PSR | Protective Security Requirements

Policy Version: 1.0 ***Last Review Date: Oct 2025***

Protective Security Requirements (PSR) Policy Framework:

INFORMATION SECURITY (INFOSEC) MANDATORY REQUIREMENTS 1-4

Introduction for document reviewers

What is this document?

This document is the final V1.0 consolidated PSR policy framework on information security (INFOSEC) implemented on 01 October 2025. It replaces all previous PSR policy information published on the PSR website.

Why has this document been developed?

In the past, PSR policy requirements were expressed on the PSR website and in publications, rather than in authoritative policy framework documents. Similar and overlapping content was spread across multiple webpages and at times expressed unclearly. This made PSR policy requirements difficult for stakeholders to find, understand, and apply.

This document aims to resolve these issues by establishing a clear and appropriate policy framework for information security. Separate policy frameworks have been developed for other PSR domains.

What has changed in this version of the framework?

This consolidated policy framework compiles the information security policy requirements set out previously on the PSR website, Capability Maturity Model, and relevant PSR guidance publications.

The content is structured according to the mandatory requirements, with consistent use of sub-headings within each mandatory requirement and numbered paragraphs.

The security measures required to comply with the PSR are expressed clearly, using MUST, SHOULD, and COULD statements.

The intent of this consolidated PSR policy framework is to clarify existing requirements, and to better support agencies to check that they are meeting these requirements. The intent is not to introduce significant or substantive change to these requirements.

Some policy requirement changes have been made, including those required to:

- resolve inconsistencies resulting from repetition and duplication of content
- incorporate essential elements (including as regards the Classification System – see below)
- align with broader expectations or existing practice (including for consistency with the NZISM – see below).

How does this document incorporate essential elements of the Classification System?

The Classification System is integral to the INFOSEC mandatory requirements. At section 2.3 of this document we have represented the existing essential elements of the Classification System, including the measures:

- contained in the Classification System policy requirements introduced in 2022 (which are in section 2.3.a), and
- included in the Classification System prior to that date (sections 2.3.b-d).

How does this policy requirement align with the NZISM?

We have worked closely with the National Cyber Security Centre in compiling this policy, which contains a small number of proposed changes to align with the NZ Information Security Manual (NZISM) and existing practices.

Has the minimum baseline for PSR changed?

The policy framework has been reviewed and clarified to ensure that it remains a robust protective security policy framework aligned with security best practice. The policy framework now articulates the minimum set of security capability and measures required for all organisations no matter their level of risk.

The minimum requirements are expressed as MUST statements and has been aligned to the PSR Capability Maturity (PS-CMM) level of 2 “Planned and Tracked” (formerly called ‘Basic’).

Table of Contents

Purpose

1. The purpose of this policy framework is to provide information to help an organisation implement effective information security measures to protect people, information, and assets. The Information Security (INFOSEC) policy requirements captures any form of information, information assets or information resources (herein referred to as 'information') including:

   a. documents and papers
   b. electronic data
   c. the software or systems and networks on which the information is stored, processed or communicated
   d. intellectual information acquired by individuals, and
   e. physical items from which information regarding design, components or use could be derived.

Who should read this policy

2. This policy framework is primarily intended for use by organisations that implement the Protective Security Requirements (PSR). This includes:

   a. government organisations that are mandated to implement the PSR, and
   b. organisations that implement the PSR on a voluntary basis.

3. As good security practice, non-mandated organisations in the public and private sectors are encouraged to adopt the PSR as appropriate to their context.

4. This policy framework should be read along with the **Information Security Policy Appendices**, **New Zealand Government Security Classification System** (Classification System), **PSR Personnel Security (PERSEC)**, **Physical Security (PHYSEC)**, and **Security Governance (GOV)** policy frameworks and appendices. This policy framework should be read along with the other protective security guidance and resources found on the PSR website.

5. This policy framework should be read along with the separate requirements and best practices for information systems and cyber security services as defined in New Zealand Information Security Manual (NZISM), NCSC Minimum Cyber Security Standards, and New Zealand National Cyber Security Centre (NCSC).

6. This information should be used by leaders and those with functional responsibility for protective security to establish their own security policies and measures to address their risks.

Introduction to the PSR

7. The PSR is New Zealand's best practice policy framework. It sets out what an organisation must do to manage security effectively. It also contains best practice guidance. See PSR Policy Framework Overview for a summary of the PSR policy requirements.

8. Protective security is a business enabler. It allows organisations to work together securely in an environment of trust and confidence, to maintain public trust and confidence, and to support strategic and operational objectives.

Required and recommended measures

9. The PSR describes when an organisation needs to consider specific security measures – also called "controls" – to comply with mandatory requirements.

10. The measures required depend on the level of risk to be managed.

Required measures

11. A measure expressed with 'MUST' (or 'MUST NOT') is mandatory for all levels of risk. An organisation must implement all mandatory measures unless it can demonstrate that a given control is not relevant in its context.

12. If a mandatory measure cannot be directly implemented, suitable compensating measures MUST be selected to manage identified risks.

Recommended measures

13. A measure expressed using 'SHOULD' (or 'SHOULD NOT') is recommended for organisations with moderate and above risks.

14. A measure expressed using 'COULD' is recommended for organisations with high and above risks.

15. Valid reasons for an organisation not implementing recommended measures could include:

    a. a measure is not relevant because there is no apparent risk, or
    b. the residual risk is acceptable, or
    c. an alternative measure of equal strength is in place.

16. Not using recommended measures without due consideration may increase residual risk for an organisation. Pose the following questions before choosing not to implement a recommended measure.

    a. Is the organisation willing to accept additional risk? If so, what is the justification for this choice?
    b. Has the organisation considered the implications for all-of-government security? If so, what is the justification for this choice?

17. A formal auditable record of how an organisation considers and decides which measures to adopt is required as part of an organisation's governance and assurance processes.

Compliance with legislation

18. When legislation requires an organisation to manage protective security in a way that is different to the PSR, that legislation takes precedence.

Why information security matters

19. Every organisation relies on the confidentiality, integrity, and availability of the information it processes, stores, and communicates.

20. Information exists in many forms (for example, electronic, printed, or spoken) and may reside inside or outside an organisation, including with providers and clients, and in the cloud.

21. Information in all forms needs to be appropriately protected: information security is a broad concept that also includes cyber-security, digital security, and ICT security.

22. Robust information security is a business enabler by helping organisations to:

    a. maintain the trust and confidence of the public, customer, and partners
    b. keep important information safe and available to those that need it
    c. reduce the risks of information being lost, damaged, or compromised
    d. avoid costs of recovery after an incident, as well as costs of downtime and lost productivity, and
    e. comply with regulation and legislation.

