or outsourced.
All-of-Government	Refers to the entire New Zealand state sector.
Application Whitelisting	An approach in which all executables and applications are prevented from executing by default, unless explicitly permitted.

Asset	Anything of value to an agency, such as IT equipment and software, information, personnel, documentation, reputation and public confidence.
Attack Surface	The IT 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	A structured process of examination, review, assessment, testing and reporting against defined requirements or objectives. Auditors should be independent of any IT system, business process, agency, function, site, supplier or other subject area being audited.
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 ASD, which is responsible for the overall operation of the program.
Authentication	The process of identifying an individual, device or system before granting access to system resources or data. Usually based on a set of credentials such as an identifier (such as a user or device name) and an authenticator (such as a password or some other authentication factor). **Authentication** is distinct from **Authorisation.**
Authentication Header	Part of the protocol used for authentication within IPSec, it provides authentication, integrity and anti-replay for the entire packet (both the header and data payload).
Authorisation	**Authorisation** is the process of granting (or revoking) access privileges to an individual, device or system.
Baseline	Information and controls that are used as a minimum implementation or starting point to provide a consistent minimum standard of systems security and information assurance.
Blacklist	A set of items to be excluded, blocked or prevented from execution. A Blacklist can also be known as a Deny List or Block List. It is the opposite of a Whitelist (Allow List) which confirms that items are acceptable.
Brute Force Attack	A brute force attack is when an automated continuous attack is conducted against a system or file to decrypt or discover passwords and data. Often used as an entry point for privilege escalation.
Cascaded Connections	Links to other systems that occur when connected systems are themselves connected to other systems. This may result in multiple indirect (cascaded) connections to systems with differing security implementations, data, equipment and other aspects important for the security and assurance of systems.
Caveat	A marking that indicates that the information has special requirements in addition to those indicated by the classification and any prescribed endorsement. The term covers codewords, source codewords, releasability indicators and special-handling caveats. See also Endorsements.
Certification	The process by which the controls and management of an information system is formally evaluated against any specific risks identified and the requirements of the NZISM. A key output is a formal assurance statement that the system conforms to the requirements of the NZISM.
Certification Authority	An official with the authority to assert that a system complies with prescribed controls within 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.
Characterisation	In the NZISM "characterisation" is a synonym for "unique identifier". This is typically applied to an operating system, programme, library or other programmatic element in the form of a checksum which can be calculated from a "known good" component and stored for comparison should there be any concern that components have been damaged or compromised. Forensic methods may also provide characterisation indicators but are likely to require additional levels of expertise. See also **Checksum** and **Hash.**

Checksum	A checksum verifies or **checks** the integrity of data.
	A good checksum algorithm:
	
	    • is easily to compute;
	    • will usually output a significantly different value, even for small changes made to the input; and
	    • can detect many types of data corruptions.
	
	Checksums are often used to verify the integrity of operating system, programme, library or other programmatic elements, images and firmware updates. Checksums typically range in length from one to 64-bits, depending on the intended usage and algorithm used to determine the checksum.
	Checksums are related to hash functions, fingerprints, randomisation functions, and cryptographic hash functions. Note, however, each of those concepts are distinct, have different applications and therefore different design goals. Check digits and parity bits are special uses of checksums. It is important to recognise that, although related, a hash is not a checksum. See also **Hash.**

Chief Information Security Officer	A senior executive with overall responsibility for the governance and management of information risks within an agency. This may include coordination between security, ICT and business functions to ensure risks are properly identified and managed.
Classified Information	Government information that requires protection from unauthorised disclosure.
Classified Systems	Systems that process, store or communicate classified information.
Codewords	A short (usually a single word) descriptions of a project, operation or activity, typically assigned used for reasons of reliability, clarity, brevity, or secrecy. Each code word is assembled in accordance with the specific rules of the code and assigned a unique meaning. Synonymous with *Codename*.
Coercivity	A measure of the resistance of a magnetic material to changes in magnetisation, equivalent to the field intensity necessary to demagnetise any magnetised material. The amount of coercive force required to reduce any residual magnetic induction to zero. Normally used in describing the characteristics of degaussing magnetic media (see Degausser).
Common Criteria	A formal, internationally-recognised scheme, defined in the ISO 15408 standard. This standard describes process to specify, design, develop, test, evaluate and certify as secure IT systems, where 'secure' is explicitly and formally defined.
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	Controls applied taken to deny unauthorised access to information derived from information and communication systems and to ensure the authenticity of related communications and data.
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.
ConOp	Concept of Operations, a document describing the characteristics of an information systems and its intended use. It is used to communicate the intent and system characteristics to all stakeholders
Consumer Guide	Product specific advice concerning evaluated products can consist of findings from mutually recognised information security evaluations. This may include the Common Criteria, findings from GCSB internal evaluations, any recommendations for use and references to relevant policy and other standards.
Content Filtering	The process of monitoring communications, including email and web pages, analysing them for any suspicious or unwanted content, and preventing the delivery of suspicious or unwanted content.
Contract	Contract means an agreement between two or more persons or entities, which is intended to be enforceable at law and includes a contract made by deed or in writing,