23. Threats and risks are increasing and evolving. Threats can come from inside and outside the organisation. Organisations are far more exposed today than ever before. Contributing factors include:

    a. increasing quantities of electronic information, and organisations are often heavily dependent on it to function.
    b. increasing use of cloud, social media, mobile, and other emerging technologies, which have increased the ways critical information can be accessed.
    c. continually evolving threats, making detection of security breaches challenging. An organisation can experience an information security breach without being aware of it. Even when the organisation is alerted to the breach, confirming the extent of the impact can be difficult.

24. Information security breaches can disrupt an organisation's ability to do business, expose its people and customers to more or increased risks, and damage its reputation. Breaches can:

    a. make it difficult or impossible to process transactions or provide core services
    b. involve a loss of intellectual property
    c. violate laws governing privacy or other types of information held in trust
    d. expose an organisation to legal proceedings from affected parties
    e. cause embarrassment at an international, national, or regional level, and
    f. erode trust between an organisation and the people it serves or works with.

Information Security Policy

25. Robust security practices are required to protect an organisation's information. When an organisation's information security measures are well designed and implemented, it reduces the risks of its information being compromised.

26. An organisation MUST keep the organisation's information secure with robust information security across the information security lifecycle and in compliance with the INFOSEC mandatory requirements.

INFOSEC Mandatory Requirements Overview

27. The four INFOSEC mandatory requirements help organisations to implement robust information security across the lifecycle. These are:

    a. INFOSEC1 – Understand what you need to protect
    b. INFOSEC2 – Design your information security
    c. INFOSEC3 – Validate your security measures
    d. INFOSEC4 – Keep your security up to date.

INFOSEC 1: Understand what you need to protect

Identify the information and ICT systems that your organisation manages. Assess the security risks (threats and vulnerabilities) and the business impact of any security breaches.

INFOSEC 1.1 Understand the value of your information

28. An organisation MUST identify the information and ICT systems that the organisation manages and its value, importance, and sensitivity. This will determine the required measures to protect it from harm.

INFOSEC 1.1.a Create an inventory of information and ICT systems

29. A comprehensive inventory helps identify the value and risk of the information used within an organisation, including those that support business continuity and disaster recovery plans.

30. An organisation MUST carry out an inventory of its information assets and ICT systems, including those that support business continuity and disaster recovery plans.

31. For each type of information asset or ICT system, an organisation SHOULD record:

    a. how the organisation (including its providers and partners) uses, processes, shares, or stores information
    b. any relevant confidentiality, integrity, availability, privacy, or legislative requirements
    c. how long it needs to keep and protect the information
    d. the minimum level of system performance or information accessibility required for the organisation to function
    e. what destruction or disposal requirements apply, and
    f. the location of the information and its physical security requirements.

INFOSEC 1.1.b Assess the impact of possible information security incidents

32. Not all information needs to be treated equally. The consequences of compromise of some information would create more harm, requiring a greater level of protection.

33. In line with the New Zealand Government Security Classification System (Classification System) and GOV2 (Take a risk-based approach), an organisation MUST assess the impact and level of harm of the information being compromised.

34. The Business Impact Levels (BILs) are a tool to help organisations assess the level of impact and consequences if its information is compromised. For example, consider the impact if:

    a. a database with official or classified information was corrupted
    b. there is unauthorised disclosure of sensitive information with a third party such as the media, another country etc., or
    c. information was accidentally released to third parties.

35. Collections of information (aggregated information) includes collections of physical documents and collections of information stored in ICT systems. Aggregated information can be more valuable than the single pieces of information it's made up of; an organisation may need extra security measures to protect it.

36. An organisation MUST consider if extra security measures are required for aggregated information. For example, if the information is classified as IN-CONFIDENCE, but should have security measures applied for the aggregation at SENSITIVE/RESTRICTED.

INFOSEC 1.2 Assess the risks to information security

37. As part of GOV2, an organisation MUST assess its information security risks and determine how it will treat the risks. Refer to GOV2 for more information.

INFOSEC 2: Design your security measures

Consider information security early in the process of planning, selection, and design. Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with:

- the New Zealand Government Security Classification System
- the New Zealand Information Security Manual
- any privacy, legal, and regulatory obligations that you operate under.

Adopt an appropriate information security management framework that is appropriate to your risks.

INFOSEC 2.1 Adopt an appropriate information security management framework

38. An information security management framework is the set of security approaches, standards, policies, and procedures adopted to manage and address the organisation's specific information security risks.

39. Consider example best-practice information security management frameworks and standards outlined in **Information Security Appendix A: INFOSEC Supporting Frameworks and Resources** for adoption depending on the specific industry and information security threats and risks.

40. An organisation MUST establish a framework to direct and coordinate the management of its information security that:

    a. is appropriate to the level of security risk in an organisation's information environment
    b. is consistent with an organisation's business needs and legal obligations, and
    c. integrates with any other frameworks governing the organisation's security.

INFOSEC 2.2 Design and implement information security measures

41. Security measures used to protect government information include:

    a. Procedural measures that restrict who can access and what can be done with government information and equipment, such as organisational policies, processes, and procedures.
    b. Physical measures that control access to areas where government information is stored or used, such as physical barriers, safes, and cabinetry.
    c. Technical measures that help to protect government information, such as security access control systems, firewalls, and encryption.

42. An organisation MUST design and implement the appropriate information security measures required to protect its information's confidentiality, integrity and availability, proportionate to the risks it faces and in line with:

    a. The New Zealand Government Security Classification System

b. The New Zealand Information Security Manual

c. Any privacy, legal, and regulatory obligations that you operate under.

INFOSEC 2.2.a Use appropriate information security design approaches

43. Effective security for information can be achieved by using multiple defensive measures which address current security threats and challenges. This approach is referred to as 'defence-in-depth' — the security of an asset is not significantly reduced with the loss or breach of any single layer of security. A defence-in-depth strategy:

a. reduces the likelihood of a successful malicious attack, and

b. minimises the damage that results from an attack.

44. An organisation MUST use appropriate and up-to-date information security design approaches when designing its security measures to address its specific risks (e.g., defence-in-depth, zero-trust architectures, security-by-design).

INFOSEC 2.2.b Implement appropriate access controls

45. An organisation MUST have measures in place for controlling access to all information, ICT systems, networks (including remote access), infrastructure and applications, as defined in the NZISM 16. Access Controls and Passwords.

46. When designing access control measures, an organisation MUST consider the following:

a. classification of the information being protected

b. threat environment

c. user access management — who should be able to access what information, including applying the principle of least privilege

d. user responsibilities and segregation of duties to protect information

e. network access control — what resources can be accessed on a network

f. system access control — secure logins

g. privileged user access management – including policies and governance

h. application and information access control

i. risks associated with mobile computing and remote working, and Bring Your Own Device (BYOD).

INFOSEC 2.2.c Address the points where your information could face critical risks

47. An organisation SHOULD use best-practice security measures to address its specific risk scenarios assessed during its risk assessment. Refer to NCSC Information Security Guidance for further information on risk scenarios that may apply.