Cross-Domain Solution	A Cross-Domain Solution (CDS) is a controlled interface that enables secure manual and/or automatic access and/or information transfer between different security domains while protecting the confidentiality, integrity and availability of each domain. There are several types of CDS including access, multi-level and transfer gateways.
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.
Cryptoperiod	The useful life of the cryptographic key.
Cryptographic Protocol	Specified cryptographic algorithms, parameters (such as key length) and processes for managing, establishing and using encrypted communications.
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, cryptographic key, equipment, devices, documents, firmware or software that contains or describes cryptographic logic.
Data At Rest	Information residing on media storage facility or a system that is not in use.
Data Diode	A device that allows data to flow in only one direction.
Data In Transit	Information that is being conveyed across a communication medium.
Data In Use	Information that has been decrypted for processing by a system.
Data Remanence	Residual information remaining on a device or storage media after clearing or sanitising the device or media. Sometimes described as data persistence.
Data Spill	An information 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. Subsequently an administrative decision can be made to formally authorise its release into the public domain.
Degausser	An electrical device or permanent magnet assembly which generates a coercive magnetic force to destroy magnetic storage patterns in order to sanitise magnetic media.
Delegate	A person or group of personnel who may authorise noncompliance with requirements in this manual on the specific authority of the agency head.
Demilitarised Zone	A small network with one or more servers that is kept separate from an agency's core network, either on the outside of the agency's firewall, or as a separate network protected by the agency's firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet.
Department	Term used to describe Public Service Departments and Non-Public Service Departments within the state sector. Refer State Services Commission list of Central Government Agencies – http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf
Device Access Control Software	Software that can be installed to restrict access to communications ports such as USB, Serial HDMI and Ethernet Ports. 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.

Direct Control	In relation to the NZISM, is the immediate and continuous physical and **Direct Control** logical control, responsibility for and operation of agency information systems and data.
Dual-Stack Device	A product that implements both IP version 4 and 6 protocol stacks.
Emanation Security	The counter-measures, techniques and processes 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 within IPSec.

Endorsement	Certain information may bear an endorsement marking in addition to a security classification. Endorsement markings are not security classifications in their own right and must not appear without a security classification. Endorsement markings are warnings that the information has special requirements in addition to those indicated by the security classification and should only be used when there is a clear need for special care. Endorsement markings may indicate:
	    • the specific nature of information;
	    • temporary sensitivities;
	    • limitations on availability; or
	    • how recipients should handle or disclose information.

Escort	An individual who supervises visitors to secure areas to ensure uncleared visitors are not exposed to classified information, conversations equipment and other classified materials. Such visitors may include maintenance staff, IT contractors and building inspectors.
Evaluation Assurance Level	A numeric representation of the security functionality of a product gained from undertaking a Common Criteria evaluation. Each EAL comprises a number of assurance components, covering aspects of a product's design, development and operation. The range covers EAL0 (lowest) to EAL7 (highest).
Exception	The formal acknowledgement that a requirement of the NZISM cannot be met and that a dispensation from the particular compliance requirement is granted by the Accreditation Authority. This exception is valid for the term of the Accreditation Certificate or some lesser time as determined by the Accreditation Authority.
Exceptions and Waivers	An exception is NOT the same as a waiver. An exception means that the requirement need not be followed. A waiver means that some alternative controls or conditions are implemented.
Facility	An area that facilitates government business. For example, a facility can be a building, a floor of a building or a designated area on the floor of a building.
Filter	A device that manages or restricts 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 cable that connects IT equipment to the fixed infrastructure of the facility. For example, the cable that connects a workstation to a network wall socket.
Foreign National	A person who is not a New Zealand citizen.
Foreign System	A system that is not owned and operated by the New Zealand Government.
Functional Segregation	Segregation based on the device function or intended function.