INFOSEC 2.3 Follow the Classification System

48. Government information is all information regardless of form or format (including documents, data, audio recordings and visual images) that the New Zealand government collects, stores, processes, generates, or shares to deliver services and conduct business. This includes information from or exchanged with the public, external partners, foreign governments, contractors, or consultants and includes email, phone calls, verbal conversations, text messages, metadata, and datasets.

49. The New Zealand Government Information Security Classification System (Classification System) provides a framework for assessing the potential harm should government information be compromised and defines the minimum requirements for protecting government information.

50. A security classification defines the sensitivity of the information (i.e. the likely harm that would result from its compromise) and identifies the security measures needed to protect it. All government information requires an appropriate degree of protection to ensure its continued integrity, availability, and confidentiality.

51. See the PSR website for classification system resources.

INFOSEC 2.3.a Adopt Classification System principles

2.3.a.1 Principle 1: Organisational Accountability

52. All organisations who handle government information MUST establish the conditions that enable people to handle government information correctly and safely.

53. Organisation heads own their organisation's approach to classification and security and invest in ongoing capability and improvement. The Classification System policy and principles are embedded within their organisation's policies and procedures and people are supported and encouraged to conduct desired behaviour.

54. Organisation heads MUST establish an organisational classification policy and procedures in line with the Classification System and ensure that all people who handle government information do so correctly and safely.

55. The following requirements need to be considered when establishing classification policies and procedures:

    a. **Resource and invest** – Organisation heads MUST own and maintain their organisation's approach to classification and security, and resource and invest in ongoing capability and improvement commensurate with the risks of information compromise that the organisation faces.

    b. **Obligations** – Government information and assets MUST be handled in line with all relevant legislation, the Classification System, and regulatory requirements, including any international agreements and obligations. Organisations MUST understand their obligations and build these requirements into the organisational classification policy and procedures.

    c. **Availability and transparency** – Under legislation such as the Official Information Act 1982, Local Government Official Information and Meetings Act 1987, Privacy Act 2020, and Public Records Act 2005, organisations have an obligation to make government information available unless there is a good reason to withhold it. The relevant legislation sets the criteria for withholding information. Organisations MUST consider the public right to government information and define how they will meet these obligations within their organisational classification policies and procedures. This principle supports the core values of government transparency, accountability, and public participation. Information SHOULD be considered open, unless there is a compelling reason to withhold it.

d. **Protection** – Classification drives the appropriate security of the information. Classified information MUST be protected to ensure its availability, integrity, and confidentiality commensurate with its classification. Protection of classified information is controlled through appropriate personnel, physical, and information security mechanisms as defined within the PSR and NZISM.

e. **Originator-controlled** – The authority to classify or declassify rests with the originator and the organisation or government that controls the information. To ensure information is protected across its whole lifecycle, the originator and organisation or government that controls the information are responsible for establishing, communicating, reviewing, and managing how the information is handled by everyone with access to it. Organisations' classification policy and procedures MUST detail how originator control will be maintained over the information's lifecycle.

f. **Partner information** – Government information or assets received from or exchanged with external partners MUST be protected in accordance with legislative or regulatory requirements, including any international agreements and obligations. This policy applies equally to information entrusted to the New Zealand government by others, such as foreign governments, international organisations, NGOs, private organisations, and private individuals. Organisations' policy and procedures MUST detail the partner information security and management requirements and how these will be adhered to and monitored.

g. **Education and training** – Organisation heads MUST provide their people with timely and ongoing classification training, assess their understanding and ensure that they have the ability to fulfil their government information obligations within the Classification System. This includes training on how to securely handle government information, including how to classify it, how to share it, and how to declassify it. This training SHOULD form part of the organisation's wider information management and security training.

h. **Regular reviews** – Information sensitivity will change over the information lifecycle and the organisation's policy SHOULD prescribe when subsequent reviews of classification levels and protective markings are to take place for particular information types as part of their information and records management practices. The purpose of the review is to ensure that the protective markings were correctly applied initially and are still appropriate for the information as the information ages or changes. Outcomes of reviews should be tracked, reported, and used as learning opportunities.

i. **Measuring function and performance** – In line with PSR GOV8 (Assess your capability), Organisation heads MUST ensure that their organisation's classification capability and performance is assessed using the PSR Capability Maturity Model and annual PSR assurance process as part of their overall protective security programme.

2.3.a.2 Principle 2: Personal responsibility

56. Everyone who works in or with the New Zealand public sector, including employees, contractors, and suppliers, has a duty to classify, declassify and handle information appropriately. Individual classification, declassification, and sharing decisions are based on an effective risk assessment of the harm and impact of information compromise and in line with the organisation's classification system policies and procedures.

57. Everyone MUST take responsibility to understand and fulfil their obligations to classify, declassify, and handle information correctly in line with the organisation's classification policy and legislative, regulatory, and other organisational obligations.

58. The following requirements need to be considered and included in policy and practice to encourage personal responsibility for classifying, declassifying, and handling government information:

    a. **Duty to safeguard** – Individuals are responsible for protecting government information and assets in their care in line with their classification. Accidentally or deliberately compromising government information without authorisation may lead to harm or damage and can be a criminal offence under relevant legislation (e.g. Crimes Act 1961, Criminal Disclosure Act 2008, Summary Offences Act 1981.)

    b. **Risk assessment** – Individuals MUST make classification decisions based on the best information available. Decisions MUST be made transparently, based on a risk assessment that considers the level of harm and the likelihood of compromise.

    c. **Harm and impact** – Individuals MUST assess and be able to articulate the level of harm and impact that could eventuate to the organisation, individuals, government, or partners if the information or asset is compromised.

    d. **A considered approach** – Information is of most value when it can be used appropriately by everyone who could benefit from its use. When assessing the harm of compromise, individuals SHOULD consider all audiences who could benefit from its use and look for ways to reach the widest audience to achieve the greatest benefit. When in doubt, individuals should consider whether the particularly sensitive information could be redacted or reframed at a lower classification level to achieve the greatest value of releasing or sharing the information for a specific audience.

    e. **Avoid over-classifying** – Individuals MUST use classification appropriately. Over-classifying information causes serious harm, such as limiting access to necessary information, requiring infrastructure to store it and people to manage it, and increasing administration and cost to the New Zealand Government. Government information should only be classified when the result of compromise warrants the expense of increased protection. Government information must be classified and protectively marked at the lowest level possible that will still provide the necessary level of protection for its sensitivity.

f. **Seeking and acting on learning opportunities** – An organisation SHOULD encourage a no blame culture that focuses on learning and improving classification and handling decisions over time. Accidental or unintended over- or under-classification will occur and should be challenged and used as learning opportunities. People should be open to challenging others and being challenged themselves on classification decisions and security behaviours.

g. **Don't withhold information inappropriately** – Individuals MUST NOT use classification to withhold information inappropriately. For example, government information must not be withheld to:

i. hide violations of law, inefficiency, or administrative error

ii. prevent embarrassment to an individual, organisation, or the government

iii. restrain competition, and

iv. prevent or delay the release of information that does not need protection in the public interest.