Gateway	Connections between two or more systems from different security domains to allow access to or transfer of information according to defined security policies. Some gateways can be automated through a combination of physical or software mechanisms. Gateways are typically grouped into three categories: access gateways, multilevel gateways and transfer gateways.
General User	A system user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security.
Government Chief Information Officer	Government Chief Information Officer (GCIO) is a role undertaken by the Chief Executive of the Department of Internal Affairs in order to provide leadership on ICT matters within the NZ Government.
Hardware	A generic term for any physical component of information and communication technology, including peripheral equipment and media used to process information.
Hardware Security Module	Hardware Security Modules (HSMs) are a device, card or appliance usually installed inside of a PC or server to provide cryptographic functions. HSM's are usually physically and electronically hardened to reduce the possibility of tampering or other interference.
Hash	A hash is the result of a one-way, cryptographic function that converts a data string of any length into a unique fixed-length bit string. Typically applied to passwords and messages to protect against loss and/or add resistance to attacks. Hashing algorithms or functions are often are designed as a one-way cryptographic transformation so that it's impossible to reverse the hash process and reconstitute the original string. The values returned by a hash function are variously described as hash values, hash codes, digests, or simply hashes. One common use of a hash is a data structure called a hash table, widely used in computer software for indexing and rapid retrieval of database elements. Note that a hash is not the same as data encryption although it does utilise cryptographic functions. See also Checksum.
Hash Value	See Hash. Also known as "message digest".
Hashed Message Authentication Code Algorithms	In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) using a cryptographic hash function and a cryptographic key.
High Assurance	High Assurance is a generic term encompassing Common Criteria Evaluation Assurance Levels (EAL) 5, 6 and 7. Alternatively refers to the independent (unrelated) ASD High Assurance Evaluation Scheme.
High Assurance Cryptography	The U.S. ranks cryptographic products and algorithms through a certification programme and categorising the products and algorithms into product types. Product types are defined in the US National Information Assurance Glossary (CNSSI No. 4009) which defines Type 1 and 2 products, and Type 3 and 4 algorithms. Type 1 products are used to protect systems requiring the most stringent protection mechanisms.
High Assurance Cryptographic Equipment (HACE)	The equivalent to United States Type 1 cryptographic products & equipment. Previously described as High Grade Cryptographic Products & Equipment, the term HACE includes classified CCI, and other GCSB-Specific devices.
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 information security incidents as defined by the individual agency.
Identity and Access Management	**Identity and Access Management (IAM)** is a framework of business processes, policies and technologies that enable and support the management of electronic or digital identities, authorisation, privileges and access to organisational resources. **Identity management** deals with attributes related to a user (including people, machines, devices and systems). **Access Management** applies organisation processes, policies and security to enable and manage access. The two aspects are highly interdependent and are most effectively managed conjointly. An IAM framework is a key element in Privileged Access Management (PAM) and Zero Trust architectures.

Image persistence / Image retention	LCD/LED/OLED and plasma technologies can be susceptible to persistence or retention of an image or "ghost" image on the screen. This can also led to screen burn-in, as can occur in traditional CRT monitors.
Information	Any communication or representation of knowledge such as facts, data, and opinions in any medium or form, electronic as well as physical. Information includes any text, numerical, graphic, cartographic, narrative, or any audio or visual representation.
Information Asset	Information asset is any information or related equipment has value to an organisation. This includes equipment, facilities, patents, intellectual property, software and hardware. Information Assets also include services, information, and people, and characteristics such as reputation, brand, image, skills, capability and knowledge
Information and Communications Technology (ICT)	Information and Communications Technology (ICT) includes: • Information management; • Technology infrastructure; and • Technology-enabled business processes and services
Information Security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or any other means.
Information 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 or by any other process or system and processes.
Information Security Policy	A high-level document that describes how an agency protects its information. The CSP is normally developed to cover all systems and can exist as a single document or as a set of related documents.
Information Technology Security Manager	ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. The main responsibility of ITSMs is the administrative controls relating to information security within the agency.
Infrared Device	A device such as a mouse, keyboard, pointing device, laptop and smart phone that have an infrared communications capability.
Internet Key Exchange Extended Authentication	Used to provide 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.
Intrusion Detection System	An automated system used to identify an infringement of security policy from an internal or external source.
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.
IP Security	A suite of protocols for secure IP communications through authentication or encryption of IP packets including protocols for cryptographic key establishment.
IP Telephony	The management and transport of voice communications over IP networks. Also described as Voice Over IP (VOIP).
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.
ISAKMP Aggressive Mode	An IPSec protocol that uses a reduced Exchange to establish an IPSec connection. Connection negotiation is quicker but potentially less secure.
ISAKMP Main Mode	An IPSec protocol that offers improved security using additional negotiation to establish an IPSec connection.
ISAKMP Quick Mode	An IPSec protocol that is used for refreshing security association information. Similar to aggressive mode