2.3.a.3 Principle 3: Information-sharing

59. Government organisations recognise that appropriately sharing decision-useful information with relevant organisations is a core foundation to protecting New Zealand and New Zealanders from threats, and for realising the potential of information to aid government effectiveness and enable wellbeing of New Zealanders. This is underpinned by a culture of trust between partners that shared information is handled and used appropriately and safely.

60. Organisation heads MUST ensure that policies and procedures for handling classified information reinforce the value of information-sharing, collaboration, and cross-partner trust. They MUST implement effective and safe information-sharing practices within their organisation and with other trusted partners. People are supported and empowered to achieve decision-useful sharing appropriately and safely. Refer to PSR Information Sharing Guidance for more information.

61. The following requirements need to be considered when establishing organisational information-sharing policies and procedures:

a. **Stakeholders' needs** – Organisations MUST understand the stakeholders they should share classified information with or collaborate with to achieve good stewardship of government information and get the maximum benefit of the information for all New Zealanders. Organisations should look beyond their common information-sharing partners including other sector government organisations, international partners, local government, civil defence, hapū, iwi, and local communities. Organisations need to work collaboratively to understand stakeholder needs and what decision-useful information-sharing looks like.

b. **Legislative requirements** – Organisations MUST understand their information-sharing obligations under relevant legislation (e.g. Privacy Act), and regulatory or partner agreements that enable and hinder information-sharing across partners.

c. **Information flows and barriers** – Organisations SHOULD understand how classified information flows between partners (e.g., information types, channels, methods, systems) and identify the barriers to effective information-sharing. Where barriers exist, organisations should prioritise investment in removing those barriers where possible.

d. **Use of information-sharing instruments** – When appropriate, organisations SHOULD make appropriate use of available government information-sharing instruments (e.g. AISA, MoU). These instruments should include the criteria and rules for sharing between parties and any requirements for handling and declassifying classified information in compliance with their obligations.

e. **Empowering information-sharing** – Organisations MUST establish policies, procedures, and training for sharing classified information. This will give people confidence that they are complying with their obligations, contribute to increased trust in classified information-sharing, and empower people to share information appropriately, safely, and timely.

2.3.a.4 Principle 4: Information declassification

62. Government information MUST NOT remain classified indefinitely without being subject to review for declassification as defined within organisation's declassification policy. This policy MUST be in line with the Public Records Act 2005 and information management standards and SHOULD be made available to the public to improve transparency and accountability of declassification decisions.

63. Organisation heads MUST establish an organisational declassification policy and procedures in line with the Classification System and relevant legislation including Official Information Act 1984, Public Records Act 2005, Privacy Act 2020, and requirements contained in relevant international agreements or arrangements. Refer to the PSR Declassification Guidance for more information.

64. The following requirements need to be considered when establishing organisational declassification policies and procedures:

a. **Understanding classified information holdings** – To inform the design of declassification policy and criteria, an organisation MUST have a clear understanding of its classified information holdings as part of their obligations under the Public Records Act 2005 and the Information and Records Management Standard.

b. **Declassification policy** – An organisation that holds classified information MUST have a policy that establishes a systematic approach to declassifying government information. This policy must prohibit the indefinite classification of government information without transparent criteria. This policy should be made available to the public to improve transparency and accountability of declassification decisions.

c. **Declassification criteria** – Not all information may be suitable for declassification if it is of short-term or low value. Within the classification policy, an organisation MUST set up and use criteria to clearly articulate the rules for declassification in the organisation (e.g. information types, review periods, harm test rules, declassification topics and priorities). These criteria should be consistent with information and records management practices and decisions (e.g. appraisal, sentencing, and disposal.) The criteria should be used to prioritise how resources are allocated and to agree the scope and plan for a declassification programme. These criteria should be clear, transparent, and objective; and reflect the expected value to New Zealand of the declassification programme.

d. **Declassification governance** – An organisation MUST establish an appropriate governance framework for declassification. Governance must ensure that investment in declassification delivers value for the public, set precedents for reviews, arbitrate declassification decisions when conflicting opinions arise, and make final decisions on declassification matters that are referred for consideration.

e. **Declassification programme** – An organisation MUST appropriately resource and establish a regular programme for declassifying government information in line with their policy and priorities. Government organisations must report transparently to its governance body and NZ government when requested on the progress, results, and expected value that the programme delivered.

65. See also: www.archives.govt.nz/manage-information/how-to-manage-your-information.

INFOSEC 2.3.b Classify and assign protective markings

66. A security classification and any other protective markings help to keep government information secure. Protective markings are placed on information and assets as a reminder of the sensitivity of the information or equipment and define the security measures and special handling requirements that apply to it.

67. Requirements to apply protective markings also apply to information held within information and communications technology (ICT) systems such as databases, document management systems, email, or removable media. Protective markings can also be applied to information that will be delivered verbally.

68. Protective markings include classifications and endorsements. A classification determines the level of protections required while an endorsement determines the special handling and need-to-know dissemination requirements.

69. An organisation MUST classify and protectively mark information in line with the Classification System. Refer to Classification System for additional information and requirements on how to classify and protectively mark information.

70. An organisation MUST classify and label New Zealand Government equipment in line with NZISM 12.3. Product Classifying and Labelling standards.

2.3.b.1 Who sets and controls protective marking

71. The person and organisation responsible for creating or preparing the information is the 'originator' and decides on its protective marking.

72. When information is created, the originator MUST do a risk assessment of the harm or prejudice that would result from information, or assets being compromised. If adverse consequences could occur, or the organisation is legally required to protect the information, it MUST be given a protective marking. Refer Classification System for more information on how to classify.

73. Information derived directly from protectively-marked sources MUST carry, at a minimum, the highest security classification and protective marking of any of the source classifications and protective markings unless the originator agrees it can be changed.

2.3.b.2 Who can change protective markings

74. Information sensitivity will change over the information lifecycle and the protective markings need to be reviewed and changed to reflect the changes in sensitivity.

75. Only the organisation that assigns the original protective marking (the originating organisation) can change it. All organisations MUST respect this rule. If the originating organisation is disestablished or merged, the organisation assuming the former organisation's responsibilities is considered the originating organisation.

76. Originating organisations SHOULD ensure that information shared with other organisations and partners are informed of changes to protective markings and does not withhold information inappropriately.

77. If the information shared by another organisation or originator is assessed as over-classified, an organisation COULD seek agreement to remove or change a protective marking.

78. If the originating organisation does not agree to remove or change the marking, the protective markings MUST NOT be changed.

79. If your organisation wants to release, share, or transmit information that originated from another organisation, an organisation MUST agree the appropriate process with the originating organisation first.

2.3.b.3 Use of endorsement markings

80. Endorsement markings may indicate:

    a. the specific nature of information
    b. temporary sensitivities
    c. limitations on access and dissemination
    d. how recipients should handle or disclose information.

81. An endorsement MUST NOT appear without a security classification.

82. Endorsement markings SHOULD only appear when there is a clear need for special care. Refer to Classification System for how to use and apply endorsement markings.

INFOSEC 2.3.c Protect classified information

2.3.c.1 General requirements for protectively-marked information

Create a registration system

83. An organisation MUST have a system for controlling and handling government and protectively-marked information. For each document or file, an organisation's registration system needs to detail:

    a. when it was created
    b. where it is stored, and
    c. when it will be destroyed.

84. An organisation MUST follow requirements for the registration of media in the NZISM 13.2.14 Registering Media.

Manage 'Accountable material'

85. 'Accountable material' is information that requires the strictest control over its access and movement. What constitutes 'Accountable material' may vary from organisation to organisation. 'Accountable material' includes:

    a. TOP SECRET classified information.
    b. Any classified information designated as ACCOUNTABLE MATERIAL by the originator.

86. When information is made 'Accountable material', an organisation MUST ensure that 'Accountable material':

    a. has page and reference numbering.
    b. is clearly marked and handled in accordance with any special handling requirements imposed by the originator and endorsement owner as defined in the Classification System and organisation's security classification policies.
    c. has an auditable record of all incoming and outgoing material, transfer, copy or movements (such as a Classified Document Register or electronic document management system or repository).

Maintain a Classified Document Register

87. An organisation MUST maintain a Classified Document Register (CDR) for all TOP SECRET and ACCOUNTABLE MATERIAL produced or received within the organisation.

88. The CDR SHOULD include details of the documents received and all retained copies.

89. An organisation SHOULD maintain a register for SECRET information.

90. An organisation COULD use CDRs for documents with lower classifications when necessary for risk mitigation.

Audit information and systems

91. An organisation MUST develop a policy and system for allowing for auditing of hardcopy information that has protective markings.

92. An organisation MUST follow audit requirements for ICT systems and equipment as defined in the NZISM 4.3 Conducting Audits.

Use a receipt process to increase security

93. An organisation SHOULD consider having a receipt process for when protectively-marked information or equipment is delivered to your organisation. The benefits include being able to:

    a. provide confirmation that information has been delivered
    b. trace the movement of protected information, and
    c. ensure the recipient takes responsibility for protecting the information.

94. An organisation SHOULD consider the following guidance when designing their receipt process:

    a. Any type of receipt mechanism is suitable, as long as it identifies the document either by reference number or title.
    b. A reference number is often easier than a title, as the title of a document may describe the content of a protectively-marked document or, in limited cases, contain a word such as 'secret' or 'confidential'.
    c. Specify a period on the receipt (for example, 7 days) in which the recipient must sign and return the receipt.
    d. Confirm it has received all expected receipt returns within a month of their due date.

Spot-check government information

95. If held, an organisation MUST conduct or arrange at irregular intervals, a spot check of a small sample of TOP SECRET and ACCOUNTABLE MATERIAL to ensure it is accounted for and being handled and stored correctly.

96. An organisation MUST maintain a record of spot checks.

97. An organisation MUST raise and categorise any discrepancies identified as a security incident. Refer to GOV 6 – Manage security incidents for more about managing information security incidents.

98. An organisation SHOULD consider conducting spot checks at irregular intervals for other classification levels and protectively marked materials.

2.3.c.2 Specific requirements on information from foreign governments

Manage reciprocal protections under bilateral security agreements

99. New Zealand government organisations MUST adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which New Zealand or the organisation is a party. For example:

    a. Bilateral security agreements can include reciprocal protection for the exchange of protectively-marked information. In such cases, an organisation applies the equivalent New Zealand security classification marking and ensure the protection is equivalent to, but not less than, that required by the government providing the information.

b. Under bilateral agreements, an organisation usually must get permission before releasing information owned or controlled by foreign governments. This permission should be obtained in writing.

Considerations for release of foreign government information

100. Under the OIA, the organisation who receives the request for information release has the obligation to decide on whether the information can be released or withheld. In addition, the Inquiries Act may request information from an organisation on behalf of a government inquiry.

101. The absence of permission from another party to release information does not absolve an organisation from its obligations under the respective Act. The responding organisation MUST:

a. Consider the request on its own merits using harm criteria defined within the Act. The justification for withholding any particular information must outweigh the justification of the public interest of its disclosure.

b. If the harm assessment indicates that the information may be releasable, obtain permission to release the information from the originating party.

c. If authorisation attempts are exhausted, undertake due diligence to assess the harm to the bilateral information-sharing relationship and agreement if the information was released without permission. Consult MFAT for advice.

2.3.c.3 Specific requirements for protective markings that restrict access by foreign nationals

New Zealand Eyes Only (NZEO)

102. An endorsement marking of New Zealand Eyes Only (NZEO) indicates that access to information is restricted to New Zealand citizens with an appropriate security clearance on a need-to-know basis. For example, NZEO endorsement should be used when:

a. the consequences of revealing the information may jeopardise or undermine the state’s ability to decide on a particular course of action that may eventually require foreign assistance;

b. material that contains free and frank opinions/information about another state and its citizens;

c. it contains tradecraft or capability specific to the state; and/or

d. the information relates to topical matters that require National Interest considerations that may not be conducive to foreign partners wanting to conduct joint ventures.

103. An organisation MUST NOT allow foreign nationals access to NZEO endorsed information unless they have been granted an exceptional waiver.

104. Where systems process, store, or communicate NZEO endorsed information, an organisation MUST implement security controls (including encryption) that ensure that NZEO information is not passed to, or made accessible to, foreign nationals as defined in the NZISM.

105. The NZEO endorsement SHOULD NOT be used for government information with a security classification of IN-CONFIDENCE, SENSITIVE, or RESTRICTED. Refer to the NZISM for more information on NZEO requirements within systems.

106. The application of the NZEO endorsement SHOULD be carefully assessed. It requires organisations to have the systems and processes for managing NZEO and restrict who can manage and support the information and systems with NZEO markings. When the information is disseminated to different organisations, it extends the same requirements to all organisations who have access to or receive the information.

107. In exceptional situations where there is an essential business need to share NZEO endorsed information classified at CONFIDENTIAL, SECRET, or TOP SECRET with foreign nationals, an organisation MUST obtain approval from the Director-General of Security or their delegate to waive this requirement.

Releasable To (REL)

108. The Releasable To (REL) endorsement marking identifies information that is releasable to the countries or citizens of those indicated countries only. For example, //REL NZL, GBR means that the information may be passed to citizens and the governments of the United Kingdom and New Zealand only. Refer to Classification System for more information on REL and formatting and three letter nation codes.

109. 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 the country represented.