Isolation	Includes disconnection from other systems and any external connections. In some cases system isolation may not be possible for architectural or operational reasons. Isolation may also include the quarantine of suspected or known malware and unwanted content.
IT Equipment	Any equipment to support the acquisition, processing and storage of information. This may include servers, routers, switches, switch panels, UPSs, PCs, laptops printers, MFDs etc.
Key Management	The 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	Describes how cryptographic services are securely deployed within an agency. It documents critical key management controls to protect keys and associated material during their life cycle, along with other controls to provide confidentiality, integrity and availability of keys.
Key Stretching	A defence against brute force and similar system attacks by increasing the time required to complete hashing and making an attack more time-consuming.
Limited Higher Access	The process of granting a system user access to a system that they do not hold appropriate security clearances for, for a limited 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 records system events and associated details, the transmission (if necessary) of these records (logs) and how they are stored and secured.
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. More usually as Malware
Malicious Code Infection	An information security incident that occurs when malicious code is used to infect a system. Examples of malicious code infection viruses, worms and Trojans.
Malware	Mal icious Soft or Malicious Code. ware
Management Traffic	Communications generated by system administrators and processes over a network in order to manage and control a device.
Mandatory Controls	Controls within this manual with either a 'MUST' or a 'MUST NOT' compliance requirement.
Media	A generic term for any type of hardware or material that is capable of storing or retaining data. The following examples, while not a definitive list, includes any type of "floppy disk", tapes, all types of optical disks, HDD, SSD, USB, RAM, Flash, ROM, EPROM, printer cartridges, printer drums and so on.
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, or disposing of when no longer required, in a secure manner that ensures that no data can be recovered from the media
Media Sanitisation	The process of securely erasing or overwriting data stored on media.
Multi-Factor Authentication	Multi-Factor Authentication (MFA) is a security system that verifies a user's identity by requiring multiple credentials, which may be of the same factor or type. Initial authentication normally requires a username and password. MFA requires other—additional—credentials, for example as a code from the user's smartphone, the answer to a security question, a fingerprint, or facial recognition.

Multifunction Devices	The class of devices that combines printing, scanning, copying, faxing or voice messaging functionality within the one piece of equipment. These are often designed to connect to computer and communications 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 domain.
Need-To-Know	The principle of telling a person only the information that they require to fulfil their role.
Network Access Control	Policies and processes 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 category of network device used specifically to protect a network. For example, a firewall, session border controller etc.
NZ Eyes Only	A caveat indicating that the information is not to be passed to or accessed by foreign nationals.
NZ Government Information Security Manual	National security policy that aims to provide a common approach to ensure that the implementation of information security reduces both agency specific, and whole of government, information security risks to an acceptable level.
NZ Government Protective Security Manual	The PSM was superseded by the Protective Security Requirements (PSR) in December 2014.
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-Agency Control	This description applies where an Agency does NOT haveof elements of **direct control** agency information systems and data. This may occur, for example, where data centre operations are outsourced.
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. May not be effective on smart phones / cell phones.
Official Information	Any information held by a government department or agency. See the Official Information Act 1982 (as amended).
OpenPGP	An open-source implementation of Pretty Good Privacy (PGP), a widely available cryptographic toolkit.
Oversight	The term is used in this document in the following ways: 1. In the context of governance where the term is used to describe the responsibility and requirement to manage, govern, inspect or direct activities to ensure particular outcomes, e.g. the oversight of supply contracts. 2. In the physical security context to describe the ability to observe activity (surveillance) and/or read materials which should be protected and shared only under strict guidelines. It enables the systematic observation of places and people by visual, audio, electronic, photographic or other means. Typically this is caused by poor placing of computer screens and desks and proximity to windows, doors, corridors or other means of physical access and overview or oversight. Other physical factors may contribute.