110. An organisation MUST only allow foreign nationals access to REL endorsed information where they are a citizen of the country or countries listed.

INFOSEC 2.3.d Handle government information securely

111. Levels of protection for protectively-marked information and equipment increase in line with their security classifications. The higher the security classification, the greater the need for protection.

112. An organisation MUST follow and implement all classification level specific handling requirements to protect protectively-marked information from compromise when it is created, received, stored, used, copied, shared, removed, transported, archived, or destroyed as defined in Classification Quick Guides and the section below. The quick guides provide the minimum handling requirements at each classification level (IN-CONFIDENCE, SENSITIVE/RESTRICTED, CONFIDENTIAL, SECRET, and TOP SECRET.)

2.3.d.1 Use government information securely

Dealing with verbal information

113. If information that carries a protective marking is delivered verbally (for example, through classified discussions in person or over the phone), the recipient(s) MUST be told the classification and protective marking and told how the information needs to be protected before the information is conveyed.

    a. For example, "The information I am about to convey is RESTRICTED. This information cannot be discussed or shared with anyone else without agreement from the CSO."

114. An organisation MUST ensure that verbal discussions cannot be overheard by those who are unauthorised to receive the information. Refer to: Security zones for more information.

Dealing with virtual meetings

115. An organisation MUST ensure that users understand the maximum classification level of information that they can share or discuss in virtual meetings across the different ICT systems used by the organisation.

116. Before sharing classified information virtually (e.g. verbally and/or screen sharing), an organisation MUST ensure that the systems used are accredited to protect information at the classification level or higher.

117. Information MUST NOT be used or shared at higher classifications than the ICT system is accredited to protect. For example, if an ICT system is accredited for sharing up to IN-CONFIDENCE information, you cannot disseminate, share, or discuss information at SENSITIVE or higher classifications using that ICT system.

2.3.d.2 Copy, reproduce, and transmit information securely

Copying and using photocopiers

118. To help control protectively-marked information, an organisation MUST keep the number of copies to a minimum. Only reproduce protectively-marked information when necessary.

119. Your organisation MUST develop a policy for use of photocopiers, fax machines, multifunction devices (MFDs), network printers, and similar devices to govern their use and minimise the risks associated with the devices. Refer to NZISM 11.2 for more information. These devices may:

    a. retain images of copied documents that can then be transmitted, or
    b. be connected to ICT systems that don't have the necessary level of protection.

Reducing risks when you copy and transmit protected information

120. An organisation SHOULD take steps to reduce risks of compromise when copying and transmitting protectively-marked information such as:

    a. Use 'follow me printing' capability to hold print jobs until the user authenticates and releases the job to the printer;
    b. Put approved devices in an area where all copying and transmitting activity can be observed;
    c. Ensure an authorised person stays near the device until all activity is finished; and
    d. Ensure documents are removed from the device as soon as activity is over.

Devices you can't use for copying and transmitting

121. If a device is connected to an ICT system and a document has a higher protective marking than your ICT system, the device MUST NOT be used to copy or transmit that document.

122. A protected document MUST NOT be copied or transmitted using a device connected to a public network, or a fax machine (unless that information is protected in line with the NZISM 11. Communications systems and devices.

Transmitting electronic data

123. Protectively-marked data that is imported, exported, or transferred electronically MUST be protected in line with the NZISM – 20. Data Management.

Reproducing protectively-marked information

124. When government information is reproduced, the original protective-marking and handling requirements still applies to all reproduced information. Reproduced information MUST be marked at the original marking levels or higher. These requirements apply to all government information (with or without security classifications).

2.3.d.3 Control access to information

125. Access and sharing of government information may be restricted due to its nature and sensitivity including:

    a. Limiting access to authorised people (e.g. those with the appropriate security clearance and authorisation)
    b. Limiting access to those with a need-to-know (e.g. those who require the information to perform their job.)

126. An individual's access may be restricted on:

    a. Physical locations
    b. File system permissions, including physical documents and files, such as the ability to create, read, edit or delete
    c. Application or program permissions, such as the right to run a program
    d. Data and information rights, such as the right to retrieve, print, update, or delete information in a database or system.

127. An organisation MUST brief individuals about the significance of the information and any special handling requirements before they are given access to it. Refer to the following for more information:

    a. NZISM section 16. Access Control and Passwords for information on ICT access controls
    b. See **Physical Security Appendix C: Security Zones Requirements** for specific physical location zone access controls.

Limiting access to authorised people

128. Before granting access to information with a protective marking, an organisation MUST check that the person has the right level of security clearance. See PERSEC for more information.

Limiting access to those with a 'need-to-know'

What is 'need-to-know'?

129. 'Need-to-know' is the principle that a user must have a legitimate reason to access and use information or equipment to meet an operational need. The concept of 'need-to-know' is simply that one should confirm that it is appropriate to share a piece of information before one does so.

130. For example, while a piece of intelligence may be shared relatively widely the details of the source of that information may be much more tightly guarded. Equally, a doctor at a hospital does not have a 'need-to-know' the details of a patient that they are not treating.

Who decides on 'need to know?'

131. Information is 'originator controlled' and the originator and controlling organisation or government MUST decide if the information has restrictions based on a 'need-to-know'. They will assign an endorsement marking or compartmented marking to indicate the 'need-to-know' compartment which will identify the special handling requirements for the information.

Requesting access to 'need-to-know' compartmented information

132. In most normal circumstances, 'need-to-know' is a two-way process that relies both on the organisation holding the information, and on the requestor making a reasonable request, i.e., an individual or agency should only request information when it needs it to carry out its functions. It is not sufficient to request information just because you want to know – there must be a legitimate need for the request. Further, the 'gatekeepers' of information requests may lack the knowledge to know if an information request by another person or agency is reasonable or not. If there is a valid 'need to know' then the information should be shared.

133. An organisation holding government information maintains the responsibility to check whether information should be shared. To ensure effective information sharing an organisation SHOULD use a fair and appropriate process to assess requests to share government information.

2.3.d.4 Store and file information securely

134. Government and protectively-marked information MUST be stored in line with Security Zones and NZISM requirements.

Storing electronic information

135. Government information stored electronically within ICT systems require strong security measures to protect it from compromise. The standard for ICT system security is defined within the NZISM. The organisation's Chief Information Security Officer (CISO) is responsible for ensuring their systems and that of any supplier to government who holds organisation information comply with the NZISM to ensure the information is adequately protected.

136. An ICT system will be accredited to hold government information and data up to a certain classification level. An organisation MUST register their core ICT systems classification level and accreditation status with the accreditation authority. ICT systems that are classified can include (but not limited to):

    a. Email systems
    b. Document management systems
    c. Collaboration and conferencing systems
    d. Human resource systems
    e. Financial systems, and
    f. Operational business systems and databases.

137. ICT systems may be hosted in house or in the cloud and MUST meet the NZISM minimum standards.

138. When working with ICT systems, an organisation MUST understand the highest level of classification that the system is accredited to hold. Information MUST not be stored at higher classifications than the system is accredited to hold. For example, if a system is accredited to hold up to RESTRICTED, it can only hold information classified at UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, or RESTRICTED.

Filing electronic information

139. When electronic information is added to an ICT system, where possible the classification and other protective markings SHOULD be recorded within its metadata. This will enable the automation of protective security measures based on the protective marking on the information.

140. An organisation's classification policy and procedures SHOULD detail any user requirements for recording classification and protective markings, and filing information into ICT systems that they use. Refer to the organisation's system user manuals for details on how to protectively mark and handle classified information within each ICT system that you use.

Storing physical files

141. At a minimum, a file MUST carry a protective marking equal to the highest security classification of information within it.

142. Access, usage and storage of classified physical information MUST meet the PSR physical security zone requirements. See Security Zones for more information.

Filing physical documents

143. When new information is added to a file, the file user MUST ensure that the protective marking is still appropriate. If information is added that is at a higher security classification than the file itself, the file user MUST reclassify the file before attaching the new document.

144. An organisation MUST ensure that the protective markings on files are clear and easy to distinguish from other markings.

145. An organisation MUST place TOP SECRET and SECRET documents in an appropriate file or cover immediately.

146. An organisation MUST record the location of TOP SECRET files in the CDR.

147. For information marked below SECRET, an organisation SHOULD place information in an appropriate file as soon as possible after it is created or received.

2.3.d.5 Remove, transport, and receive information securely

148. The security measures required to protect classified information during physical moves depend on:

  a. the protective markings
  b. where it is going from and to
  c. the method used for transferring the information.

149. The intended recipient MUST have the appropriate 'need-to-know' and the required level of security clearance before the information is transferred.

150. An organisation SHOULD develop a policy based on the minimum measures, as well as policy for information and material too large for the 'double barrier' principle.

151. An organisation SHOULD understand how to protect all government information with or without protective markings when you take it away from your premises.

Putting policies and processes in place

152. If there is a need to take (remove) protectively-marked information from your premises, an organisation MUST have policies and processes in place to ensure it is protected. An individual may want to take protected information to another organisation or workplace for a meeting or to work from home.

153. An organisation MUST not allow removal of TOP SECRET information for short-term work at home without approval from the New Zealand Security Intelligence Service (NZSIS) and the originating agency (if not your agency).

154. However, protected information SHOULD only be removed from an organisation's premises when:

  a. there is a definite need, and
  b. the right level of protection can be maintained en-route and at the destination.

155. An organisation MUST follow all requirements for the secure removal and transport of protectively marked information. Refer to the Classification System Resources and Classification Quick Guides for specific handling requirements at different classification levels.

Authorising removals

156. An organisation MUST ensure that removal of protectively-marked information is approved before it is taken from secure and authorised work areas.

157. An organisation MUST decide who can authorise removals. The approver MUST:

  a. be satisfied that a genuine need exists
  b. brief the person removing the information on the risks involved
  c. be satisfied that there are adequate arrangements for the safe custody of the information

d. be prepared to accept responsibility for the safe custody of the information
e. accept the risk associated with the removal.

158. An organisation MUST keep a record of all removals at TOP SECRET and SECRET levels.

Preparing for transport

159. An organisation MUST use security measures to protect protectively-marked information when it is in transit. Refer to Classification System Resources and Classification Quick Guides for more information on measures in transit. Measures can include:

a. using NZSIS-approved briefcases, satchels, seals, pouches, or transit bags
b. using special enveloping procedures
c. transporting information by hand between people with the appropriate security clearance or by authorised messengers.

Protecting electronic media

160. Electronic media, such as laptops, CDs, and USBs, used to process protectively-marked information MUST be protected to the same degree as paper-based materials.

161. The level of protection MUST be equivalent to the highest level of protectively-marked information initially placed on the media until it is sanitised.

Working away from the office or off-site

162. For regular and long-term arrangements for people working away from the office, an organisation MUST consider security requirements and recommendations in:

a. NZISM 21. Distributed Working.

163. An organisation SHOULD consider arranging for information to be transferred to a secure location (e.g., regional or branch office) rather than allowing it to be taken to a place where its safety cannot be guaranteed. For example, keeping protected information in a hotel room overnight might not be secure enough.

Receiving hard copies

164. Before allowing anyone in the organisation to receive hard copies of protectively-marked information, an organisation MUST ensure the person is aware of their responsibilities and, when necessary, hold the appropriate security clearance.

165. Protectively-marked documents SHOULD only be opened by the addressee or the alternative addressee. However, your agency head may authorise a specified person or area to open all mail and perform the related information or security management functions.

166. When someone other than the intended addressee is charged with its opening, an organisation MUST adopt the normal practice of opening the outer envelope only. The inner envelope is only be opened in the presence of the addressee.

167. The recipient of a package containing protectively-marked documents MUST verify that the:

a. information was transported by the appropriate means

b. seals and packaging are still intact.

168. An organisation MUST report any breakages, signs of tampering, or inappropriate transport methods to your CSO and the CSO of the sending agency. If the package was delivered by an NZSIS-endorsed courier , you MUST advise the NZSIS.

169. The recipient MUST check that the contents and their integrity are preserved. For example, check the pages and table of contents, and sign and return any receipt accompanying the information.

170. If your organisation keeps a register for protectively-marked documents, you MUST make sure the information is registered.

2.3.d.6 Destroy information securely

171. An organisation MUST ensure that approved procedures for destroying ICT media and information with protective markings are followed. These requirements apply to all government information and assets that are protectively marked including photographic and microfiche material. Refer to the following for destruction requirements for information and ICT assets at different classification levels:

    a. Classification System - Destroying information
    b. Classification Quick Guides
    c. NZISM 12.6 Product Sanitation and Disposal
    d. NZISM 13. Media Management Decommissioning and Disposal.

172. An organisation MUST also follow requirements when securely transporting or removing sensitive information and assets for destruction. For information on securely transporting sensitive information or assets for destruction, refer to Remove, transport, and receive information securely.

Getting advice and setting policy

173. Waste, whether it is placed in a rubbish skip or other area for collection, or delivered directly to a waste disposal service, is extremely vulnerable.

174. A Chief Security Officer (CSO) may seek advice from the NZSIS about approved methods for routine or emergency destruction of protectively-marked information.

175. An organisation MUST not use rubbish or recycling services or systems to dispose of protectively-marked information unless it has already been through an NZSIS-approved destruction process such as shredding.

176. An organisation SHOULD have a policy for destroying government information without protective markings — a policy that is in line with your security risk management plan.

Getting approval to use a contractor

177. Before your organisation enters into a contract for the destruction of paper-based information that is protectively marked CONFIDENTIAL or above, you MUST have the NZSIS's approval. They will need to be satisfied that the contractor can safeguard the information throughout the destruction process.