Patch Cable	A metallic (usually copper) or fibre optic cable used for routing signals between two components in an enclosed container or rack or between adjacent containers or racks.
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.
Principles of Separation and Segregation	Systems architecture and design incorporating separation and segregation in order to establish trust zones, define security domains and enforce boundaries.
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.
Private Network	A private network is a network and infrastructure owned, managed and controlled by a single entity for its exclusive use. This term includes networks used by private organisations, nongovernment organisations, state owned enterprises, or government department, agencies and ministries. If any part of the transmission path utilises**any** element of a public network, such as telecommunications or data services from a service provider that utilise any component of local, regional or national infrastructure, then the network is defined as a public network
Privileged Access Management (PAM)	Privileged Access Management (PAM) – sometimes also described as Privileged Account Management, refers to a set of processes and tools for granting, controlling, monitoring, and auditing privileged access.
Privileged Account	A Privileged Account is a user account with high levels of access to systems, devices and data. Privileged accounts may, for example, be able to install or remove software, upgrade operating systems, or modify system or application configurations. They may also have access to data that is not normally accessible to standard users.
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 unclassified or classified information to indicate the security measures and handling requirements that are to be applied to the information to ensure that it is appropriately protected.
Protective Security Requirements	The Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security.
Protective Security Requirements Framework	The Protective Security Requirements Framework (PSRF) is a four-tier hierarchical approach to protective security. Strategic Security Directive (tier one); Core policies, strategic security objectives and the mandatory requirements (tier two); Protocols, standards and good practice requirements (tier three); Agency-specific policies and procedures (tier four).
Public Domain Information	Official information authorised for unlimited public access or circulation, such as agency publications and websites.
Public Key Infrastructure	The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover and revoke public key certificates. SOURCE: CNSSI-4009
Public Network	A public network contains components that are outside the control of the user organisation. These components may include telecommunications or data services from a service provider that utilise any component of local, regional or national infrastructure.

Public Switched Telephone Network	An historic term describing a public network where voice is communicated using analogue communications. Today almost all communication networks are substantially or entirely digital networks.
Push-To-Talk	Handsets that have a button which must be pressed by the user before audio can be communicated, thus improving off-hook audio protection.
Quality Of Service	A process to prioritise network traffic based on availability requirements.
Radio Frequency Device	Devices including mobile phones, wireless enabled personal devices and laptops.
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	A change to 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 within the physical control of the system owner.
Removable Media	Storage media that can be easily removed from a system and is designed for removal.
Residual Risk	The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk (Institute of Internal Auditors). Also sometimes referred to as "net risk" or "controlled risk".
Rogue Wireless Access Point	An unauthorised Wireless Access Point operating outside of the control of an agency.
Salt	Salts are a random data string added to the start or the end of a hash to strengthen its resistance to attack. Typically used in the generation of a password hash or checksums.
Seconded Foreign National	A representative of a foreign government on exchange or long-term posting to an agency.
Secure Area	An area that has been certified to physical security requirements as either a Secure Area; a Partially Secure Area; or an Intruder Resistant Area to allow for the processing of classified information. Refer to the PSR for more detail on Physical Security.
Secure Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of Multipurpose Internet Mail Extension-encoded email messages.
Secure Shell	A network protocol that can be used to securely log into a remote server or workstation, executing commands on a remote system and securely transfer file(s).
Security Association	A collection of connection-specific parameters containing information about a one-way connection within IPSec that is required for each protocol used.
Security Association Lifetimes	The duration for which security association information is valid.
Security Domains	A system or collection of systems operating under a security policy that defines the classification and releasability of the information processed within the domain. It can be defined by a classification, a community of interest or releasability within a certain classification. This term is NOT synonymous with *Trust Zone*.
Security Domain Owner	The individual responsible for the secure configuration of the security domain throughout its life-cycle, including all connections to/from the domain.
Security Risk Management Plan	A plan that identifies the risks and appropriate risk treatments including controls needed to meet agency policy.
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.