178. Your organisation SHOULD determine the processes you and the contractor will use to maintain an appropriate level of security throughout the pickup, transportation, and destruction of the waste.

179. Appropriate processes include:

a. the waste MUST not be left unattended at any time
b. the vehicle and storage areas MUST be appropriately secured
c. the destruction MUST be performed immediately after the material has arrived at the premises
d. organisation representatives with the right level of security clearance MUST escort the waste and witness its destruction, and
e. the destruction company staff MUST have a security clearance to the highest level of the protectively-marked information being transported and destroyed.

180. Information marked TOP SECRET and ACCOUNTABLE MATERIAL MUST be destroyed within organisation premises and only once the originating organisation has been notified. The originators may also apply special conditions to the destruction of some protectively-marked information that might prevent contracting out destruction.

INFOSEC 3: Validate your security measures

Confirm that your information security measures have been correctly implemented and are fit for purpose. Complete the certification and accreditation process to ensure your ICT systems have approval to operate.

181. The validation step provides senior executives with the confidence that information and its associated technology are well-managed, risks are properly identified and mitigated, and governance responsibilities can be met.

182. An organisation MUST validate its information security measures to find out if they've been correctly implemented and are fit for purpose.

INFOSEC 3.1 Ensure appropriate certification and accreditation

183. An organisation MUST conduct the appropriate certification and accreditation processes required for the type of security measures being implemented:

    a. Follow the certification and accreditation process defined in the NZISM 4. System Certification and Accreditation for all ICT systems.

    b. Complete certification and accreditation for the physical security of buildings, security and equipment prior to getting its ICT system accredited. Refer to PHYSEC 3 (Validate your security measures) for more information on physical security certification and accreditation.

INFOSEC 4: Keep your security up to date

Ensure that your information security remains fit for purpose by:

- monitoring for security events and responding to them
- keeping up to date with evolving threats and vulnerabilities
- maintaining appropriate access to your information

184. Threats, vulnerabilities, and risks evolve over time as technology, business, and information demands change.

185. An organisation MUST ensure that their security measures keep pace with this change to remain relevant and effective.

INFOSEC 4.1 Analyse evolving security vulnerabilities and threats

186. Vulnerabilities may exist within your existing security measures. For example, consider:

   a. How well would the current security measures protect information against the identified risks and effects?
   b. How well are your security procedures followed? How do you know?
   c. If information such as customer records, financial data and intellectual property were stolen, could the organisation quickly and accurately determine what was lost and be able to recover it?
   d. Are there multiple layers of security in place within current security measures, referred to as 'defence-in-depth, to reduce the risk of breach if there is a loss of a single layer?
   e. What action is required to improve the organisation's current security measures?

INFOSEC 4.1.a Monitor for security events and vulnerabilities

187. To manage vulnerabilities in its information security an organisation MUST:

   a. Monitor its systems, networks, and processes for security vulnerabilities and security events. Observe system and network events, configurations, and processes to detect suspicious or unauthorised events.
   b. Assess its security measures against best practice and known security vulnerabilities.
   c. Document, analyse, prioritise, and report on vulnerabilities that pose the most immediate risk to the organisation.
   d. Apply fixes and track them to completion to mitigate the risk of an organisation's information being compromised.

INFOSEC 4.1.b Monitor evolving threats to information security

188. An organisation MUST identify and document the potential threats to its information security, assess its risks, and ensure that the risks are adequately managed.

189. Threats are continually evolving. An organisation SHOULD refer to international information security threat information to stay ahead of emerging threats. Refer to Appendix A for list of international threat catalogues.

INFOSEC 4.2 Keep information security measures up to date

190. An organisation's security measures are only effective if they reflect its actual assessed risks, and they are kept updated to reflect emerging risks and threats. An organisation MUST:

   a. Document and maintain its operating procedures and make them available to all users who need them.
   b. Keep access control systems up to date as personnel (including contractors and suppliers) join, change jobs, and leave the organisation, and when access measures are introduced or changed.
   c. Protect its ICT equipment from malware, including personal devices that have access to an organisation's information.
   d. Apply security patches and updates regularly to ensure that its information is protected from identified and addressed security vulnerabilities.
   e. As part of GOV 3, test its business continuity and disaster recovery plans when new processes, ICT systems, and capability are introduced. Ensure the organisation is adequately prepared for a significant service interruption, attack or other serious security incident.

INFOSEC 4.3 Respond to information security incidents

191. When an incident happens, an organisation needs to act quickly to reduce any impact and to recover as quickly as possible. Later it may also need to restore the confidence of any partners or clients affected by an incident.

192. When an information security incident occurs, an organisation MUST follow GOV6 to ensure that the incident is managed effectively. Refer to GOV6 for more information.

INFOSEC 4.4 Review security measures

193. An organisation MUST undertake regular reviews of its information security framework to ensure its security measures remain fit for purpose.

INFOSEC 4.4.a Conduct periodic reviews and assure compliance

194. As part of GOV8, an organisation MUST conduct an annual information security self-assessment. See GOV8 for more information.

195. An organisation MUST regularly monitor, review, and audit the degree to which its information security policies are being implemented and followed. This includes:

   a. use of operational procedures
   b. handling of protectively-marked materials
   c. supply chain and partners services, reports and records, and
   d. compliance with relevant legislation, requirements and standards.

196. An organisation MUST minimise the opportunity for unauthorised access to information system audit tools to limit the potential to misuse or compromise them.

197. To minimise the risk of disruption to organisational business processes, an organisation SHOULD plan, review, and agree suitable monitoring requirements for operational systems.

INFOSEC 4.4.b Identify changes required to organisational information security

198. Your organisation's environment is dynamic and will change. An organisation MUST identify which changes in its environment might affect its information security and be prepared to restart the information security lifecycle. These changes may trigger either the:

    a. **Retire** phase of the information security lifecycle when systems or information are no longer required, or
    b. **Understand** phase to re-start the information security lifecycle as information security requirements change.

199. When changes occur in how an organisation uses and organises its information, an organisation MUST use this information to inform improvements to security measures. Consider these change scenarios:

    a. Is the information it holds being used in new ways? This includes information the organisation collects from others (inputs), information it provides to others (outputs), work and information flows inside or outside the organisation (processes), and information interfaces between organisations or systems (connections).
    b. Is a new supplier, provider, or partner entering the organisation to fulfil a specific need?
    c. Are there improvements to internal or external security services being planned?
    d. Have new security threats or vulnerabilities been identified?

INFOSEC 4.5 Retire information securely

200. An organisation MUST archive, repurpose, or securely destroy of information and supporting ICT systems that are no longer required in compliance with relevant legislation, Classification System, NZISM, and best practice standards. Consider:

    a. declassification of information and equipment when it no longer needs to be protectively marked
    b. disposal of information and related equipment
    c. any obligations to contact the original author, and
    d. archiving and / or disposal of information stored in the cloud.