Segmentation	**Segmentation** is a logical grouping of the separate components of a network or system for design, control, installation, security and management purposes. This may occur where similarities of function, control and management exist or will be of advantage.
Segregation	**Segregation** includes the development, enforcement and monitoring of rules in order to control access to systems and information and to manage or restrict the communication between network components, devices, hosts and service. Segregation is essential in all networks but particularly in entirely virtual networks, such as cloud-hosted networks.
Separation	**Separation** includes partitioning and physically dividing systems and networks into smaller components. Separation should be applied as a design and control principle to networks where agencies have physical control over devices and components, such as in-office Wi-Fi systems, MFD's, desktops, laptops and other system or user devices.
Separation, segmentation and segregation	**Separation, segmentation and segregation** are architectural, design and management strategies to limit the effect and impact of network intrusions and system attacks and exploits. They will improve the ability to detect, and also improve the speed and effectiveness of any response to such events.
Server	A computer used to run programs that provide services to multiple users. For example, a file server, email server or database server.
Session Border Controller (**SBC**)	A device (physical or virtual) used in IP networks to control and manage the signalling and media streams of real-time UC and VoIP connections. It includes establishing, controlling, and terminating calls, interactive media communications or other VoIP connections. SBCs enable VoIP traffic to navigate gateways and firewalls and ensure interoperability between different SIP implementations. Careful selection of SBCs will provide such functionality as prevention of toll fraud, resistance to denial of service attacks and resistance to eavesdropping.
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.
SSH-Agent	A programme storing private keys used for public key authentication thus enabling 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. An SOE can be applied to servers, workstations, laptops and mobile devices.
Standard Operating Procedures	Procedures for the operation of system and complying with security requirements.
System	A related set of IT equipment 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 highest classification of information for which the system is approved to store or process.
System Security 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 IT Equipment	IT equipment that has been specifically designed to minimise TEMPEST emanations.
The Principle of Least Privilege	The minimisation of access rights and permissions for users, accounts, applications, systems, devices and computing processes to the absolute minimum necessary in order to perform routine, authorised activities and maintain the safe and secure operation of agency or organisational systems.
TOP SECRET Area	Any area certified to operate at TOP SECRET, containing TOP SECRET servers, workstations or associated network infrastructure.
Traffic Flow Filter	A device that has been configured to automatically filter and control the form of network data.
Transfer Gateway	Facilitates the secure transfer of information, in one or multiple directions (i.e. 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.
Trust Boundary	The interface between two or more Trust Zones.
Trust Zone	A logical construct encompassing an area with a high degree of trust between the data, users, providers and the systems. It may include a number of capabilities such as secure boot, codesigning, trusted execution and Digital Rights Management (DRM). This term is NOT synonymous with *Security Domain*.
Trusted Source	A person or system formally identified as being capable of reliably producing information meeting defined parameters, such as a maximum data classification and reliably reviewing information produced by others to confirm compliance with defined parameters.
Tunnel Mode	An IPSec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet. The entire packet is encrypted and authenticated.
UNCLASSIFIED Information	Information that is assessed as not requiring a classification.
UNCLASSIFIED Systems	Systems that process, store or communicate information produced by the New Zealand Government that does not require a classification.
Unified Communications	The integration of real-time and near real time communication and interaction services in an organisation or agency. Unified Communications (UC) may integrate several communication systems including unified messaging, collaboration, and interaction systems; real-time and near real-time communications; and transactional applications.
Unsecure Area	An area that has not been certified to meet 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.
Virtual Private Network Split Tunnelling	Functionality that allows personnel to access both a public network and a VPN connection at the same time, such as an agency system and the Internet.
Virtualisation	The software simulation of the components of an information system and may include the simulation of hardware, operating systems, applications, infrastructure and storage.
Volatile Media	A type of media, such as RAM, which gradually loses its information when power is removed.
Waiver	The formal acknowledgement that a particular compliance requirement of the NZISM cannot currently be met and that a waiver is granted by the Accreditation Authority on the basis that full compliance with the NZISM is achieved or compensating controls are implemented within a time specified by the Accreditation Authority. Waivers are valid in the short term only and full accreditation cannot be granted until all conditions of the waiver have been met.

Waivers and Exceptions	A waiver means that some alternative controls or conditions are implemented. An exception means that the requirement need not be followed. An exception is NOT the same as a waiver.
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 list that confirms items being analysed are acceptable. A Whitelist can also be known as Allow List. It is the opposite of a Blacklist (Deny List).
Wi-Fi Protected Access	Protocols designed to replace WEP. They refer to components of the 802.11i security standard.
Wired Equivalent Privacy	Wired Equivalent Privacy (WEP), a deprecated 802.11 security standard.
Wireless Access Point	Typically also the device which connects the wireless local area network to the wired local area network. Also known as AP
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 upon 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.